

REPORT ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN
PARLIAMENT AND OF THE COUNCIL ON PREVENTING THE DISSEMINATION OF
TERRORIST CONTENT ONLINE

(2018/0331(COD) – COM(2018)0640 –LIBE/8/14582)

SECTION I
GENERAL PROVISIONS

Compromise 1

Covers: AMs CULT 1, 14 (Rapp), 15 (Rapp), 16 (Rapp), 254 (Schaake), 255 (Weidenholzer), 256 (Gomes), 261 (Schaake), 262 (Weidenholzer), 263 (Dalton), 264 (Gomes), 265 (Joly), 266 (Schaake), 267 (Ernst), 271 (Hedh), 272 (Pagazaurtundúa), 273 (Wikström), 274 (Corazza), 276 (Weidenholzer), 277 (Schaake), 278 (Ernst), 279 (Sippel), 280 (Sippel), 281 (Corazza), 282 (Joly), 283 (Weidenholzer), 306 (Ernst), IMCO 38, 39, 42, 43, CULT 25, 26, 28, 29,

AMs falling: AMs 37, 257 (Ernst), 258 (Joly), 259 (Sippel), 260 (Ernst), 268 (Schaake), 269 (Weidenholzer), 270 (Zijlstra), 275 (Joly), 284 (Sippel), IMCO 40, 41, CULT 27

Title

Report on the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on **tackling** ~~preventing~~ the dissemination of terrorist content online

Article 1

Subject matter and scope

1. This Regulation lays down **targeted uniform (254)** rules to **tackle prevent (254, 255)** the misuse of hosting services for the **public (256)** dissemination of terrorist content online. It lays down in particular:
 - (a) rules on **reasonable and proportionate (261)** duties of care to be applied by hosting service providers in order to **tackle prevent the public (262, 263, 264)** dissemination of terrorist content through their services and ensure, where necessary, its swift removal;
 - (b) a set of measures to be put in place by Member States to identify terrorist content, to enable its swift removal by hosting service providers **in accordance with Union law providing suitable safeguards for freedom of expression and the freedom to receive and impart information and ideas in an open and democratic society (266, 267)** and to facilitate cooperation

with the competent authorities in other Member States, hosting service providers and where appropriate relevant Union bodies.

2. This Regulation shall apply to hosting service providers offering services in the Union **to the public (CULT 29)**, irrespective of their place of main establishment.
 - 2a. ***This Regulation shall not apply to content which is disseminated for educational, artistic, journalistic or research purposes, or for awareness raising purposes against terrorist activity, nor to content which represents an expression of polemic or controversial views in the course of public debate. (272, 275, 276, 277, 306)***
 - 2b. ***This Regulation shall not have the effect of modifying the obligation to respect the rights, freedoms and principles as referred to in Article 6 of the Treaty on the European Union, and shall apply without prejudice to fundamental principles in Union and national law relating to freedom of speech, freedom of the press and the freedom and pluralism of the media. (273, 274, 280)***
 - 2c. ***This Regulation is without prejudice to Directive 2000/31/EC. (278, 279, 282, 283)***

Corresponding recitals to Article 1 (recitals 1 to 7):

Covers: AMs 39 (Joly), 44 (Chinnici), IMCO 1, CULT 2

AMs falling: AMs 40 (Bay), 41 (Sippel), 42 (Weidenholzer), 43 (Ernst), 45 (Boni), 46 (Pagazaurtundúa), 47 (Benova)

- (1) This Regulation aims at ensuring the smooth functioning of the digital single market in an open and democratic society, by **tackling** ~~preventing~~ (39) the misuse of hosting services for terrorist purposes **and contributing to public security in European societies (44)**. 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, **the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media. (39)**

Covers: CULT 4

AMs falling: AMs 50 (Chinnici), 51 (Grapini), 52 (Weidenholzer), 53 (Ernst), IMCO 3

- (2) Hosting service providers active on the internet play an essential role in the digital economy by connecting business and citizens, **providing learning opportunities (50)** 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.

Covers: AMs 1 (Rapp), 56 (Chinnici), 58 (Joly), 57 (Bay), IMCO 4, CULT 5

AMs falling: AMs 55 (Ernst), 59 (Sippel), 60 (Weidenholzer)

- (3) ***While not the only factor,*** the presence of terrorist content online has ***proven to be a catalyst for the radicalisation of individuals who have committed terrorist acts, and therefore has (CULT 4)*** 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 ***proportionate to (58)*** 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 (58)*** tackle terrorist content disseminated through their services, ***whilst taking into account the fundamental importance of the freedom of expression and freedom to receive and impart information and ideas in an open and democratic society. (56, 57, IMCO 4)***

Covers: AMs 64 (Joly), IMCO 5

AMs falling: AMs 61 (Ernst), 62 (Weidenholzer), 65 (Grapini), 63 (Chinnici), CULT 6

- (4) Efforts at Union level to counter terrorist content online commenced in 2015 through a framework of voluntary cooperation between Member States and hosting service providers need to be complemented by a clear legislative framework in order to further reduce accessibility to terrorist content online and adequately address a rapidly evolving problem. This legislative framework seeks to build on voluntary efforts, which were reinforced by the Commission Recommendation (EU) 2018/334¹ 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 (64)*** and by the European Council to improve the automatic detection and removal of content that incites to terrorist acts.

Covers: AMs 66 (Joly), 67 (Boni), 68 (Mamikins), 71 (Ernst), 72 (Weidenholzer), IMCO 6

AMs falling: AMs 69 (Pagazaurtundúa), 70 (Schaake), 73 (Grapini), CULT 7

- (5) The application of this Regulation should not affect 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

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).

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).

providers in specific cases where the conditions under ~~Article 14~~ of Directive 2000/31/EC for liability exemption are not met.

Covers: AMs 74 (Joly), 75 (Weidenholzer), IMCO 7

AMs falling: AM 76 (Ernst)

- (6) Rules to *tackle* ~~prevent~~ the misuse of hosting services for the dissemination of terrorist content online in order to guarantee the smooth functioning of the internal market are set out in this Regulation **and should fully (75)** ~~in full~~ respect of the fundamental rights protected in the Union's legal order and notably those guaranteed in the Charter of Fundamental Rights of the European Union.

Covers: AMs 2 (Rapp), 80 (Weidenholzer), 79 (Chinnici), CULT 9

AMs falling: AMs 77 (Joly), 78 (Ernst), 81 (Boni), 82 (Sippel), IMCO 8

- (7) This Regulation **seeks to (80)** ~~contributes to~~ the protection of public security **and should establish (80)** ~~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, **the freedom to receive and impart (80) information and ideas, the rights to respect for private and family life and the protection of personal data** (CULT 9) which constitutes ~~one of~~ the essential foundations of a pluralist, democratic society, and ~~are is one of~~ the values on which the Union is founded. **Any measures should avoid (2) constituting** interference in the freedom of expression and information **and insofar as possible (2)** ~~should be strictly targeted, in the sense that they must serve to~~ **tackle** ~~prevent~~ the dissemination of terrorist content **through a strictly targeted approach**, but without thereby affecting the right to lawfully receive and impart information, taking into account the central role of hosting service providers in facilitating public debate and the distribution and receipt of facts, opinions and ideas in accordance with the law. **Effective online counterterrorism measures and the protection of freedom of expression are not conflicting, but complementary and mutually reinforcing goals. (79)**

Compromise 2

Covers: AMs 17 (Rapp), 18 (Rapp), 287 (Ernst), 288 (Joly) 289 (Boni), 290 (Sippel), 291 (Gomes), 292 (Dati), 293 (Weidenholzer), 294 (Pagazaurtundúa), 295 (Joly), 301 (Dati), 302 (Sippel), 303 (Weidenholzer), 304 (Boni), 345 (Schaake), 346 (Pagazaurtundúa), 347 (Dati), 348 (Joly), 349 (Boni), 350 (Gomes), 351 (Ernst), 352 (Sippel), 353

(Weidenholzer) 354 (Sippel), 355 (Weidenholzer), 360 (Weidenholzer), 361 (Joly) 362 (Ernst), 363 (Boni), IMCO 44, 45, 52, CULT 30, 31, 32, 37, 62

AMs falling: AMs 285 (Pagazaurtundúa), 286 (Schaake), 296 (Weidenholzer), 297 (Sippel), 298 (Joly), 299 (Weidenholzer), 300 (Joly), 342 (Weidenholzer), 356 (Sippel), 357 (Ernst), 358 (Weidenholzer), 359 (Joly), IMCO 46, 47, 48, 49, 50, 51, CULT 33-36, 38, 39

Article 2
Definitions

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

- ~~-(1) 'information society services' means the services as referred to in point (a) of Article 2 of Directive 2000/31/EC. (360)~~
- (1) 'hosting service provider' means a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to **the public** ~~third parties.~~(288, 289, 290, 291, 292, 293, 294, 295) **This applies only to services provided to the public at the application layer. Cloud infrastructure providers and cloud providers are not considered hosting service providers. It does not apply either to electronic communications services as defined in Directive (EU) 2018/1972; (IMCO 44, 287)**
- (2) 'content provider' means a user who has provided information that is, or that has been, stored **and made available to the public (295)** at the request of the user by a hosting service provider;
- (3) 'to offer services in the Union' means: enabling legal or natural persons in one or more Member States to use the services of the hosting service provider which has a substantial connection to that Member State or Member States, such as
- (a) establishment of the hosting service provider in the Union;
 - (b) significant number of users in one or more Member States;
 - (c) targeting of activities towards one or more Member States.
- ~~(4) 'terrorist offences' means offences as defined in Article 3(1) of Directive (EU) 2017/541~~
- (5) 'terrorist content' means one or more of the following **material information**:
- (a) ~~inciting or advocating, including~~ **the commission of one of the intentional 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** ~~acts~~ **may** be committed intentionally;
 - (b) **soliciting another person or group of persons to commit or contribute to the commission of one of the offences listed in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, thereby causing a danger that one of more such**

~~offences may be committed intentionally; encouraging the contribution to terrorist offences~~

~~(c) **soliciting another person or group of persons to participate in promoting the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way in particular by encouraging the participation in or support to a terrorist group within the meaning of Article 4 2(3) of Directive (EU) 2017/541, thereby causing a danger that one of more such offences may be committed intentionally;**~~

~~(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; (IMCO AM 47, 48, 49, 50)**~~

~~(e) **depicting the commission of one or more of the offences listed in points (a) to (i) of Article 3 (1) of Directive (EU) 2017/541, and thereby causing a danger that one or more such offences may be committed intentionally;**~~

- (6) 'dissemination of terrorist content' means making terrorist content available to **the public (342, 343, 346, 347, 348, 349, 350, 351, CULT 37)** third-parties on the hosting service providers' services;
- (5) 'terms and conditions' means all terms, conditions and clauses, irrespective of their name or form, which govern the contractual relationship between the hosting service provider and their users;
- ~~(1) '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;~~
- (6) 'main establishment' means the head office or registered office within which the principal financial functions and operational control are exercised;-
- (9a) 'competent authority' means a single designated judicial authority or functionally independent administrative authority in the Member State (CULT 31).**

Corresponding recitals to Article 2 (Recitals 9-10)

Covers: AM 89 (Voss), 93 (Dati), IMCO 12

AMs falling: AM 90 (Weidenholzer), 91 (Sippel), 92 (Joly), 94 (Gomes), 95 (Chinnici), 96 (Bay), 97 (Ernst), 98 (Boni), 99 (Benova), 100 (Schaake), CULT 11

- (9) In order to provide clarity about the actions that both hosting service providers and competent authorities should take to **tackle 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 Council³. Given the need to **tackle** address the most harmful terrorist **content** propaganda online, the definition should capture material and information that incites, encourages or **solicits** advocates the commission or contribution to the commission of terrorist offences, provides instructions for the commission of such offences or **solicits** promotes the participation in activities of a terrorist group **thereby causing a danger that one or more such offences may be committed intentionally. The definition should also cover content that intentionally provides guidance for the making and the use of explosives, firearms, any other weapons, noxious or hazardous substances as well as Chemical, Biological, Radiological and Nuclear (CBRN) substances and any guidance on other methods and techniques, including the selection of targets, for the purpose of committing terrorist offences. (AM 89)** 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 and their potential to lead to harmful consequences, thereby affecting the security and safety of persons. The fact that the material was produced by, is attributable to or disseminated on behalf of an EU-listed terrorist organisation or person constitutes an important factor in the assessment. Content disseminated for educational, journalistic, research purposes **or for awareness-raising purposes against terrorist activity** 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.

- (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 **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 **the public** 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. **It should not apply to cloud services, including business-to-business cloud services, with respect to which the service provider has no contractual rights concerning what content is stored or how it is processed or made publicly available by its customers or by the end-users of such customers, and where the service provider has no technical capability to remove specific content stored by their customers or the end-users of their services.**

³ 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).

Corresponding changes in the Annex I, Section B, paragraph 2, indents 3-4

Covers:

Ams falling: 739 (Joly), 740 (Joly), 741(Joly) , 742(Joly) , 743(Joly) , 744 (Joly)

Annex I, Section B, lines relating to the definition of terrorist content

.....

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 **listed in points (a) to (i) of Article 3 (1) of Directive (EU) 2017/541** (Article 2 (5) a);

~~encourages the contribution~~ **solicits another person or group of persons to commit** or contribute to **the commission** ~~to~~ of terrorist offences **listed in points (a) to (i) of Article 3 (1) of Directive (EU) 2017/541** (Article 2 (5) b);

~~promotes the activities of a terrorist group, encouraging participation in or support of the group (Article 2 (5) c)~~ **solicits another person or group of persons to participate in** the activities of a terrorist group ~~terrorist group~~ **listed in points (a) to (i) of Article 3 (1) of Directive (EU) 2017/541** (Article 2 (5) c);

provides instructions or techniques **on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods** ~~instructions or~~ techniques for committing terrorist offences **listed in points (a) to (i) of Article 3 (1) of Directive (EU) 2017/541** (Article 2 (5) d);

depicting the commission of offences listed in points (a) to (i) of Article 3 (1) of Directive (EU) 2017/541 (Article 2(5)(e).

SECTION II

MEASURES TO PREVENT THE PUBLIC DISSEMINATION OF TERRORIST CONTENT ONLINE

Compromise 3

Covers: AMs 19 (Rapp), 365 (Joly), 366 (Weidenholzer), 367 (Sippel), 368 (Boni), 369 (Schaake), 370 (Sippel), 371 (Weidneholzer), 372 (Ernst), 373 (Schaake), 377 (Sippel), 378 (Weidenholzer), IMCO 53, CULT 40, 41, 42

AMs falling: AMs 364 (Ernst), 374 (Joly), 375 (Weidenholzer), 376 (Sippel)

Article 3
Duties of care

1. ~~Hosting service providers shall take appropriate, reasonable and proportionate actions **act** in accordance with this Regulation against the dissemination of terrorist content and to **to protect users from terrorist content. They shall do so** In doing so, they shall act take appropriate, reasonable and proportionate actions in accordance with this Regulation, 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 (19, 365, IMCO 53)** to the fundamental rights of the users and take into account the fundamental importance of the freedom of expression, **the freedom to receive and impart information and ideas** in an open and democratic society **and with a view to avoiding removal of content which is not terrorist.**(366).~~
 - 1a. **These duties of care shall not amount to a general obligation on hosting service providers to monitor the information they transmit or store (19, 365, 368), nor to a general duty to actively seek facts or circumstances indicating illegal activity (370, 371, IMCO 53).**
 2. ~~Hosting service providers shall include in their terms and conditions, and apply, provisions to prevent the **public** dissemination of terrorist content.~~
 - 2 a. **Where hosting service providers obtain knowledge or awareness of terrorist content on their services, they shall inform the competent authorities of such content and remove it expeditiously (377, 378).**
 - 2b. **Hosting service providers who meet the criteria of the definition of video-sharing platforms providers under Directive (EU) 2018/1808 shall take appropriate measures to tackle the dissemination of terrorist content in accordance with Article 28b, paragraph 1(c) and paragraph 3 of Directive (EU) 2018/1808.**(CULT 42)

Corresponding Recital to Article 3: Recital 12

Covers: AMs 114 (Joly), 116 (Weidenholzer), IMCO 14

AMs falling: AMs 115 (Bay), 117 (Ernst), CULT 13

- (12) Hosting service providers should apply certain duties of care, in order to **tackle prevent (114, 116)** the dissemination of terrorist content on their services **to the public**. 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 (IMCO 14)**. Duties of care should include that, when applying this Regulation, hosting services providers act in a **transparent, (IMCO 14)** 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~~, **the freedom to receive and impart information and ideas in an open and democratic society and the freedom and pluralism of the media (114, IMCO 14)**.

Compromise 4 (Rapporteur)

Covers: AMs 380 (Rapp), 381 (Pagazaurtundúa), 382 (Weidenholzer), 383 (Mamikins), 384 (Joly), 385 (Sippel), 387 (Pagazaurtundúa), 390 (Joly), 391 (Boni), 392 (Lenaers), 393 (Sippel), 394 (Weidenholzer), 395 (Schaake), 396 (Ernst), 397 (Sippel), 398 (Weidenholzer), 399 (Joly), 400 (Ernst), 401 (Weidenholzer), 402 (Pagazaurtundúa), 404 (Schaake), 405 (Schaake), 407 (Weidenholzer), 408 (Joly), 409 (Schaake), 410 (Joly), 411 (Weidenholzer), 415 (Joly), 416 (Ernst),), 426 (Ernst), 429 (Ernst), 441 (Lenaers), 442 (Dalton), IMCO 55, 58, 59, 60, 61, 64, CULT 43, 44, 46, 48, 53

AMs falling: AMs 379 (Gomes), 386 (Ernst), 388 (Ernst), 389 (Gomes), 403 (Schaake), 406 (Joly), 412 (Ernst), 413 (Boni), 414 (Joly), 417 (Weidenholzer), 418 (Gomes), 419 (Rapp), 420 (Pagazaurtundúa), 421 (Gomes), 422 (Pagazaurtundúa), 423 (Joly), 424 (Pagazaurtundúa), 425 (Grapini), 427 (Weidenholzer), 428 (Schaake), 430 (Joly), 431 (Dati), 432 (Ernst), 433 (Weidenholzer), 434 (Joly), 435 (Schaake), 436 (Schaake), 437 (Ernst), 438 (Weidenholzer), 439 (Pagazaurtundúa), 440 (Joly), 441 (Lenaers), 442 (Rapp), 443 (Voss), IMCO 57, 62, 63, CULT 45, 47, 14

Article 4

Removal orders

1. ~~If the competent authority considers that the response to a referral has been insufficient it~~ The competent authority **of the Member State of main establishment of the hosting service provider** shall have the power to issue a ~~decision~~ **removal order** requiring the hosting service provider to remove terrorist content or disable access to it **in all Member States**.
- 1a. **The competent authority of a Member State where the hosting service provider does not have its main establishment or does not have a legal representative may request access to be disabled to terrorist content and enforce this request within its own territory.**
- 1b. **If the relevant competent authority has not previously issued a removal order to a hosting service provider it shall contact the hosting service provider, providing information on procedures and applicable deadlines, at least 12 hours before issuing a removal order.**
2. Hosting service providers shall remove terrorist content or disable access to it **as soon as possible and** within one hour from receipt of the removal order.
3. Removal orders shall contain the following elements in accordance with the template set out in Annex I:
 - (a) identification of the competent authority **via an electronic signature** 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 **and a specific (401)**at least, reference to the categories of terrorist content listed in Article 2(5);

- (c) *an exact* Uniform Resource Locator (URL) and, where necessary, additional information enabling the identification of the content referred;
 - (d) a reference to this Regulation as the legal basis for the removal order;
 - (e) date and time stamp of issuing;
 - (f) *easily understandable* information about redress available to the hosting service provider and to the content provider, *including redress with the competent authority as well as recourse to a court as well as deadlines for appeal*;
 - (g) where ~~relevant~~ *necessary and proportionate*, the decision not to disclose information about the removal of terrorist content or the disabling of access to it referred to in Article 11.
- ~~4. Upon request by the hosting service provider or by the content provider, the competent authority shall provide a detailed statement of reasons, without prejudice to the obligation of the hosting service provider to comply with the removal order within the deadline set out in paragraph 2.~~
 5. The competent authorities shall address removal orders to the main establishment of the hosting service provider or to the legal representative designated by the hosting service provider pursuant to Article 16 and transmit it to the point of contact referred to in Article 14(1). Such orders shall be sent by electronic means capable of producing a written record under conditions allowing to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order.
 6. Hosting service providers shall ~~acknowledge receipt and (426)~~, 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, *including for technical or operational reasons*, it shall inform, without undue delay, the competent authority, explaining the reasons, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the reasons invoked are no longer present.
 8. ~~If~~ the hosting service provider *may refuse to execute the removal order if cannot* ~~comply with the removal order because the removal order contains manifest errors or does not contain sufficient information to execute the order.~~ It shall inform the competent authority without undue delay, asking for the necessary clarification, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the clarification is provided.
 9. The competent authority which issued the removal order shall inform the competent authority which oversees the implementation of *specific* ~~proactive~~ measures, referred to in Article 17(1)(c) when the removal order becomes final. A removal order 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 4a (new)

Consultation procedure for removal orders

1. *The competent authority which issues a removal order under article 4(1a) shall submit a copy of the removal order to the competent authority referred to in Article 17(1)(a) in which the main establishment of the hosting service provider is located at the same time it is transmitted to the hosting service provider in accordance with Article 4(5).*
2. *In cases where the competent authority of the Member State in which the main establishment of the hosting service provider is located has reasonable grounds to believe that the removal order may impact fundamental interests of that Member State, it shall inform the issuing competent authority. The issuing authority shall take these circumstances into account and shall, where necessary, withdraw or adapt the removal order.*

Article 4b (new)

Cooperation procedure for issuing an additional removal order

1. *Where a competent authority has issued a removal order under article 4(1a), that authority may contact the competent authority of the Member State where the hosting service provider has its main establishment in order to request that the latter competent authority also issue a removal order under Article 4(1).*
2. *The competent authority in the Member State where the main establishment of the hosting service provider is located shall either issue a removal order or refuse to issue an order as soon as possible but no later than within one hour of being contacted under paragraph 1 and shall inform the competent authority that issued the first order of its decision.*
3. *In cases where the competent authority in the Member State of main establishment needs more than one hour to make its own assessment of the content, it shall send a request to the hosting service provider concerned to disable temporarily the access to the content for up to 24 hours, during which time the competent authority shall make the assessment and send the removal order or withdraw the request to disable the access.*

Corresponding Recital to Article 4: Recitals 13 and 14

- (13) The procedure and obligations resulting from legal **removal** 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 **a judicial authority**ies or a **functionally independent** administrative **or** law enforcement **authority** 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.~~

(14) The competent authority should transmit the removal order directly to ~~the addressee and contact~~ point of contact the **hosting service provider and where the hosting service provider’s main establishment is in another Member State, to the competent authority of that Member state** by any electronic means capable of producing a written record under conditions that allow the service provider to establish authenticity, including the accuracy of the date and the time of sending and receipt of the order, such as by secured email and platforms or other secured channels, including those made available by the service provider, in line with the rules protecting personal data. This requirement may notably be met by the use of qualified electronic registered delivery services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council⁴.

Corresponding Annexes :

Annex I text under title and Section A

Covers:
Ams falling: AM 735 (Joly), AM 736 (Joly), AM 737 (Joly), IMCO 124,IMCO 125,

ANNEX I

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

Under Article 4 of Regulation (EU)...⁵ the addressee of the removal order shall remove terrorist content or disable access to it, within one hour from receipt of the removal order from the competent authority.

In accordance with Article 7 of Regulation (EU) ...⁶, addressees must preserve content and related data, which has been removed or access to it disabled, for six months or longer upon request from the competent authorities or courts.

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

SECTION A:

Issuing Member State:

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

Addressee (legal representative)

Addressee (contact point)

4 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

5 Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (OJ L ...).

6 Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (OJ L ...).

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

 Time and date of issuing the removal order

 Reference number of the removal order:

Annex I, Section B, title and paragraphs 1 and 3

Covers :

Ams falling; AM 738, IMCO 126, IMCO 127, AM 744 (Joly), IMCO 128

SECTION B: Content to be removed or access to it disabled within one hour:
 A URL and any additional information enabling the identification and exact location of the content referred:
(.....) Paragraph 2 covered under COMP 2 on definitions
 Additional information on the reasons why the content is considered terrorist content (optional):

Annex I, Section D

Covers:

Ams falling; 747 (Joly)

SECTION D: Informing Member State of jurisdiction
 Tick if the state of jurisdiction of the addressee is other than the issuing Member State:
 a copy of the removal order is sent to the relevant competent authority of the state of jurisdiction

Annex I, Section E

Covers:

Ams falling: AM 748 (Joly), 749(Joly), 750 (Joly)

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

- judge, court, or investigating judge
- law enforcement authority
- other competent authority → please complete also Section (F)

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

Name of authority:

.....

Name of its representative:

.....

Post held (title/grade): File No:.....

.....

Address:.....

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

.....

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

.....

Email:

Date:

.....

Official stamp (if available) and signature⁷:

.....

Annex I, Section F

Covers:

Ams falling: 751 (Joly)

SECTION F: Contact details for follow-up

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

.....

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

⁷ A signature may not be necessary if sent through authenticated submission channels.

.....

Annex III, Section B
Covers: AM 752 (Dati) and CULT 84
AMs falling: AM 753 (Joly)

SECTION B: Reasons for non-execution

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

- force majeure* or de facto impossibility not attributable to the addressee or the service provider, **including for technical or operational reasons (752, CULT 84)**
- the removal order contains manifest errors
- the removal order does not contain sufficient information

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

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

Alternative Compromise 4a (Greens/EFA - GUE/NGL)

Covers: 380 (Rapp), 381 (Pagazaurtundúa), 382 (Weidenholzer), 383 (Mamikins), 384 (Joly), 385 (Sippel), 387 (Pagazaurtundúa), 390 (Joly), 391 (Boni), 392 (Lenaers), 393 (Sippel), 394 (Weidenholzer), 395 (Schaake), 396 (Ernst), 397 (Sippel), 398 (Weidenholzer), 399 (Joly), 400 (Ernst), 401 (Weidenholzer), 402 (Pagazaurtundúa), 404 (Schaake), 405 (Schaake), 407 (Weidenholzer), 408 (Joly), 409 (Schaake), 410 (Joly), 411 (Weidenholzer), 415 (Joly), 416 (Ernst),), 426 (Ernst), 429 (Ernst), 441 (Lenaers), 442 (Dalton), IMCO 55, 58, 59, 60, 61, 64, CULT 43, 44, 46, 48, 53

AMs falling: AMs 379 (Gomes), 386 (Ernst), 388 (Ernst), 389 (Gomes), 403 (Schaake), 406 (Joly), 412 (Ernst), 413 (Boni), 414 (Joly), 417 (Weidenholzer), 418 (Gomes), 419 (Rapp), 420 (Pagazaurtundúa), 421 (Gomes), 422 (Pagazaurtundúa), 423 (Joly), 424 (Pagazaurtundúa), 425 (Grapini), 427 (Weidenholzer), 428 (Schaake), 430 (Joly), 431 (Dati), 432 (Ernst), 433 (Weidenholzer), 434 (Joly), 435 (Schaake), 436 (Schaake), 437 (Ernst), 438 (Weidenholzer), 439 (Pagazaurtundúa), 440 (Joly), 441 (Lenaers), 442 (Rapp), 443 (Voss), IMCO 57, 62, 63, CULT 45, 47, 14

Article 4
Removal orders

2. ~~If the competent authority considers that the response to a referral has been insufficient it~~ The competent authority **of the Member State of main establishment of the hosting service provider** shall have the power to issue a ~~decision~~ **removal order** requiring the hosting service provider to remove terrorist content or disable access to it **in all Member States**.
- 1a. **The competent authority of a Member State where the hosting service provider does not have its main establishment or does not have a legal representative may request access to be disabled to terrorist content and enforce this request within its own territory.**
- 1b. **If the relevant competent authority has not previously issued a removal order to a hosting service provider it shall contact the hosting service provider, providing information on procedures and applicable deadlines, at least 12 hours before issuing a removal order.**
2. Hosting service providers shall remove terrorist content or disable access to it **as soon as possible and** ~~within one hour from~~ **after the** receipt of the removal order.
3. Removal orders shall contain the following elements in accordance with the template set out in Annex I:
 - (a) identification of the competent authority **via an electronic signature** 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 **and a specific (401)** ~~at least~~, reference to the categories of terrorist content listed in Article 2(5);
 - (c) **an exact** Uniform Resource Locator (URL) and, where necessary, additional information enabling the identification of the content referred;
 - (d) a reference to this Regulation as the legal basis for the removal order;
 - (e) date and time stamp of issuing;
 - (f) **easily understandable** information about redress available to the hosting service provider and to the content provider, **including redress with the competent authority as well as recourse to a court as well as deadlines for appeal**;
 - (g) where ~~relevant~~ **necessary and proportionate**, the decision not to disclose information about the removal of terrorist content or the disabling of access to it referred to in Article 11.
4. ~~Upon request by the hosting service provider or by the content provider, the competent authority shall provide a detailed statement of reasons, without prejudice to the obligation of the hosting service provider to comply with the removal order within the deadline set out in paragraph 2.~~
5. The competent authorityies 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 (426)~~, 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, **including for technical or operational reasons**, it shall inform, without undue delay, the competent authority, explaining the reasons, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the reasons invoked are no longer present.
8. ~~If the hosting service provider may refuse to execute the removal order if cannot comply with the removal order because the removal order contains manifest errors or does not contain sufficient information to execute the order.~~ It shall inform the competent authority without undue delay, asking for the necessary clarification, using the template set out in Annex III. The deadline set out in paragraph 2 shall apply as soon as the clarification is provided.
9. The competent authority which issued the removal order shall inform the competent authority which oversees the implementation of **specific** ~~proactive~~ measures, referred to in Article 17(1)(c) when the removal order becomes final. A removal order 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 4a (new)

Consultation procedure for removal orders

3. ***The competent authority which issues a removal order under article 4(1a) shall submit a copy of the removal order to the competent authority referred to in Article 17(1)(a) in which the main establishment of the hosting service provider is located at the same time it is transmitted to the hosting service provider in accordance with Article 4(5).***
4. ***In cases where the competent authority of the Member State in which the main establishment of the hosting service provider is located has reasonable grounds to believe that the removal order may impact fundamental interests of that Member State, it shall inform the issuing competent authority. The issuing authority shall take these circumstances into account and shall, where necessary, withdraw or adapt the removal order.***

Article 4b (new)

Cooperation procedure for issuing an additional removal order

4. ***Where a competent authority has issued a removal order under article 4(1a), that authority may contact the competent authority of the Member State where the hosting service provider has its main establishment in order to request that the latter competent authority also issue a removal order under Article 4(1).***

5. *The competent authority in the Member State where the main establishment of the hosting service provider is located shall either issue a removal order or refuse to issue an order as soon as possible but no later than within one hour of being contacted under paragraph 1 and shall inform the competent authority that issued the first order of its decision.*
6. *In cases where the competent authority in the Member State of main establishment needs more than one hour to make its own assessment of the content, it shall send a request to the hosting service provider concerned to disable temporarily the access to the content for up to 24 hours, during which time the competent authority shall make the assessment and send the removal order or withdraw the request to disable the access.*

Corresponding Recital to Article 4: Recitals 13 and 14

- (13) The procedure and obligations resulting from legal **removal** 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 **a judicial authority**^{ies} or a **functionally independent** administrative **or** law enforcement **authority** 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 **as soon as possible and, if possible, depending on the size and economic capacity of the hosting service provider**, 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.~~
- (14) The competent authority should transmit the removal order directly to ~~the addressee and contact~~ point of ~~contact~~ the **hosting service provider and where the hosting service provider's main establishment is in another Member State, to the competent authority of that Member state** by any electronic means capable of producing a written record under conditions that allow the service provider to establish authenticity, including the accuracy of the date and the time of sending and receipt of the order, such as by secured email and platforms or other secured channels, including those made available by the service provider, in line with the rules protecting personal data. This requirement may notably be met by the use of qualified electronic registered delivery services as provided for by Regulation (EU) 910/2014 of the European Parliament and of the Council⁸.

Corresponding Annexes :

Annex I text under title and Section A

⁸ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

Covers: AM 735 (Joly)

Ams falling: AM 736 (Joly), AM 737 (Joly), IMCO 124, IMCO 125

ANNEX I

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

Under Article 4 of Regulation (EU)...⁹ the addressee of the removal order shall remove terrorist content or disable access to it, ~~within one hour from~~ **as soon as possible after** receipt of the removal order from the competent authority.

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

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

SECTION A:

Issuing Member State:

.....

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

Addressee (legal representative)

.....

Addressee (contact point)

.....

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

.....

Time and date of issuing the removal order

.....

Reference number of the removal order:

.....

Annex I, Section B, title and paragraphs 1 and 3

Covers : AM 738

Ams falling; IMCO 126, IMCO 127, AM 744 (Joly), IMCO 128

SECTION B: Content to be removed or access to it disabled *as soon as possible* ~~within one hour~~:

9 Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (OJ L ...).

10 Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (OJ L ...).

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

(.....) Paragraph 2 covered under COMP 2 on definitions

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

Annex I, Section D

Covers:

Ams falling; 747 (Joly)

SECTION D: Informing Member State of jurisdiction

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

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

Annex I, Section E

Covers:

Ams falling: AM 748 (Joly), 749(Joly), 750 (Joly)

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

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

judge, court, or investigating judge

law enforcement authority

other competent authority → please complete also Section (F)

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

Name of authority:

.....

Name of its representative:

.....

Post held (title/grade): File No:.....

.....

Address:.....

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

.....

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

 Email:
 Date:

 Official stamp (if available) and signature¹¹:

Annex I, Section F

Covers:

Ams falling: 751 (Joly)

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

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

Annex III, Section B

Covers: AM 752 (Dati) and CULT 84

AMs falling: AM 753 (Joly)

SECTION B: Reasons for non-execution
 (i) The removal order cannot be executed or cannot be executed within the requested deadline for the following reason(s):
 force majeure or de facto impossibility not attributable to the addressee or the service provider, **including for technical or operational reasons (752, CULT 84)**
 the removal order contains manifest errors
 the removal order does not contain sufficient information
 (ii) Please provide further information as to the reasons for non-execution:

¹¹ A signature may not be necessary if sent through authenticated submission channels.

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

Compromise 5

Deletion of Article 5 and its corresponding Recital 15

Covers: AMs 450 (Sippel), 456 (Pagazaurtundúa), IMCO 65, 67, 68, 69, 71

AMs falling: AMs 444 (Weidenholzer), 445 (Schaake), 446 (Joly), 447 (Ernst), 448 (Sippel), 449 (Sippel), 451 (Sippel), 452 (Sippel), 453 (Sippel), 454 (Sippel), 455 (Sippel), IMCO 66, 70, 72

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 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.~~

Corresponding Recital to Article 5: Recital 15

~~(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, 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) 2016/794¹² remains unaffected.~~

Compromise 6

Covers: AMs 22 -24 (Rapp), 463 (Joly), 467 (Ernst), 473 (Rapp), 477 (Sippel), 478 (Joly), 479 (Schaake), 485 (Sippel), 486 (Schaake), 487 (Joly), 501 (Joly), 502 (Pagazaurtundúa), 503 (Mamikins), 504 (Lenaers), 511 (Dati), IMCO 76, 77, 78, CULT 55, 60

AMs falling: AMs 457 (Weidenholzer), 458 (Schaake), 459 (Sippel), 460 (Joly), 461 (Schaake), 462 (Sippel), 464 (Mamikins), 465 (Pagazaurtundúa), 466 (Dati), 468 (Ernst), 469 (Schaake), 470 (Schaake), 471 (Sippel), 472 (Ernst), 474 (Pagazaurtundúa), 475 (Joly), 476 (Lenaers), 480 (Gomes), 481 (Pagazaurtundúa), 482 (Bay), 483 (Lenaers), 484 (Ernst), 488 (Bay), 489 (Ernst), 490 (Schaake), 491 (Ernst), 492 (Sippel), 493 (Schaake), 494 (Sippel), 495 (Joly), 496 (Lenaers), 497 (Pagazaurtundúa), 498 (Sippel), 499 (Schaake), 500 (Ernst), 505 (Joly), 506 (Schaake), 507 (Sippel), 508 (Pagazaurtundúa), 509 (Ernst), 510 (Lenaers), 512 (Pagazaurtundúa), 513 (Pagazaurtundúa), 514 (Sippel), 515 (Schaake), 516 (Ernst), 517 (Dati), 518 (Rapp), 519 (Gomes), 520 (Joly), IMCO 73, 74, 75, 79, 80, 81, CULT 56, 57, 58, 59, 61

Article 6

Specific measures

- ~~1. ***Without prejudice to Directive (EU) 2018/1808 and Directive 2000/31/EC (CULT 55)*** Hosting service providers shall, where appropriate, ***may take specific*** measures to protect their services against the ***public*** dissemination of terrorist content. The measures shall be effective, ***targeted (22, 467)*** and proportionate, ***paying particular attention to*** taking into account the risk and level of exposure to terrorist content, the fundamental rights of the users, and the fundamental importance of the ***right to (467)*** freedom of expression and the ***freedom to receive and impart information and ideas*** in an open and democratic society.~~
- ~~2. Where it has been informed according to Article 4(9), the competent authority referred to in Article 17(1)(c) shall request the hosting service provider to submit a report, within three months after receipt of the request and thereafter at least on an~~

¹² 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).

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.

- 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, **After establishing that a hosting service provider has received a substantial number of removal orders**, the competent authority referred to in Article 17(1)(c) may send issue a decision imposing **request for necessary, proportionate and effective specific additional specific** necessary and proportionate proactive measures **that the hosting service provider will have to implement. The competent authority shall not impose a general monitoring obligation, nor the use of automated tools (24, 463).** The request shall take into account, in particular, the **technical feasibility of the measures (CULT 60), the size and** 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 **the freedom to receive and impart information and ideas in an open and democratic society.** 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 hosting service provider shall regularly report on the implementation of such measures as specified by the competent authority referred to in Article 17(1)(c).
- 5. A hosting service provider may, at any time, request the competent authority referred to in Article 17(1)(c) a review and, where appropriate, to revoke a request or decision pursuant to paragraphs 2,3, and 4 respectively. The competent authority shall provide a reasoned decision within a reasonable period of time after receiving the request by the hosting service provider.

Corresponding Recitals to Article 6: Recital 16, 17, 18 and 19

Covers: AMs 8 - 9 (Rapp), IMCO 21

AMs falling: AMs 138 (Sippel), 139 (Weidenholzer), 140 (Schaake), 141 (Pagazaurtundúa), 142 (Chinnici), 143 (Joly), 144 (Dati), 145 (Ernst), 146 (Schaake), 147 (Ernst), 148 (Bay), 149 (Joly), 150 (Weidenholzer), 151 (Pagazaurtundúa), 152 (Sippel), 153 (Weidenholzer), 154 (Ernst), 155 (Joly), 156 (Chinnici), 157 (Pagazaurtundúa), 158 (Gomes), 159 (Bay), 160 (Dati), 161 (Sippel), 162 (Weidenholzer), 163 (Schaake), 164 (Ernst), 165 (Joly), 166 (Pagazaurtundúa), 167 (Mamikins), 168 (Gomes), 169 (Dati), 170 (Ernst), IMCO 19, 20, 22, CULT 15 (AVMSD), 16, 17

- (16) Given the scale and speed necessary for effectively identifying and removing terrorist content, proportionate *specific* proactive measures, ~~including by using automated means in certain cases~~, are an essential element in tackling terrorist content online. With a view to reducing the accessibility of terrorist content on their services, hosting service providers should assess whether it is appropriate to take *specific* 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~~ **to receive and impart information, in particular where there is a substantial level of exposure to terrorist content and receipt of removal orders**. Consequently, hosting service providers should determine what appropriate, *targeted*, effective and proportionate *specific* proactive measure should be put in place. This requirement should not imply a general monitoring obligation. **Those specific measures may include regular reporting to the competent authorities, increase of human resources dealing with measures to protect the services against public dissemination of terrorist content, and exchange of best practices**. In the context of this assessment, the absence of removal orders ~~and referrals~~ addressed to a hosting provider, is an indication of a low level of exposure to terrorist content.
- (17) When putting in place *specific* proactive measures, hosting service providers should ensure that users' right to freedom of expression and *freedom to* ~~including to freely receive and impart information and ideas in an open and democratic society~~ is preserved. In addition to any requirement laid down in the law, including the legislation on protection of personal data, hosting service providers should act with due diligence and implement safeguards, including notably human oversight and verifications, ~~where appropriate~~, to avoid any unintended and erroneous decision leading to removal of content that is not terrorist content. ~~This is of particular relevance when hosting service providers use automated means to detect terrorist content. Any decision to use automated means, whether taken by the hosting service provider itself or pursuant to a request by the competent authority, should be assessed with regard to the reliability of the underlying technology and the ensuing impact on fundamental rights.~~
- (18) In order to ensure that hosting service providers exposed to terrorist content take appropriate measures to prevent the misuse of their services, the competent *authorities* should request hosting service providers having received a **substantial number of final** removal orders, ~~which has become final~~, to report on the *specific* 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 **necessary**,⁽¹⁸⁾ 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 (18)** and proportionality of the measures, competent authorities should take into account relevant parameters including the number of removal orders ~~and referrals~~ issued to the provider, their **size and** economic capacity and the impact of its service in disseminating terrorist content (for example, taking into account the number of users in the Union), **as well as the safeguards put in place to protect the freedom of expression and information and the number of incidents of restrictions on legal content.**⁽¹⁸⁾

- (19) Following the request, the competent authority should enter into a dialogue with the hosting service provider about the necessary *specific* proactive measures to be put in place. If necessary, the competent authority should **request the hosting provider to re-evaluate the measures needed or impose request** the adoption of appropriate, effective and proportionate *specific* proactive measures where it considers that the measures taken **do not respect the principles of necessity and proportionality or** are insufficient to meet the risks. **The competent authority should only request specific measures that the hosting service provider can reasonably be expected to implement, taking into account, among other factors, the hosting service provider's financial and other resources.**⁽¹⁹⁾ A request to implement 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 public dissemination of terrorist content, the decisions adopted by the competent authorities on the basis of this Regulation could, in exceptional circumstances, (19) 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 the freedom to receive and impart information and ideas in an open and democratic society and the freedom to conduct a business, and provide appropriate justification.~~

Compromise 7

Covers: AMs 526 (Weidenholzer), 527 (Pagazaurtundua), 535 (Joly), 536 (Weidenholzer), 537 (Gomes), 538 (Pagazaurtundua), 539 (Sippel), IMCO 84

AMs falling: AMs 521(Ernst), 522 (Pagazaurtundua), 523 (Joly), 524 (Weidenholzer), 525 (Sippel), 528 (Ernst), 529 (Weidenholzer), 530 (Ernst), 531 (Ernst), 532 (Gomes), 533 (Joly), 534 (Joly), 540 (Lenaers), 541 (Weidenholzer), 542 (Weidenholzer), 543 (Joly), IMCO 82, 83

Article 7

Preservation of content and related data

1. Hosting service providers shall preserve terrorist content which has been removed or disabled as a result of a removal order, ~~a referral~~ or as a result of *specific* proactive

measures pursuant to 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, **or remedy** (526, 527),

(b) the prevention, detection, investigation and prosecution **by law enforcement authorities** of terrorist offences.

2. The terrorist content and related data referred to in paragraph 1 (a) shall be preserved for six months **and deleted after this period.** (535, 537, 536, 538, 539.) The terrorist content shall, upon request from the competent authority or court, be preserved for a **further specified** longer period **only if, when** and for as long as necessary for ongoing proceedings of administrative, or judicial review **or remedies** referred to in paragraph 1(a). **Hosting service providers shall preserve the terrorist content and related data referred to in paragraph 1(b) until the law enforcement authority reacts to the notification made by the hosting service provider in accordance with Article 13(4) but no later than six months**

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.

Corresponding recitals to Article 7: Recital 20, 21, 22 and 23

Covers:

AMs falling: AMs 170 (Ernst), 171 (Sippel), 172 (Weidenholzer), IMCO 24

(20) The obligation on hosting service providers to preserve removed content and related data, should be laid down for specific purposes and limited in time to what is necessary. There is need to extend the preservation requirement to related data to the extent that any such data would otherwise be lost as a consequence of the removal of the content in question. Related data can include data such as ‘subscriber data’, ~~including~~ in particular data pertaining to the identity of the content provider as well as ‘access data’, including for instance data about the date and time of use by the content provider, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the content provider.

Covers:

AMs falling: AMs 173 (Weidenholzer), 174 (Ernst), 175 (Schaake), 176 (Joly)

- (21) The obligation to preserve the content for proceedings of administrative, ~~or~~ judicial review **or remedy** is necessary and justified in view of ensuring the effective measures of redress for the content provider whose content was removed or access to it disabled as well as for ensuring the reinstatement of that content as it was prior to its removal depending on the outcome of the review procedure. The obligation to preserve content for investigative and prosecutorial purposes is justified and necessary in view of the value this material could bring for the purpose of disrupting or preventing terrorist activity. Where companies remove material or disable access to it, ~~in particular through their own proactive~~ **specific** measures, **they should inform the competent law enforcement authorities promptly without undue delay** and do not inform the relevant authority because they assess that it does not fall in the scope of Article 13(4) of this Regulation, law enforcement may be unaware of the existence of the content. ~~Therefore,~~ The preservation of content for purposes of prevention, detection, investigation and prosecution of terrorist offences is also justified. For these purposes, **the terrorist content and the related data should be stored only for a specific period allowing the law enforcement authorities to check the content and decide whether it would be needed for those specific purposes. This period should not exceed six months. For the purposes of prevention, detection, investigation and prosecution of terrorist offences,** the required preservation of data is limited to data that is likely to have a link with terrorist offences, and can therefore contribute to prosecuting terrorist offences or to preventing serious risks to public security.

Covers:

AMs falling: Ams 177 (Weidenholzer), 177 (Lenaers), 179 (Ernst), 180 (Joly), 181 (Gomes), 182 (Pagazaurtundua)

- (22) To ensure proportionality, the period of preservation should be limited to six months to allow the content providers sufficient time to initiate the review process ~~and~~ **or** to enable law enforcement **authorities'** access to relevant data for the investigation and prosecution of terrorist offences. However, this period may be prolonged for the period that is necessary in case the review **or remedy** proceedings are initiated but not finalised within the six months period upon request by the authority carrying out the review. This duration should **also** be sufficient to allow law enforcement authorities to preserve the necessary **evidence material** in relation to investigations **and prosecutions**, while ensuring the balance with the fundamental rights concerned.

Covers:

AMs falling: AMs 183 (Gomes), 184 (Pagazaurtundua)

- (23) This Regulation does not affect the procedural guarantees and procedural investigation measures related to the access to content and related data preserved for the purposes of the investigation and prosecution of terrorist offences, as regulated under the national law of the Member States, and under Union legislation.

Compromise 8

Covers: AMs 550 (Joly), 554 (Schaake), 556 (Ernst), 565 (Joly), 566 (Weidenholzer), 567 (Sippel), 564 (Joly), 568 (Ernst), 569 (Ernst), 571 (Joly), 26 (Rapp), 27 (Rapp), IMCO 86, 91, CULT 63, 64, 65, 67

AMs falling: AMs 25 (Rapp), 544 (Joly), 545 (Weidenholzer), 546 (Joly), 547 (Ernst), 548 (Mamikins), 549 (Pagazaurtundua), 551 (Weidenholzer), 552 (Mamikins), 553 (Pagazaurtundua), 555 (Weidenholzer), 557 (Pagazaurtundua), 558 (Joly), 559 (Weidenholzer), 560 (Weidenholzer), 561 (Joly), 562 (Ernst), 563 (Ernst), 564 (Joly), IMCO 85, 87, 88, 89, 90, 92, CULT 66

Article 8

Transparency obligations for hosting service providers

1. **Where applicable**, hosting service providers shall set out **clearly** in their terms and conditions their policy to prevent the dissemination of terrorist content, including, where **applicable** appropriate, a meaningful explanation of the functioning of **specific** proactive measures including the use of automated tools.
2. Hosting service providers **which are or have been subject to removal orders in that year (26, 550, 551)**, shall **make publicly available** publish annual transparency reports on action taken against the dissemination of terrorist content.
3. Transparency reports shall include at least the following information:
 - (a) information about the hosting service provider's measures in relation to the detection, identification and removal of terrorist content;
 - (b) information about the hosting service provider's measures to 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, **in particular where automated technology has been used (556)**;
 - (c) number of pieces of terrorist content removed or to which access has been disabled, following removal orders, referrals, or **specific** proactive measures, respectively, **and the number of orders where the content has not been removed in accordance with Article 4(7) and (8) together with reasons for refusal.(565)**.
 - (d) **number overview** and outcome of complaint procedures **and actions for judicial review, including the number of cases in which it was established that content was wrongly identified as terrorist content (27, 566, 567, 564, 568, 569)**.

Article 8a

Transparency obligations for competent authorities

1. **Competent authorities shall publish annual transparency reports that shall include at least the following information:**
 - (a) **number of removal orders issued, the number of removals and the number of refused or ignored removal orders;**
 - (b) **number of identified terrorist content which led to investigation and prosecution and the number of cases of content wrongly identified as terrorist;**

(c) a description of measures requested by the competent authorities pursuant to Article 6 (4).

Corresponding recital to Article 8: Recital 24

Covers: AMs 10 (Rapp), 185 (Pagazaurtundua), 188 (Joly)

AMs falling: AMs 186 (Dati), 187 (Bay), 189 (Weidenholzer), IMCO 25

(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. **Only** hosting service providers **which are subject to removal orders for that year** should **be obliged to** publish annual transparency reports containing meaningful information about action taken in relation to the detection, identification and removal of terrorist content.

(24a) **The authorities competent to issue removal order should also publish transparency reports containing information on the number of removal orders, the number of refusals, the number of identified terrorist content which led to investigation and prosecution of terrorist offences and the number of cases of content wrongly identified as terrorist (10, 185, 188).**

Compromise 9

Covers: AMs 28 (Rapp), 585 (Joly), IMCO 96, CULT 68, 69

AMs falling: AMs 572 (Joly), 573 (Sippel), 574 (Weidenholzer), 575 (Joly), 576 (Weidenholzer), 577 (Bay), 578 (Ernst), 579 (Sippel), 581 (Ernst), 582 (Sippel), 583 (Joly), 584 (Weidenholzer), 586 (Weidenholzer), IMCO 94, 95,

Article 9

*Safeguards regarding the use and implementation of **specific proactive** measures*

1. Where hosting service providers use automated tools pursuant to this Regulation in respect of content that they store, they shall provide effective and appropriate safeguards to ensure that decisions taken concerning that content, in particular decisions to remove or disable **access to** content considered to be terrorist content, are accurate and well-founded.
2. Safeguards shall consist, in particular, of human oversight and verifications ~~where appropriate and, in any event,~~ **of the appropriateness of the decision to remove or deny access to content, in particular with regard to the right to freedom of expression and freedom to receive and impart information and ideas in an open and democratic society.** ~~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.~~

Compromise 10

Covers: AMs 3, 88, 585, IMCO 11, IMCO 97

ARTICLE 9A
EFFECTIVE REMEDIES

1. **Content providers, whose content has been removed or access to which has been disabled following a removal order, and hosting service providers that have received a removal order, shall have a right to an effective remedy. Member States shall put in place effective procedures for exercising this right (585, IMCO 97).**

Corresponding recital to Article 9a: Recital 8

- (8) The right to an effective remedy is enshrined in Article 19 TEU and Article 47 of the Charter of Fundamental Rights of the European Union. Each natural or legal person has the right to an effective judicial remedy before the competent national court against any of the measures taken pursuant to this Regulation, which can adversely affect the rights of that person. The right includes, in particular the possibility for hosting service providers and content providers to effectively contest the removal orders before the court of the Member State whose authorities issued the removal order **and the possibilities for content providers to contest the specific measures taken by the hosting provider (3, 88, IMCO 11).**

Compromise 11

Covers: AMs 29 (Rapp), 592 (Joly), 593 (Sippel), 594 (Weidenholzer)

AMs Falling: AMs 30 (Rapp), 587 (Joly), 588 (Sippel), 589 (Weidenholzer), 590 (Ernst), 591 (Schaake), 595 (Ernst), 596 (Sippel), 597 (Joly), 598 (Pagazaurtundúa), 599 (Weidenholzer), IMCO 98, 99

Article 10
Complaint mechanisms

1. Hosting service providers shall establish **an** 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 **specific** proactive measures pursuant to Article 6, to submit a complaint against the action of the hosting service provider requesting reinstatement of the content.
2. Hosting service providers shall promptly examine every complaint that they receive and reinstate the content without undue delay where the removal or disabling of access was unjustified. They shall inform the complainant about the outcome of the examination **within two weeks of the receipt of the complaint (29) with an explanation in cases where the hosting service provider decides not to reinstate the content. A reinstatement of content shall not preclude further judicial measures against the decision of the hosting service provider or of the competent authority. (592, 593, 594).**

Corresponding Recital to Article 10: Recital 25

Covers: AMs 11 (Rapp), 191 (Joly), 192 (Ernst), 193 (Boni), 194 (Weidenholzer)

AMS falling: CULT 19, IMCO 27

- (25) Complaint procedures constitute a necessary safeguard against erroneous removal of content protected under the freedom of expression and ***freedom to receive and impart (194) information and ideas in an open and democratic society***. 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.

Compromise 12

Covers: AMs 31 (Rapp), 600 (Joly), 601 (Weidenholzer), 602 (Weidenholzer), 603 (Joly), 607 (Weidenholzer), 608 (Joly), IMCO 100, 101, 102

AMs Falling: AMs 604 (Gomes), 605 (Pagazaurtundúa), 606 (Ernst), 609 (Ernst), 610 (Ernst)

Article 11

Information to content providers

1. Where hosting service providers removed (600) terrorist content or disable access to it, they shall make available to the content provider ***comprehensive and concise*** information on the removal or disabling of access to terrorist content ***and the possibilities to contest the decision, and shall provide him or her with a copy of the removal order issued in accordance with Article 4 upon request.***
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. (602, 603)~~
3. The obligation pursuant to paragraphs 1 ~~and 2~~ (607) shall not apply where the competent authority decides ***based on objective evidence and considering the proportionality and necessity of such decision***, that there should be no disclosure for reasons of public security, such as the prevention, investigation, detection and prosecution of terrorist offences, for as long as necessary, but not exceeding four weeks (608) 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.

Corresponding Recital to Article 11: Recital 26

Covers: AMs 12 (Rapp), 195 (Joly), CULT 20

AMs Falling: AMs 196 (Ernst), 198 (Gomes), 197 (Weidenholzer), 199 (Pagazaurtundúa), IMCO 28

- (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 **such as the reasons for the removal or disabling of access, the legal basis for the action** 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.~~ (195) 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.

Corresponding Annex:

Annex I, section C

Covers:

Ams falling: 745 (Joly), 746(Joly)

SECTION C: Information to content provider

Please note that (tick, if applicable):

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

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

Compromise 13

Covers: AMs 616 (Dati), 619 (Dati), 622 (Sippel), 624 (Voss), Sippel (625), 626 (Dati), 634 (Ernst), 635 (Voss)

AMS falling: AMs 615 (Weidenholzer), 617 (Weidenholzer), 618 (Ernst), 620 (Joly), 621 (Weidenholzer), 623 (Maite), 627 (Joly), 628 (Joly), 629 (Sippel), 630 (Weidenholzer), 631 (Weidenholzer). 632 (Ernst), 633 (Sippel), 636 (Weidenholzer), IMCO 103, CULT 73

Article 13

Cooperation between hosting service providers, competent authorities and where appropriate ~~relevant~~ **competent** Union bodies

1. Competent authorities in Member States shall inform, coordinate and cooperate with each other and, where appropriate, with ~~relevant Union bodies such as~~ Europol with regard to removal orders ~~and referrals~~ to avoid duplication, enhance coordination and avoid interference with investigations in different Member States.
2. Competent authorities in Member States shall inform, coordinate and cooperate with the competent authority referred to in Article 17(1)(c) and (d) with regard to measures taken pursuant to Article 6 and enforcement actions pursuant to Article 18. Member States shall make sure that the competent authority referred to in Article 17(1)(c) and (d) is in possession of all the relevant information. For that purpose, Member States shall provide for the appropriate **and secure (622)** communication channels or mechanisms to ensure that the relevant information is shared in a timely manner.
3. Member States ~~and hosting service providers may~~ **may choose to (624, 625)** make use of dedicated tools, including, ~~where appropriate,~~ those established by ~~relevant competent~~ **competent** Union bodies such as Europol, to facilitate in particular:
 - (a) the processing and feedback relating to removal orders pursuant to Article 4;
 - ~~(c) the processing and feedback relating to referrals pursuant to Article 5;~~
 - (h) co-operation with a view to identify and implement **specific** proactive measures pursuant to Article 6.
4. Where hosting service providers become aware of ~~any evidence of~~ terrorist **content (634)** offences, they shall promptly inform authorities competent for the investigation and prosecution in criminal offences in the concerned Member State ~~or~~ **Where it is impossible to identify the Member State concerned, the hosting service provider shall notify (635)** the point of contact in the Member State pursuant to Article 17(2), where they have their main establishment or a legal representative **and also** ~~Hosting service providers may, in case of doubt,~~ transmit this information to Europol for appropriate follow up.

4a. Hosting service providers shall cooperate with competent authorities ~~or Europol when requested.~~

Corresponding recital to Article 13: Recital 27

- (27) In order to avoid duplication and possible interferences with investigations **and to minimise the expenses of the affected service providers**, the competent authorities should inform, coordinate and cooperate with each other and where appropriate with Europol when issuing removal orders ~~or sending referrals~~ to hosting service providers. In implementing the provisions of this Regulation, Europol could provide support in line with its current mandate and existing legal framework.
- (27a) **Referrals by 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 with its own terms and conditions, should remain available in addition to removal orders. For**

that reason it is important that hosting service providers cooperate with Europol and assess Europol's 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, Europol's mandate as laid down in Regulation (EU) 2016/794¹³ remains unaffected.

Compromise 14

Covers: AMs 637 (Dati), 638 (Joly)

AMS falling: AMs 639 (Weidenholzer), 640 (Ernst), 641 (Ernst), 642 (Weidenholzer), 643 (Joly), 644 (Weidenholzer), 645 (Joly), 646 (Ernst)

Article 14

Points of contact

1. Hosting service providers ***previously in receipt of one or more removal orders*** shall establish a point of contact allowing for the receipt of removal orders ~~and referrals~~ by electronic means and ensure their ~~swift~~ ***expeditious (638)*** processing pursuant to Articles 4 ~~and 5~~. They shall ensure that this information is made publicly available.
2. The information referred to in paragraph 1 shall specify the official language or languages (s) of the Union, as referred to in Regulation 1/58, in which the contact point can be addressed and in which further exchanges in relation to removal orders ~~and referrals~~ pursuant to Articles 4 ~~and 5~~ shall take place. This shall include at least one of the official languages of the Member State in which the hosting service provider has its main establishment or where its legal representative pursuant to Article 16 resides or is established.
3. ~~Member States shall establish a point of contact to handle requests for clarification and feedback in relation to removal orders and referrals issued by them. Information about the contact point shall be made publicly available.~~

Corresponding recital to Article 14: Recital 33

- (33) Both hosting service providers and Member States should establish points of contact to facilitate the ~~swift~~ ***expeditious*** handling of removal orders ~~and referrals~~. In contrast to the legal representative, the point of contact serves operational purposes. The hosting service provider's point of contact should consist of any dedicated means allowing for the electronic submission of removal orders ~~and referrals~~ and of technical and personal means allowing for the ~~swift~~ ***expeditious*** processing thereof. The point of contact for the hosting service provider does not have to be located in the Union and the hosting service provider is free to nominate an existing point of contact, provided that this point of contact is able to fulfil the functions provided for in this Regulation. With a view to ensure that terrorist content is removed or access to it is disabled within one

13 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).

hour from the receipt of a removal order, hosting service providers should ensure that the point of contact is reachable 24/7. The information on the point of contact should include information about the language in which the point of contact can be addressed. In order to facilitate the communication between the hosting service providers and the competent authorities, hosting service providers are encouraged to allow for communication in one of the official languages of the Union in which their terms and conditions are available.

Compromise 15

Covers: AMs 34 (Rapp), 650 (Joly), 656 (Joly)

AMs Falling: AMs 651 (Weidenholzer), 652 (Pagazaurtundúa), 653 (Joly), 654 (Sippel), 655 (Ernst)

Article 15 Jurisdiction

1. The Member State in which the main establishment of the hosting service provider is located shall have the jurisdiction for the purposes of Articles 6, 18, and 21. A hosting service provider which does not have its main establishment within one of the Member States shall be deemed to be under the jurisdiction of the Member State where the legal representative referred to in Article 16 resides or is established.
2. Where a hosting service provider ***which does not have its main establishment within one of the Member States (650)*** fails to designate a legal representative, all Member States shall have jurisdiction. ***Where a Member State decides to exercise this jurisdiction, it shall inform all other Member States.***
3. ~~Where an authority of another Member State has issued a removal order according to Article 4(1), that Member State has jurisdiction to take coercive measures according to its national law in order to enforce the removal order.~~

Corresponding Recital to Article 15: Recital 34

Covers: AM 226 (Pagazaurtundúa),

AMs Falling: AMs 224 (Ernst), 225 (Weidenholzer), 227 (Joly), IMCO 31, CULT 23

- (34) In the absence of a general requirement for service providers to ensure a physical presence within the territory of the Union, there is a need to ensure clarity under which Member State's jurisdiction the hosting service provider offering services within the Union falls. As a general rule, the hosting service provider falls under the jurisdiction of the Member State in which it has its main establishment or in which it has designated a legal representative. ~~Nevertheless, where another Member State issues a removal order, its authorities should be able to enforce their orders by taking coercive measures of a non-punitive nature, such as penalty payments.~~(226) With regards to a hosting service provider which has no establishment in the Union and does not designate a legal representative, any Member State should, nevertheless, be able to issue penalties, provided that the principle of *ne bis in idem* is respected.

Compromise 16

Covers: AMs 33 (Rapp), 663 (Ernst), 664 (Schaake), 666 (Pagazaurtundúa), 669 (Boni), 678 (Dati), IMCO 105

AMs Falling: AMs 665 (Sippel), 667 (Joly), 668 (Weidenholzer), 670 (Joly), 671 (Weidenholzer), 672 (Ernst), 673, 674 (Sippel), 675 (Weidenholzer), 676 (Pagazaurtundúa), 677 (Joly), IMCO 106, 107, 108, 109

Article 17

Designation of competent authorities

1. Each Member State shall designate **a judicial or a functionally independent administrative (33, 663, 664, 666, 669)** authority competent to
 - (a) issue removal orders pursuant to Article 4;
 - (b) ~~detect, identify and refer terrorist content to hosting service providers pursuant to Article 5;~~
 - (c) oversee the implementation of **specific** ~~proactive~~ measures pursuant to Article 6;
 - (d) enforce the obligations under this Regulation through penalties pursuant to Article 18.
- 1a. **Member States shall designate a point of contact within the competent authorities to handle requests for clarification and feedback in relation to removal orders issued by them. Information on the contact point shall be made publicly available.**
2. By [six months after the entry into force of this Regulation] at the latest Member States shall notify the Commission of the competent authorities referred to in paragraph 1. The Commission shall **set up an online register listing all those competent authorities and the designated contact point for each competent authority. The Commission shall (678)** publish the notification and any modifications of it in the *Official Journal of the European Union*.

Corresponding Recitals to Article 17: Recital 37

Covers: AMs 229 (Weidenholzer), 230 (Boni), 232 (Pagazaurtundúa), 234 (Dati), IMCO 33

AMs Falling: AMs 231 (Ernst), 233 (Joly)

- (37) For the purposes of this Regulation, Member States should designate **a single competent judicial or functionally independent administrative** authorities. **This**

requirement to designate ~~an administrative or judicial~~ competent authorities does not **necessitate** necessarily require the establishment of **a** new authorities but can be **an** existing bodies tasked with the functions set out in this Regulation. This Regulation requires designating **an** authorities competent for issuing removal orders, referrals and for overseeing **specific** proactive measures and for imposing penalties. It is for Member States to decide how many authorities they wish to designate for these tasks. (229) **Member States should communicate the competent authority designated under this Regulation to the Commission, which should publish online a compilation of the competent authority of each Member State. The online registry should be easily accessible to facilitate the swift verification of the authenticity of removal orders by the hosting service providers (234)**

Compromise 17

Covers: AM 681 (Rapp), IMCO110, 112, 118, CULT 76,

AMs falling: AMs 683 (Weidenholzer), 684 (Ernst), 685 (Weidenholzer), 686 (Joly), 687 (Ernst), 688 (Sippel), 689 (Weidenholzer), 690 (Pagazaartundua), 691 (Sippel), 692 (Joly), 693 (Ernst), 694 (Ernst), 695 (Joly), 696 (Ernst), 697 (Weidenholzer), 698 (Weidenholzer), 699 (Weidenholzer), 700 (Ernst), 701 (Ernst), 702 (Ernst), 703 (Joly), 704 (Lenars), 705 (Voss), 706 (Boni), 707 (Joly), 708 (Dati), 709 (Voss), 710 (Voss), 711 (Dati), 712 (Ernst), 713 (Joly), 714 (Dati), 715 (Joly) , IMCO 111, 113, 114, 115, 116, 117, 119, CULT 74, 75, 77, 78, 79, 80

Article 18 Penalties

1. Member States shall lay down the rules on penalties applicable to **systematic and persistent (681, 682, IMCO 110)** breaches of the obligations by hosting service providers under this Regulation and shall take all necessary measures to ensure that they are implemented. Such penalties shall be limited to infringement of the obligations pursuant to:
 - (a) ~~Article 3(2) (hosting service providers' terms and conditions);~~
 - (i) Article 4(2) and (6) (implementation of and feedback on removal orders);
 - (j) ~~Article 5(5) and (6) (assessment of and feedback on referrals);~~
 - (k) Article ~~6(2) and (4)~~ (reports on **specific** proactive measures and the adoption of measures following a decision imposing specific **specific** proactive measures);
 - (l) Article 7 (preservation of data);
 - (m) Article 8 (transparency **for hosting service providers**) ~~and 8a (transparency for competent authorities);~~
 - (n) Article 9 (safeguards ~~in relation with regard to the implementation of (CULT 76)~~ **to specific** proactive measures);
 - (o) Article 10 (complaint procedures);
 - (p) Article 11 (information to content providers);

- (q) Article 13 (4) (information on evidence of terrorist offences *content*);
 - (r) Article 14 (1) (points of contact);
 - (s) Article 16 (designation of a legal representative).
2. The penalties provided for *pursuant to paragraph 1* 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;
 - d) the financial strength of the legal person held liable;
 - e) the level of cooperation of the hosting service provider with the competent authorities;-
 - f) *the nature and size of the hosting service providers, in particular for microenterprises or small-sized enterprises within the meaning of Commission recommendation 2003/361/EC.*
 4. Member States shall ensure that a systematic *and persistent* failure to comply with obligations pursuant to Article 4(2) is subject to financial penalties of up to 4% of the hosting service provider's global turnover of the last business year.

Corresponding Recitals to Article 18: Recital 38

Covers: AMs 13 (Rapp), 236 (Voss), 241 (Corazza Bildt),

AMs Falling: AMs 235 (Ernst), 238 (Pagazaurtundúa), 239 (Weidenholzer), 240 (Schaake), 242 (Bay), 243 (Grapini), 244 (Joly), 245 (Ernst), 243 (Boni) 237 (Dati), IMCO 34, CULT 24

- (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~~ *should* be ascertained in the event that the hosting service providers systematically *and persistently* fails to *comply with their obligations under this Regulation* ~~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, this 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~~ *requesting the implementation of* additional *specific* ~~proactive~~ measures pursuant to Article 6(4). When determining whether or not

financial penalties should be imposed, due account should be taken of the financial resources of the provider. **Moreover, the competent authority should take into account whether the hosting service provider is a start-up or a small and medium sized business and should determine on a case-by-case basis if it had the ability to adequately comply with the issued order.** (236) Member States shall ~~shall~~ **should** ensure that penalties do not encourage the removal of content which is not terrorist content.

Compromise 18

Covers: AM 716 (Joly), CULT 81

AMs Falling: AM 715 (Joly)

Article 19

Technical requirements and amendments to the templates for removal orders

1. The Commission shall be empowered to adopt delegated acts in accordance with Article 20 in order to supplement this Regulation with **the necessary** technical requirements for the electronic means to be used by competent authorities for the transmission of removal orders.
2. The Commission shall be empowered to adopt such delegated acts to amend Annexes I, II and III in order to effectively address a possible need for improvements regarding the content of removal order forms and of forms to be used to provide information on the impossibility to execute the removal order.

Corresponding Recitals to Article 19: Recital 39 and 40

Covers:

AM falling: AM 247 (Joly), IMCO 35

- (39) The use of standardised templates facilitates cooperation and the exchange of information between competent authorities and service providers, allowing them to communicate more quickly and effectively. It is particularly important to ensure swift action following the receipt of a removal order. Templates reduce translation costs and contribute to a high quality standard. Response forms similarly should allow for a standardised exchange of information, and this will be particularly important where service providers are unable to comply. Authenticated submission channels can guarantee the authenticity of the removal order, including the accuracy of the date and the time of sending and receipt of the order.
- (40) In order to allow for a swift amendment, where necessary, of the content of the templates to be used for the purposes of this Regulation the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to amend Annexes I, II and III of this Regulation. In order to be able to take into account the development of technology and of the related legal framework, the Commission should also be empowered to adopt delegated acts to supplement this Regulation with technical requirements for the

electronic means to be used by competent authorities for the transmission of removal orders. It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level, and that those consultations are conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making¹⁴. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

Compromise 19

Covers: AMs 717 (Joly), 720 (Weidenholzer), 723 (Joly), IMCO 121,

AMs Falling: AMs 718 (Weidenholzer), 719, 721, 724 (Ernst), 722, 725 (Joly), IMCO 120, 121, CULT 82

Article 21 Monitoring

1. Member States shall collect from their competent authorities and the hosting service providers under their jurisdiction and send to the Commission every year by [31 March] information about the actions they have taken in accordance with this Regulation. That information shall include:
 - (a) information about the number of removal orders ~~and referrals~~ issued, the number of pieces of terrorist content which has been removed or access to it disabled, including the corresponding timeframes pursuant to Articles 4 ~~and~~ 5, ***and information on the number of corresponding cases of successful detection, investigation and prosecution of terrorist offences;(717, 720)***
 - (b) information about the specific ~~proactive~~ measures taken pursuant to Article 6, including the amount of terrorist content which has been removed or access to it disabled and the corresponding timeframes;
 - (ba) information about the number of access requests issued by competent authorities regarding content preserved by hosting service providers pursuant to Article 7; (723)***
 - (c) information about the number of complaint procedures initiated and actions taken by the hosting service providers pursuant to Article 10;
 - (d) information about the number of redress procedures initiated and decisions taken by the competent authority in accordance with national law.
2. By [*one year from the date of application of this Regulation*] at the latest, the Commission shall establish a detailed programme for monitoring the outputs, results and impacts of this Regulation. The monitoring programme shall set out the indicators and the means by which and the intervals at which the data and other necessary evidence is to be collected. It shall specify the actions to be taken by the Commission and by the Member States in collecting and analysing the data and other evidence to monitor the progress and evaluate this Regulation pursuant to Article 23.

Corresponding Recitals to Article 21: Recital 41

14 OJ L 123, 12.5.2016, p. 1.

Covers: AM 248 (Joly), IMCO 36

- (41) Member States should collect information on the implementation of the legislation ***including information on the number of cases of successful detection, investigation and prosecution of terrorist offences as a consequence of this Regulation.***(248) A detailed programme for monitoring the outputs, results and impacts of this Regulation should be established in order to inform an evaluation of the legislation.

Compromise 20

Covers: AMs 35 (Rapp), 727 (Weidenholzer), 728 (Joly), 729 (Boni), 730 (Pagazaurtundúa), 731 (Sippel), IMCO 122

AMs Falling: AMs 726 (Dati)

Article 23 Evaluation

~~No sooner than [three~~ ***One*** years from the date of application of this Regulation}, the Commission shall carry out an evaluation of this Regulation and submit a report to the European Parliament and to the Council on the application of this Regulation including the functioning ***and*** the effectiveness of the safeguard mechanisms, as well as the impact on Fundamental Rights, ***in particular freedom of expression, freedom to receive and impart information and the right to respect for one's private life.*** (35) 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.

Corresponding Recitals to Article 23: Recital 42 and 43

Covers: AMs 249 (Joly), IMCO 37

AMs falling: AMs 250 (Weidenholzer), 251 (Bay), 252 (Joly), 253 (Weidenholzer)

- (42) Based on the findings and conclusions in the implementation report and the outcome of the monitoring exercise, the Commission should carry out an evaluation of this Regulation ~~no sooner than three~~ one years after its entry into force. The evaluation should be based on the ~~five~~ criteria of efficiency, ***necessity, proportionality***, effectiveness, relevance, coherence and EU added value. It ~~will~~ ***should*** assess the functioning of the different operational and technical measures foreseen under the Regulation, including the effectiveness of measures to enhance the detection, identification and removal of terrorist content, the effectiveness of safeguard mechanisms as well as the impacts on potentially affected ***fundamental*** rights, ***including the freedom of expression and freedom to receive and impart information, the freedom and pluralism of the media, the freedom to conduct a business and the rights to privacy and the protection of personal data.*** (249. ***The Commission should also assess the impact on potentially affected*** ~~and~~ interests of third parties, including a review of the requirement to inform content providers.

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