Съвет на
Европейския съюз

Брюксел, 7 декември 2018 г.
(OR. en)

15336/18

Междуинституционално досие:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	6 декември 2018 г.
До:	Делегациите
№ предх. док.:	14978/18 + COR 1
№ док. Ком.:	12129/18 + ADD 1-3
Относно:	Предложение за регламент на Европейския парламент и на Съвета за предотвратяване на разпространението на терористично съдържание онлайн — общ подход

На заседанието си от 6 декември 2018 г. Съветът постигна съгласие по общ подход, изложен в приложението.

Промените спрямо предложението на Комисията са обозначени по следния начин: добавеният текст е отбелязан с ***получер курсив***, а заличеният текст — с квадратни скоби […].

ПРИЛОЖЕНИЕ

[…]

[…] ***Проект за***

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за предотвратяване на разпространението на терористично съдържание онлайн

[…]

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет[1],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Настоящият регламент има за цел да гарантира безпрепятственото функциониране на цифровия единен пазар в едно отворено и демократично общество, като се предотвратява злоупотребата с хостинг услуги за терористични цели. Функционирането на цифровия единен пазар следва да бъде подобрено чрез засилване на правната сигурност за доставчиците на хостинг услуги, укрепване на доверието на ползвателите в онлайн средата и засилване на гаранциите за свободата на изразяване на мнение и свободата на информация.

[1] ОВ С , , стр.

(2) Доставчиците на хостинг услуги, осъществяващи дейност чрез интернет, играят съществена роля в цифровата икономика, като свързват бизнеса и гражданите и улесняват обществения дебат и разпространението и получаването на информация, мнения и идеи, допринасяйки в значителна степен за иновациите, икономическия растеж и създаването на работни места в Съюза. В някои случаи обаче техните услуги стават обект на злоупотреби от страна на трети лица с цел извършване на незаконни дейности онлайн. Повод за особено безпокойство буди злоупотребата с доставчици на хостинг услуги от страна на терористични групи и на техните поддръжници, за да разпространяват терористично съдържание онлайн с цел отправяне на послания, радикализиране и вербуване, както и улесняване и ръководене на терористична дейност.

(3) Наличието на терористично съдържание онлайн има сериозни отрицателни последици за ползвателите, гражданите и обществото като цяло, както и за доставчиците на онлайн услуги, които хостват такова съдържание, тъй като то подкопава доверието на техните ползватели и вреди на бизнес моделите им. Като се имат предвид централната им роля и технологичните средства и способности, свързани с предлаганите от тях услуги, доставчиците на онлайн услуги носят особени обществени отговорности да защитават своите услуги срещу злоупотреба от терористи и да помагат борбата с терористичното съдържание, разпространявано чрез използването на техните услуги.

(4) Усилията на равнището на Съюза за борба с терористично съдържане онлайн, които започнаха през 2015 г. чрез рамка за доброволно сътрудничество между държавите членки и доставчиците на хостинг услуги, трябва да бъдат допълнени с ясна законодателна рамка с цел допълнително ограничаване на достъпността на терористично съдържание онлайн и адекватно справяне с бързо развиващия се проблем. Целта на тази законодателна рамка е да се използват доброволните усилия, които бяха засилени с Препоръка (ЕС) 2018/334 на Комисията[2], и да се отговори на призивите, отправени от Европейския парламент, за засилване на мерките за справяне с незаконното и вредното съдържание, както и на тези на Европейския съвет за подобряване на автоматизираното откриване и премахване на съдържание, което подбужда към терористични актове.

[2] Препоръка (ЕС) 2018/334 на Комисията от 1 март 2018 г. относно мерки за ефективна борба с незаконното съдържание онлайн (ОВ L 63, 6.3.2018 г., стр. 50)

(5) Прилагането на настоящия регламент не следва да засяга прилагането на член 14 от Директива 2000/31/ЕО[3]. По-конкретно, всички мерки, предприети от доставчика на хостинг услуги в съответствие с настоящия регламент, включително всички проактивни мерки, не следва сами по себе си да водят до това доставчикът на услуги да загуби ползата от освобождаването от отговорност, предвидено в посочената разпоредба. Настоящият регламент не засяга правомощията на националните органи и съдилищата да определят отговорността на доставчиците на хостинг услуги в конкретни случаи, когато не са изпълнени условията по член 14 от Директива 2000/31/ЕО относно освобождаването от отговорност. ***Настоящият регламент не се прилага за дейности, свързани с националната сигурност, тъй като тя остава единствено в рамките на отговорността на всяка държава членка.***

(6) В настоящия регламент са посочени правила за предотвратяване на злоупотребата с хостинг услуги с цел разпространение на терористично съдържание онлайн, чиято цел е да се гарантира безпрепятственото функциониране на вътрешния пазар при пълно зачитане на основните права, защитени в правния ред на Съюза, и по-специално тези, гарантирани в Хартата на основните права на Европейския съюз.

[3] Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар („Директива за електронната търговия“) (ОВ L 178, 17.7.2000 г., стр. 1)

(7) Настоящият регламент допринася за защитата на обществената сигурност, като същевременно установява подходящи и стабилни гаранции за защитата на основните права. Това включва правото на зачитане на личния живот и защитата на личните данни, правото на ефективна съдебна защита, правото на свобода на изразяване, включително свободата на получаване и предаване на информация, свободата на стопанска инициатива и принципа на недискриминация. Компетентните органи и доставчиците на хостинг услуги следва да приемат само мерки, които са необходими, подходящи и пропорционални в едно демократично общество, като вземат предвид особеното значение на свободата на изразяване на мнение и свободата на информация, ***както и на свободата на печата и плурализма на медиите***, които представляват […] […] фундаменти на плуралистичното и демократично общество, както и една от ценностите, на които се основава Съюзът. Мерките, представляващи намеса в свободата на изразяване на мнение и свободата на информация, следва да бъдат строго целеви, в смисъл че трябва да служат за предотвратяване на разпространението на терористично съдържание, без това да засяга правото на законно получаване и разпространяване на информация, като се взема предвид централната роля на доставчиците на хостинг услуги за способстването на обществения дебат и разпространението и получаването на факти, становища и идеи в съответствие със закона.

(8) Правото на ефективни правни средства за защита е залегнало в член 19 от ДЕС и в член 47 от Хартата на основните права на Европейския съюз. Всяко физическо или юридическо лице има право на ефективна съдебна защита пред компетентния национален съд срещу всяка мярка, предприета съгласно настоящия регламент, която може да засегне неблагоприятно правата на това лице. Правото включва, по-специално възможността доставчиците на хостинг услуги и доставчиците на съдържание да оспорват по ефективен начин заповедите за премахване пред съда на държавата членка, чиито органи са издали такава заповед, ***както и възможността доставчиците на хостинг услуги да оспорват решение за налагане на проактивни мерки или санкции пред съда на държавата членка, в която са установени или имат законен представител***.

(9) С цел да се осигури яснота относно действията, които следва да предприемат както доставчиците на хостинг услуги, така и компетентните органи за предотвратяването на разпространението на терористично съдържание онлайн, в настоящия регламент следва да се установи определение за терористично съдържание за целите на предотвратяването въз основа на определението за терористични престъпления съгласно Директива (ЕС) 2017/541 на Европейския парламент и на Съвета[4]. Като се има предвид необходимостта да се обърне внимание на най-вредната терористична пропаганда онлайн, определението следва да обхваща материали […], които подбуждат, насърчават или пропагандират извършването на терористични престъпления или на съучастието в тях, […] или подстрекават към участие в дейности на терористична група. […]***Определението включва съдържание, което предоставя насоки за направата и използването на взривни вещества, огнестрелни или други оръжия или отровни или опасни вещества, както и ХБРЯ вещества, или за други методи и техники, включително подбор на целите, за извършване на терористични престъпления.*** Тези […] ***материали*** включват по-конкретно текст, изображения, звукозаписи и видеозаписи. Когато преценяват дали съдържанието представлява терористично съдържание по смисъла на настоящия регламент, компетентните органи, както и доставчиците на хостинг услуги следва да вземат предвид фактори като естеството и формулировката на изявленията, контекста, в който са направени изявленията, и техния потенциал да доведат до вредни последици, засягащи по този начин сигурността и безопасността на хората. Фактът, че материалът е бил произведен от терористична организация или от лице, включени в списъка на ЕС, или че този материал им се приписва или е разпространяван от тяхно име, представлява важен фактор при преценката. Съдържание, което се разпространява за образователни или […] научноизследователски цели или за цели, ***свързани с разпространение на послания, противодействащи на терористичната пропаганда***, следва да бъде адекватно защитено, ***като се постига справедлив баланс между основните права, в т.ч. по-специално свободата на изразяване на мнение и свободата на информация, и съображенията за обществена сигурност. Когато разпространяваният материал се публикува под редакционната отговорност на доставчика на съдържание, всяко решение за премахването на това съдържание следва да взема предвид журналистическите стандарти, установени чрез нормативни правила за печата или медиите, които са в съответствие с правото на Съюза и правото на изразяване на мнение и плурализъм на медиите, както е заложено в член 11 от Хартата на основните права.*** Освен това изразяването на радикални, полемични или противоречиви гледни точки в обществения дебат относно чувствителни политически въпроси не следва да се счита за терористично съдържание.

---

[4] Директива (ЕС) 2017/541 на Европейския парламент и на Съвета от 15 март 2017 г. относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета, и за изменение на Решение 2005/671/ПВР на Съвета (ОВ L 88, 31.3.2017 г., стр. 6)

(10) С цел да се обхванат услугите за онлайн хостинг, с които се разпространява терористично съдържание, настоящият регламент следва да се прилага за услуги на информационното общество, които съхраняват информация ***и материали***, предоставени от получателя на услугата по негово искане, и при предоставянето на съхраняваната информация ***и материали*** на разположение на трети страни, независимо дали тази дейност е чисто техническа, автоматизирана и пасивна. […] ***Съхраняването на съдържание се състои в съхраняване на данни в паметта на физически или виртуален сървър; това изключва от обхвата обикновените преноси и други електронни съобщителни услуги по смисъла на [Европейския кодекс за електронните съобщения] или доставчиците на услуги по кеширане или други услуги, предоставяни в други слоеве на интернет инфраструктурата, например регистри и регистратори, DNS (система за имена на домейни) или прилежащи услуги като платежни услуги или услуги за защита срещу DDoS атаки (разпределени атаки тип „отказ от обслужване“). Освен това информацията трябва да се съхранява по искане на доставчика на съдържание; единствено услугите, за които доставчикът на съдържание е пряк получател, попадат в обхвата. И накрая, съхраняваната информация се предоставя на трети страни, под което се разбира трети ползватели, които не са доставчици на съдържание. В обхвата не попадат междуличностните съобщителни услуги, които позволяват пряк междуличностен и интерактивен обмен на информация между ограничен брой лица, където лицата, които инициират или участват в комуникацията, определят ответната(ите) страна(и).*** Например такива доставчици на […] ***хостинг услуги*** включват платформи на социалните мрежи, услуги за видео стрийминг, услуги за споделяне на видео, образ и звук, услуги за споделяне на файлове и други услуги за изчисления в облак ***и съхраняване*** […]. ***Настоящият регламент се прилага за дейността по предоставяне на хостинг услуги, а не за конкретния доставчик или неговата доминираща дейност, която може да съчетава хостинг услуги с други услуги, които не попадат в обхвата на настоящия регламент***.

(10a) Регламентът следва да се прилага и за доставчици на хостинг услуги, установени извън Съюза, които предлагат услуги в рамките му, тъй като значителна част от доставчиците на хостинг услуги, изложени на терористично съдържание, са установени в трети държави. Така следва да се гарантира, че всички дружества, извършващи дейност на цифровия единен пазар, отговарят на същите изисквания, независимо в коя държава са установени. За да се установи дали даден доставчик на услуги предлага услуги в Съюза, е необходимо да се прецени дали доставчикът на услуги дава възможност на юридически или физически лица в една или няколко държави членки да използват услугите му. Самата достъпност на уебсайта на доставчика на услуги или на електронен адрес или на други координати за връзка в една или повече държави членки не следва обаче да е достатъчно условие за прилагането на настоящия регламент.

(11) За определянето на приложното поле на настоящия регламент значение следва да има наличието на съществена връзка със Съюза. Следва да се счита, че такава съществена връзка със Съюза съществува, когато доставчикът на услуги има място на установяване в Съюза или, при липса на такова, въз основа на наличието на значителен брой потребители в една или повече държави членки или на насочването на дейностите към една или повече държави членки. Насочването на дейностите към една или повече държави членки може да бъде определено въз основа на всички релевантни обстоятелства, включително фактори като използването на език или валута, които обикновено се използват в тази държава членка, или възможността за поръчване на стоки или услуги. Насочването на дейностите към дадена държава членка може също така да бъде изведено от наличието на приложение в съответния национален магазин за приложения, от предоставянето на местна реклама или реклама на езика, използван в тази държава членка, или начина на управляване на връзките с клиентите, като например чрез осигуряване на обслужване на клиентите на езика, който обикновено се използва в дадена държава членка. Също така следва да се приеме, че е налице съществена връзка, когато доставчикът на услуги насочва дейностите си към една или няколко държави членки, както е посочено в член 17, параграф 1, буква в) от Регламент (ЕО) № 1215/2012 на Европейския парламент и на Съвета[5]. От друга страна, предоставянето на услугата само с оглед на спазването на забраната за дискриминация, определена в Регламент (ЕС) 2018/302 на Европейския парламент и на Съвета[6], не може да се разглежда единствено на това основание като насочване на дейностите към определена територия в рамките на Съюза.

---

5 Регламент (ЕС) № 1215/2012 на Европейския парламент и на Съвета от 12 декември 2012 г. относно компетентността, признаването и изпълнението на съдебни решения по граждански и търговски дела (ОВ L 351, 20.12.2012 г., стр. 1).

6 Регламент (ЕС) 2018/302 на Европейския парламент и на Съвета от 28 февруари 2018 г. за преодоляване на необоснованото блокиране на географски принцип и на други форми на дискриминация въз основа на националността, местопребиваването или мястото на установяване на клиентите в рамките на вътрешния пазар и за изменение на регламенти (ЕО) № 2006/2004 и (ЕС) 2017/2394 и Директива 2009/22/ЕО (ОВ L 601, 2.3.2018 г., стр. 1).

(12) Доставчиците на хостинг услуги следва да изпълняват определени задължения за полагане на грижа с цел предотвратяване на разпространението на терористично съдържание чрез услугите им. Тези задължения за полагане на грижа не следва да представляват общо задължение за контрол. Задълженията за полагане на грижа следва да включват, че при прилагането на настоящия регламент, доставчиците на хостинг услуги действат по старателен, пропорционален и недискриминационен начин по отношение на съдържанието, което съхраняват, по-специално когато прилагат своите условия за ползване, за да се избегне премахването на съдържание, което не е терористично ***съдържание***. Премахването или блокирането на достъпа трябва да се извършва при съблюдаване на свободата на изразяване на мнение и свободата на информация.

(13) Процедурата и задълженията, произтичащи от заповеди, с които на доставчиците на хостинг услуги се нарежда да премахнат терористично съдържание или да блокират достъпа до него, вследствие на преценка от страна на компетентните органи, следва да бъдат хармонизирани. Държавите членки следва да могат и занапред да избират своите компетентни органи, което им позволява да натоварят с тази задача административни, правоприлагащи или съдебни органи. Като се има предвид скоростта, с която терористичното съдържание се разпространява сред онлайн услугите, тази разпоредба налага задължения на доставчиците на хостинг услуги да гарантират, че терористичното съдържание, посочено в заповедта за премахване, е премахнато или че достъпът до него е бил блокиран в срок от един час от получаването на заповедта за премахване. ***Без да се засяга изискването за съхраняване на данни съгласно член 7 от настоящия регламент или съгласно [проекта за законодателен акт за електронните доказателства], д***оставчиците на хостинг услуги са тези, които решават дали да премахнат това съдържание или да блокират достъпа до него за ползвателите в Съюза. ***Това следва да води до предотвратяване на достъпа или поне затрудняването му и до съществено разубеждаване на интернет потребителите, които използват услугите им, да получават достъп до съдържанието, чийто достъп е блокиран***.

(13а) Заповедта за премахване следва да включва класифициране на съответното съдържание като терористично съдържание и да съдържа достатъчно информация за локализиране на съдържанието чрез предоставяне на URL и всяка друга допълнителна информация, например снимка на екрана с въпросното съдържание. При поискване компетентният орган следва да предостави допълнително описание на причините, поради които съдържанието се счита за терористично съдържание. Не е необходимо предоставените причини да съдържат чувствителна информация, която може да застраши разследванията. Описанието на причините следва обаче да позволи на доставчика на хостинг услуги и в крайна сметка на доставчика на съдържание да упражняват ефективно правото си на съдебна защита.

(14) Компетентният орган следва да предаде заповедта за премахване директно на адресата и звеното за контакт по всички електронни средства, които дават възможност за писмено документиране при условия, които позволяват на доставчика на услуги да установи автентичността, включително точността на датата и часа на изпращане и получаване на заповедта, например чрез защитена електронна поща и платформи или други защитени канали, включително предоставените от доставчика на услуги, в съответствие с правилата за защита на личните данни. Това изискване може да бъде изпълнено, по-специално чрез използването на квалифицирани услуги за електронна препоръчана поща, както е предвидено в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета[7].

[7] Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73)

(15) […] Механизм***ът*** […] ***за сигнали*** с цел предупреждаване на доставчиците на хостинг услуги относно информация ***и материали***, които могат да се считат за терористично съдържание, с цел доставчикът доброволно да разгледа тяхната съвместимост ***със*** собствените си условия за ползване***, представлява […] особено ефективен, бърз и пропорционален начин, по който доставчиците на хостинг услуги да разберат за специфичното съдържание на услугите си*** […]. Важно е доставчиците на хостинг услуги да оценяват приоритетно такива сигнали и да предоставят бърза обратна информация за предприетите действия. Окончателното решение за това дали съдържанието да бъде премахнато или не, защото не е съвместимо с неговите условия за ползване, се взема от доставчика на хостинг услуги. При прилагането на настоящия регламент във връзка със сигналите, мандатът на Европол, определен в Регламент (ЕС) 2016/794[8], остава непроменен.

(16) Предвид мащаба и скоростта, необходими за ефективното откриване и премахване на терористично съдържание, наличието на пропорционални проактивни мерки, включително чрез използване на автоматизирани средства в някои случаи, е съществен елемент в борбата с терористичното съдържание онлайн. С цел намаляване на достъпността на терористичното съдържание, на което са изложени услугите им, доставчиците на хостинг услуги следва да преценят дали е целесъобразно да се предприемат проактивни мерки в зависимост от рисковете и степента на излагане на терористично съдържание, както и от въздействието върху правата на трети страни и обществения интерес от информация. Следователно доставчиците на хостинг услуги следва да определят каква подходяща, ефективна и пропорционална мярка следва да се въведе. Това задължение не следва да предполага наличието на общо задължение за контрол. В контекста на тази оценка липсата на заповеди за премахване и на сигнали, адресирани до доставчика на хостинг услуги, е признак за нисък ***риск или*** степен на излагане на терористично съдържание.

---

8 Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и за замяна и отмяна на решения 2009/371/ПВР, 2009/934/ПВР, 2009/935/ПВР, 2009/936/ПВР и 2009/968/ПВР на Съвета (ОВ L 135, 24.5.2016 г., стр. 53)

(17) При въвеждането на проактивни мерки доставчиците на хостинг услуги следва да гарантират, че правото на ползвателите на свобода на изразяване на мнение и на свобода на информация, включително свобода на получаване и разпространяване на информация, се запазва. В допълнение към всички изисквания, предвидени в законодателството, включително законодателството за защита на личните данни, доставчиците на хостинг услуги следва да действат с дължима грижа и да прилагат гаранции, включително по-конкретно контрол и проверки от човек, когато това е целесъобразно, за да се избегне вземането на неволно и погрешно решение, водещо до премахване на съдържание, което не е терористично. Това е особено важно, когато доставчиците на хостинг услуги използват автоматизирани средства за откриване на терористично съдържание. Всяко решение за използване на автоматизирани средства, независимо дали е взето от самия доставчик на хостинг услуги или по искане на компетентния орган, следва да се оценява предвид надеждността на използваната технология и произтичащото от това въздействие върху основните права.

(18) За да се осигури, че доставчиците на хостинг услуги, изложени на терористично съдържание, предприемат подходящи мерки за предотвратяване на злоупотреба с техните услуги, компетентните органи следва да изискват от доставчиците на хостинг услуги, получили заповед за премахване, която е станала окончателна, да докладват за предприетите проактивни мерки. Те могат да представляват мерки за предотвратяване на повторно качване на терористично съдържание, което преди това е било премахнато или достъпът до което е бил блокиран вследствие на заповед за премахване или на получени от тях сигнали, проверени спрямо публично или частно притежавани инструменти, съдържащи известно терористично съдържание. Те могат също така да използват надеждни технически средства за идентифициране на ново терористично съдържание, като за целта използват наличните на пазара средства или тези, разработени от доставчика на хостинг услуги. Доставчикът на услуги следва да докладва за конкретните проактивни мерки, които прилага, за да се даде възможност на компетентния орган да прецени дали мерките са ефективни и пропорционални и дали, ако се използват автоматизирани средства, доставчикът на хостинг услуги притежава необходимия капацитет за извършване на контрол и проверка от човек. При оценяването на ефективността и пропорционалността на мерките компетентните органи следва да вземат предвид съответните параметри, включително броя на заповедите за премахване и на подадените до доставчика сигнали, икономическия му капацитет и въздействието на неговата услуга върху разпространението на терористично съдържание (например, като се вземе предвид броят на ползвателите в Съюза).

(19) В резултат на искането компетентният орган следва да започне диалог с доставчика на хостинг услуги относно необходимите проактивни мерки, които да бъдат въведени. Ако е необходимо, компетентният орган следва да наложи приемането на подходящи, ефективни и пропорционални проактивни мерки, когато счита, че предприетите мерки са недостатъчни за справяне с рисковете. Решението за налагане на такива конкретни проактивни мерки не следва по принцип да води до налагането на общо задължение за контрол, както е предвидено в член 15, параграф 1 от Директива 2000/31/ЕО. Като се имат предвид особено сериозните рискове, свързани с разпространението на терористично съдържание, решенията, приети от компетентните органи въз основа на настоящия регламент, могат да дерогират от подхода, установен в член 15, параграф 1 от Директива 2000/31/ЕО, по отношение на някои конкретни целеви мерки, чието приемане е необходимо поради причини, свързани с обществената сигурност. Преди приемането на такива решения компетентният орган следва да постигне справедлив баланс между целите от обществен интерес и свързаните с тях основни права, по-специално свободата на изразяване на мнение и свободата на информация и свободата на стопанска инициатива, както и да предостави подходяща обосновка.

(20) Задължението на доставчиците на хостинг услуги за запазване на премахнатото съдържание и на свързаните с него данни следва да бъде определено за конкретни цели и ограничено във времето до необходимото за тези цели. Необходимо е изискването за запазване да се разшири до свързаните данни, доколкото тези данни иначе биха били загубени в резултат на премахването на въпросното съдържание. Свързаните данни могат да включват данни като „данни на абоната“, включително по-конкретно данни за самоличността на доставчика на съдържание, ***„трансакционни данни“ и*** […] „данни за достъпа“, включително, например, данни за датата и часа на ползване от страна на доставчика на съдържание, или влизането и излизането от услугата, заедно с IP адреса, предоставен от доставчика на услуги за достъп до интернет на доставчика на съдържание.

(21) Задължението за запазване на съдържанието за целите на процедури за обжалване по административен или съдебен ред е необходимо и обосновано с цел да се гарантират ефективни мерки за правна защита за доставчика на съдържание, чието съдържание е било премахнато или достъпът до което е бил блокиран, както и за да се осигури възстановяването на това съдържание във вида му преди премахването в зависимост от резултата от процедурата за обжалване. Задължението за запазване на съдържание за целите на разследването и повдигането и поддържането на обвинение е обосновано и необходимо с оглед на важността, която този материал би могъл да има за възпрепятстването или предотвратяването на терористичната дейност. Когато предприятия премахват или блокират достъпа до съдържание, по-специално чрез свои собствени проактивни мерки, но не информират съответния орган за това, тъй като преценяват, че то не попада в приложното поле на член 13, параграф 4 от настоящия регламент, правоприлагащите органи може да не знаят за съществуването на съдържанието. Поради това запазването на съдържанието за целите на предотвратяването, откриването, разследването и наказателното преследване на терористични престъпления също е оправдано. За тези цели изискваното съхранение на данни е ограничено до данни, които е вероятно да имат връзка с терористични престъпления, и следователно може да допринесат за наказателното преследване на терористични престъпления или за предотвратяването на сериозни рискове за обществената сигурност.

(22) За да се гарантира пропорционалността, периодът на съхранение следва да бъде ограничен до шест месеца, за да се даде достатъчно време на доставчиците на съдържание да започнат процеса на обжалване и да се даде възможност на правоприлагащите органи да получат достъп до съответните данни от значение за разследването и наказателното преследване на терористични престъпления. Въпреки това този срок може да бъде удължен за периода, който е необходим, в случай че процедурата по обжалване е започнала, но не е приключила в рамките на шестмесечния срок по искане на органа, занимаващ се с обжалването. Тази продължителност следва да бъде достатъчна, за да се даде възможност на правоприлагащите органи да запазят необходимите доказателства във връзка с разследванията, като същевременно се гарантира балансът със съответните основни права.

(23) Настоящият регламент не засяга процесуалните гаранции и процедурните мерки за разследване, свързани с достъпа до съдържание и свързаните с него данни, съхранявани за целите на разследването и наказателното преследване на терористични престъпления, уредени съгласно националното законодателство на държавите членки и съгласно законодателството на Съюза.

(24) Прозрачността на политиките на доставчиците на хостинг услуги във връзка с терористичното съдържание е от съществено значение за подобряване на тяхната отчетност спрямо техните ползватели и за укрепване на доверието на гражданите в цифровия единен пазар. Доставчиците на хостинг услуги, ***които са изложени на терористично съдържание,*** следва да публикуват годишни доклади за прозрачност, съдържащи полезна информация за предприетите действия във връзка с откриването, идентифицирането и премахването на терористично съдържание, ***когато това не нарушава целта на въведените мерки.***

(25) Процедурите за подаване на жалби представляват необходима предпазна мярка срещу погрешното премахване на съдържание, ***вследствие на мерките, предприети съгласно реда и условията на доставчиците на хостинг услуги***, което е защитено съгласно свободата на изразяване на мнение и свободата на информация. Поради това доставчиците на хостинг услуги следва да създадат удобни за ползвателите механизми за подаване на жалби и да гарантират, че жалбите се обработват бързо и при пълна прозрачност спрямо доставчика на съдържание. Изискването доставчикът на хостинг услуги да възстанови съдържанието, когато то е било премахнато поради грешка, не засяга възможността доставчиците на хостинг услуги да прилагат своите условия за ползване на други основания. ***Освен това доставчиците на съдържание, чието съдържание е премахнато вследствие на заповед за премахване, следва да имат право на ефективни правни средства за защита в съответствие с член 19 от ДЕС и член 47 от Хартата на основните права на Европейския съюз***.

(26) ***Като цяло, с***[…]ъгласно член 19 от ДЕС и член 47 от Хартата на основните права на Европейския съюз ефективната правна защита изисква лицата да са в състояние да установят какви са причините, поради които съдържанието, качено от тях, е било премахнато или достъпът до него е бил блокиран. За тази цел доставчикът на хостинг услуги следва да предостави на разположение на доставчика на съдържание смислена информация, позволяваща на доставчика на съдържание да оспори решението. Това обаче не изисква непременно уведомяване на доставчика на съдържанието. В зависимост от обстоятелствата доставчиците на хостинг услуги могат да заменят съдържанието, което се счита за терористично съдържание, със съобщение, че то е било премахнато или че достъпът до него е бил блокиран в съответствие с настоящия регламент. Допълнителна информация за причините, както и за възможностите доставчикът на съдържание да оспори решението, следва да бъде предоставена при поискване. Когато компетентните органи решат, че по причини, свързани с обществената сигурност, включително в рамките на разследване, се счита, че не е целесъобразно или ще има обратен ефект доставчикът на съдържание да бъде директно уведомен за премахването на съдържание или за блокирането на достъпа до него, те следва да уведомят за това доставчика на хостинг услуги.

(27) За да се избегне дублирането на работа и възможната намеса в разследвания, компетентните органи следва взаимно да се уведомяват и координират и да си сътрудничат помежду си и, когато е целесъобразно, с Европол […] ***преди*** издаването на заповеди за премахване или ***при*** изпращането на сигнали до доставчици на хостинг услуги. При вземането на решение за издаване на заповед за премахване компетентният орган следва да обърне надлежно внимание на всяко уведомление за интереси, свързани с намеса в разследванията (избягване на конфликти). […] ***При вземането на решение за издаване на заповед за премахване компетентният орган следва да обърне надлежно внимание на всяко уведомление за интереси, свързани с намеса в разследванията (избягване на конфликти). Когато даден компетентен орган е информиран от компетентен орган в друга държава членка за съществуваща заповед за премахване, не следва да се издава дублираща се заповед.*** При прилагането на разпоредбите на настоящия регламент Европол може да окаже подкрепа в съответствие със сегашния си мандат и съществуващата правна уредба.

(28) За да се осигури ефективно и достатъчно съгласувано прилагане на проактивни мерки, компетентните органи в държавите членки следва да си сътрудничат по отношение на дискусиите, които водят с доставчиците на хостинг услуги във връзка с установяването, прилагането и оценката на конкретни проактивни мерки. Подобно сътрудничество е необходимо и във връзка с приемането на правила относно санкциите, както и във връзка с изпълнението и налагането на санкции. ***Комисията следва да улеснява подобна координация и сътрудничество.***

(29) От съществено значение е компетентният орган в държавата членка, който отговаря за налагането на санкции, да бъде напълно информиран за издаването на заповеди за премахване и за подаването на сигнали, както и за последващ обмен между доставчика на услуги и съответния компетентен орган. За тази цел държавите членки предоставят подходящи канали или механизми за комуникация, позволяващи своевременното споделяне на съответната информация.

(30) За да се улесни бързият обмен на информация между компетентните органи, както и с доставчиците на хостинг услуги, а също и за да се избегне дублирането на усилия, държавите членки […] ***се насърчават*** да използват ***специалните*** разработени от Европол инструменти, като например действащото приложение за управление на сигнализирането в интернет (IRMa) или инструменти, които са негови приемници.

(31) Предвид конкретните сериозни последици от определено терористично съдържание доставчиците на хостинг услуги следва незабавно да уведомяват съответните органи в засегнатата държава членка или компетентните органи на мястото, където се намира тяхното основно място на стопанска дейност или законният им представител, за съществуването на доказателства за терористични престъпления, за които са узнали. За да се гарантира пропорционалността, това задължение е ограничено до терористичните престъпления, определени в член 3, параграф 1 от Директива (ЕС) 2017/541. Задължението за уведомяване не предполага задължение за доставчиците на хостинг услуги активно да търсят такива доказателства. Засегнатата държава членка е държавата членка, която има юрисдикция при разследването и наказателното преследване на терористичните престъпления в съответствие с Директива (ЕС) 2017/541, въз основа на гражданството на извършителя на престъплението или на потенциалната жертва на престъплението или на мястото на извършване на терористичния акт. В случай на съмнение доставчиците на хостинг услуги могат да предават информацията на Европол, който следва да действа в съответствие със своя мандат, включително да препраща информацията на съответните национални органи.

(32) Компетентните органи в държавите членки следва да могат да използват тази информация, за да предприемат мерки за разследване, които са предвидени съгласно правото на държава членка или на Съюза, включително издаването на европейска заповед за предоставяне съгласно Регламента относно европейските заповеди за предоставяне и за запазване на електронни доказателства по наказателноправни въпроси[9].

(33) Както доставчиците на хостинг услуги, така и държавите членки следва да създадат звена за контакт, които да улесняват бързото обработване на заповедите за премахване и на сигналите. За разлика от законния представител звеното за контакт служи за оперативни цели. Звеното за контакт на доставчика на хостинг услуги следва да разполага със специализирани средства, ***вътрешни или външни***, позволяващи подаването на заповеди за премахване и на сигнали по електронен път и с технически средства […] ***или*** персонал, позволяващи бързото им обработване. Не е необходимо звеното за контакт на доставчика на хостинг услуги да се намира в Съюза, като доставчикът на хостинг услуги е свободен да определи съществуващо звено за контакт, при условие че то може да изпълнява функциите, предвидени в настоящия регламент. С цел да се гарантира, че дадено терористично съдържание е премахнато или че достъпът до него е блокиран в срок от един час след получаване на заповед за премахване, ***доставчиците на хостинг услуги, които са изложени на терористично съдържание, както е видно от получаването на заповед за премахване,*** следва да гарантират, че звеното за контакт е на разположение 24 часа в денонощието седем дни в седмицата. Информацията относно звеното за контакт следва да включва информация относно езика, на който може да се общува с него. С цел да се улесни комуникацията между доставчиците на хостинг услуги и компетентните органи, доставчиците на хостинг услуги се насърчават да позволяват комуникация на един от официалните езици на Съюза, на който са налични техните условия за ползване.

(34) При липсата на общо изискване доставчиците на услуги да гарантират физическо присъствие на територията на Съюза е необходимо да се осигури яснота относно това коя държава членка има юрисдикция по отношение на доставчика на хостинг услуги, предлагащ услуги в рамките на Съюза. Като общо правило доставчикът на хостинг услуги попада под юрисдикцията на държавата членка, в която се намира неговото основно място на стопанска дейност или в която е определил свой законен представител. ***С оглед на ефективното изпълнение, спешността и обществения ред обаче всяка държава членка следва да има юрисдикция по отношение на заповедите за премахване и сигналите.***

---

9 COM(2018)225 final

(35) Доставчиците на хостинг услуги, които не са установени в Съюза, следва да определят писмено законен представител с цел да гарантират спазването и изпълнението на задълженията съгласно настоящия регламент. ***Доставчиците на хостинг услуги могат да използват съществуващ законен представител, при условие че този законен представител е в състояние да изпълнява функциите, посочени в настоящия регламент***.

(36) Законният представител следва да бъде законно упълномощен да действа от името на доставчика на хостинг услуги.

(37) За целите на настоящия регламент държавите членки следва да определят компетентни органи. Изискването за определяне на компетентни органи не означава непременно създаването на нови органи, а може да представлява възлагане на изпълнението на функциите, определени в настоящия регламент, на съществуващи органи. Настоящият регламент налага определянето на органи, компетентни да издават заповеди за премахване и сигнали, както и да следят за прилагането на проактивни мерки и за налагането на санкции. Държавите членки решават колко органа да определят за изпълнението на тези задачи.

(38) Необходими са санкции, за да се гарантира ефективното изпълнение от страна на доставчиците на хостинг услуги на задълженията съгласно настоящия регламент. Държавите членки следва да приемат правила относно санкциите, ***които могат да бъдат от административен или наказателноправен характер,*** включително, когато е целесъобразно, насоки за налагане на глоби. Особено тежки санкции следва да се налагат, в случай че доставчикът на хостинг услуги систематично не премахва терористично съдържание или не блокира достъпа до него в срок от един час от получаването на заповедта за премахване. Неспазването на изискванията в отделни случаи може да бъде санкционирано, като същевременно се спазват принципите на *ne bis in idem* и на пропорционалност и като се гарантира, че при тези санкции се взема предвид систематичното неспазване. За да се гарантира правната сигурност, в регламента следва да се определи до каква степен съответните задължения могат да бъдат предмет на санкции. Санкциите за неспазване на разпоредбите на член 6 следва да се приемат единствено във връзка със задължения, произтичащи от искане за докладване съгласно член 6, параграф 2 или решение за налагане на допълнителни проактивни мерки съгласно член 6, параграф 4. ***При оценката на естеството на нарушението и при вземането на решение за налагане на санкции, следва да се зачитат в пълна степен основните права, например свободата на изразяване на мнение.*** При определяне на това дали следва да бъдат наложени финансови санкции, следва да се вземат предвид финансовите ресурси на доставчика. Държавите членки следва да гарантират, че санкциите не насърчават премахването на съдържание, което не е терористично съдържание.

(39) Използването на стандартизирани образци улеснява сътрудничеството и обмена на информация между компетентните органи и доставчиците на услуги, като им позволява да общуват по-бързо и по-ефективно. Особено важно е да се гарантират бързи действия след получаването на заповед за премахване. Благодарение на образците се намаляват разходите за превод и се допринася за установяването на стандарт за високо качество. Формулярите за отговор следва да направят възможен стандартизирния обмен на информация, а това ще бъде от голямо значение, когато доставчиците на услуги не могат да спазят изискванията. Каналите за подаване с удостоверена автентичност могат да гарантират автентичността на заповедта за премахване, включително точността на датата и часа на изпращане и получаване на заповедта.

(40) С цел да се даде възможност за бързо изменение, когато е необходимо, на съдържанието на образците, които да бъдат използвани за целите на настоящия регламент, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от Договора за функционирането на Европейския съюз за изменение на приложения I, II и III към настоящия регламент. За да може да взема предвид развитието на технологиите и свързаната с това правна уредба, на Комисията следва да се предостави правомощието да приема делегирани актове с цел допълване на настоящия регламент с техническите изисквания за електронните средства, които да се използват от компетентните органи за връчването на заповедите за премахване. От особена важност е по време на своята подготвителна работа Комисията да проведе подходящи консултации, включително на експертно равнище, и тези консултации да бъдат проведени в съответствие с принципите, заложени в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 г.[10] По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

(41) Държавите членки следва да събират информация относно прилагането на законодателството. ***Държавите членки могат да използват докладите за прозрачност на доставчиците на хостинг услуги и при необходимост да ги допълват с по-подробна информация***. Следва да се създаде подробна програма за мониторинг на крайните продукти, резултатите и въздействието на настоящия регламент, като целта е информацията от нея да се използва за оценка на законодателството.

---

10 ОВ L 123, 12.5.2016 г., стр. 1

(42) Въз основа на констатациите и заключенията в доклада за изпълнението и на резултата от мониторинга Комисията следва да извърши оценка на настоящия регламент не по-рано от три години след влизането му в сила. Оценката следва да се основава на петте критерия за ефикасност, ефективност, уместност, съгласуваност и добавена стойност от ЕС. С нея ще се оцени функционирането на различните оперативни и технически мерки, предвидени в Регламента, включително ефективността на мерките за подобряване на откриването, идентифицирането и премахването на терористично съдържание, ефективността на предпазните механизми, както и въздействието върху потенциално засегнатите права и интереси на трети страни, включително преглед на изискването за информиране на доставчиците на съдържание.

(43) Тъй като целта на настоящия регламент, а именно да се гарантира безпрепятственото функциониране на цифровия единен пазар чрез предотвратяване на разпространението на терористично съдържание онлайн, не може да бъде постигната в достатъчна степен от държавите членки и следователно, поради обхвата и последиците от предвиденото действие, може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

РАЗДЕЛ I
ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и обхват

1. С настоящия регламент се установяват единни правила за предотвратяване на злоупотребата с хостинг услуги за разпространение на терористично съдържание онлайн. С него се установяват по-специално:

   а) правила относно задълженията на доставчиците на хостинг услуги да полагат грижи за предотвратяване на разпространението на терористично съдържание чрез техните услуги и да гарантират, когато е необходимо, бързото му премахване;

   б) набор от мерки, които да бъдат въведени от държавите членки с цел идентифициране на терористично съдържание, гарантиране на бързото му премахване от доставчиците на хостинг услуги и улесняване на сътрудничеството с компетентните органи в други държави членки, доставчици на хостинг услуги и, когато е целесъобразно, съответните органи на Съюза.

2. Настоящият регламент се прилага за доставчиците на хостинг услуги, които предлагат услуги в Съюза, независимо от тяхното основно място на стопанска дейност.

3. ***Настоящият регламент не води до изменение на задължението за спазване на основните права и основните правни принципи, залегнали в член 6 от Договора за Европейския съюз.***

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

(1) „доставчик на хостинг услуги“ означава доставчик на услуги на информационното общество, които се състоят в съхраняването по искане на доставчика на съдържание на информация, предоставяна от самия него, и в предоставяне на съхраняваната информация на разположение на трети страни;

(2) „доставчик на съдържание“ означава ползвател, предоставил информация, която се съхранява или е била съхранявана по негово искане от доставчик на хостинг услуги;

(3) „предлагане на услуги в Съюза“ означава предоставяне на възможността юридически или физически лица в една или няколко държави членки да използват услугите на доставчика на хостинг услуги, който има съществена връзка с тази държава членка или тези държави членки, например мястото на стопанска дейност на доставчика на хостинг услуги в Съюза;

При липса на такова място на стопанска дейност оценката на съществената връзка се основава на конкретни фактически критерии, например

а) значителен брой ползватели в една или няколко държави членки;

б) ***или*** насочване на дейностите към една или няколко държави членки.

(4) „терористични престъпления“ означава ***едно от умишлените деяния, посочени*** […] в член 3, параграф 1 от Директива (ЕС) 2017/541;

(5) „терористично съдържание“ означава […] ***материал, който може да допринесе за извършването на умишлените деяния, посочени в член 3, параграф 1, букви а)—и) от Директива 2017/541 чрез***:

аа) отправяне на заплаха за извършване на терористично престъпление;

а) подбуждане или пропаганда, […] ***например*** […] […]***възхваляване на терористични актове,*** извършване на терористични престъпления, като по този начин се създава опасност от извършването на такива деяния;

б) ***склоняване на лица или групи лица да извършат или*** […] да допринес***ат*** […] за извършването на терористични престъпления;

в) популяризиране на дейностите на терористична група, по-специално чрез ***склоняване на лица или група лица да*** […] участва***т*** в […] ***престъпните дейности на*** […] терористична група или да ги подкрепят по смисъла на член 2, параграф 3 от Директива (ЕС) 2017/541;

информация, с която се дават указания относно методи или техники за извършване на терористични престъпления.

(6) „разпространение на терористично съдържание“ означава предоставяне на терористично съдържание на разположение на трети страни чрез услугите на доставчици на хостинг услуги;

(7) „условия за ползване“ означава всички условия и клаузи, независимо от тяхното наименование или форма, с които се уреждат договорните отношения между доставчика на хостинг услуги и ползвателите на тези услуги;

(8) „сигнал“ означава известие от компетентен орган или, когато е приложимо, от компетентен орган на Съюза до доставчик на хостинг услуги относно информация, която може да се счита за терористично съдържание, с цел доставчикът доброволно да разгледа нейната съвместимост със собствените му условия за ползване, които имат за цел предотвратяване на разпространението на терористично съдържание;

(9) „основно място на стопанска дейност“ означава главното управление или седалището, в което се упражняват основните финансови функции и оперативният контрол ***в Съюза***.

РАЗДЕЛ II

Мерки за предотвратяване на разпространението на терористично съдържание онлайн

Член 3

Задължения за полагане на грижа

1. Доставчиците на хостинг услуги предприемат целесъобразни, разумни и пропорционални действия в съответствие с настоящия регламент срещу разпространението на терористично съдържание и за защита на ползвателите от терористично съдържание. При това те действат по старателен, пропорционален и недискриминационен начин, като зачитат надлежно основните права на ползвателите и вземат предвид фундаменталното значение на свободата на изразяване на мнение и свободата на информация в едно отворено и демократично общество.

2. Доставчиците на хостинг услуги включват в своите условия за ползване, ***че няма да съхраняват терористично съдържание***, и прилагат разпоредби за предотвратяване на разпространението на терористично съдържание.

Член 4

Заповеди за премахване

1. Компетентният орган разполага с правомощието да постанови […] ***заповед за премахване***, с която да изиска от доставчика на хостинг услуги да премахне терористично съдържание или да блокира достъпа до него.

2. Доставчиците на хостинг услуги премахват терористично съдържание или блокират достъпа до него в срок от един час след получаването на заповедта за премахване.

3. Заповедите за премахване съдържат следните елементи в съответствие с образеца, установен в приложение I:

   а) данни за компетентния орган, издаващ заповедта за премахване, и удостоверение на автентичността на заповедта за премахване от компетентния орган; […] ***оценка на съдържанието,*** най-малкото чрез позоваване на ***съответните*** категории терористично съдържание, изброени в член 2, параграф 5;

б) унифициран локатор на ресурси (URL) и, когато е необходимо, допълнителна информация, която позволява да се идентифицира въпросното съдържание;

в) позоваване на настоящия регламент като правното основание на заповедта за премахване;

г) дата и времеви печат за момента на издаване;

д) информация относно средствата за правна защита, които са на разположение на доставчика на хостинг услуги и доставчика на съдържание;

е) когато е приложимо, решението да не се оповестява информацията относно премахването на терористично съдържание или блокирането на достъпа до него, както е посочено в член 11.

4. По искане на доставчика на хостинг услуги или на доставчика на съдържание компетентният орган представя […] ***допълнително*** описание на причините, ***поради които съдържанието се счита за терористично съдържание,*** без да се засяга задължението на доставчика на хостинг услуги да изпълни заповедта за премахване в рамките на срока, посочен в параграф 2.

5. Компетентните органи отправят заповедите за премахване към основното място на стопанска дейност на доставчика на хостинг услуги или към законния представител, определен от доставчика на хостинг услуги съгласно член 16, и ги препращат на звеното за контакт, посочено в член 14, параграф 1. Тези заповеди се изпращат с електронни средства, които дават възможност за писмено документиране при условия, които позволяват установяване на автентичността на изпращача, включително точността на датата и часа на изпращане и получаване на заповедта.

6. ***Без ненужно забавяне д***[…]оставчиците на хостинг услуги потвърждават получаването и […] информират компетентния орган за премахването на терористичното съдържание или за блокирането на достъпа до него, като посочват по-специално часа и датата на предприетото действие, използвайки образеца от приложение II.

7. Ако доставчикът на хостинг услуги не може да изпълни заповедта за премахване поради непреодолима сила или фактическа невъзможност, която не се дължи на доставчика на хостинг услуги, той информира без ненужно забавяне компетентния орган за това, като обяснява причините, използвайки образеца от приложение III. Крайният срок, посочен в параграф 2, се прилага веднага щом посочените причини престанат да съществуват.

8. Ако доставчикът на хостинг услуги не може да изпълни заповедта за премахване, тъй като в нея се съдържат явни грешки или не се съдържа достатъчно информация за изпълнение на заповедта, доставчикът на хостинг услуги уведомява без ненужно забавяне компетентния орган за това, като изисква пояснения, използвайки образеца от приложение III. Крайният срок, посочен в параграф 2, се прилага веднага щом посочените пояснения бъдат предоставени.

9. Компетентният орган, издал заповедта за премахване, информира компетентния орган, който следи за прилагането на проактивните мерки, посочени в член 17, параграф 1, буква в), когато заповедта за премахване стане окончателна. Дадена заповед за премахване става окончателна, когато не е била обжалвана в рамките на срока, предвиден за това в приложимото национално законодателство, или когато е била потвърдена след обжалване.

Член 4а

Процедура на консултация за заповедите за премахване

1. Издаващият орган представя копие от заповедта за премахване на посочения в член 17, параграф 1, буква а) компетентен орган на държавата членка, в която се намира основното място на стопанска дейност на доставчика на хостинг услуги, едновременно с предаването на заповедта на доставчика на хостинг услуги в съответствие с член 4, параграф 5.

2. Когато компетентният орган на държавата членка, в която се намира основното място на стопанска дейност на доставчика на хостинг услуги, има разумни основания да смята, че заповедта за премахване може да окаже въздействие върху основните интереси на тази държава членка, той информира издаващия компетентен орган.

3. Издаващият орган взема предвид тези обстоятелства и при необходимост оттегля или адаптира заповедта за премахване.

Член 5

Сигнали

1. Компетентният орган или съответният орган на Съюза може да изпрати сигнал до доставчик на хостинг услуги.

2. Доставчиците на хостинг услуги въвеждат оперативни и технически мерки, с които се улеснява експедитивната оценка на съдържанието, изпратено за доброволно разглеждане от тяхна страна от компетентните органи и, когато е приложимо, от съответните органи на Съюза.

3. Сигналите се отправят към основното място на стопанска дейност на доставчика на хостинг услуги или на законния представител, определен от доставчика на хостинг услуги съгласно член 16, и се препращат на звеното за контакт, посочено в член 14, параграф 1. Тези сигнали се изпращат по електронен път.

4. Сигналът съдържа достатъчно […] информация […] ***за*** причините, поради които съдържанието се счита за терористично съдържание, ***и предоставя*** URL и, когато е необходимо, допълнителна информация, която позволява да се идентифицира въпросното терористично съдържание.

5. Доставчикът на хостинг услуги оценява приоритетно съдържанието, посочено в сигнала, спрямо своите условия за ползване и решава дали да премахне това съдържание или да блокира достъпа до него.

6. Доставчикът на хостинг услуги ***без ненужно забавяне*** уведомява […] компетентния орган или съответния орган на Съюза за резултата от оценката и точния момент на всяко действие, предприето вследствие на сигнала.

7. Когато доставчикът на хостинг услуги счита, че сигналът не съдържа достатъчно информация, за да се направи оценка на въпросното съдържание, той незабавно уведомява компетентните органи или съответния орган на Съюза за това, като посочва какви допълнителни сведения или пояснения са необходими.

Член 6

Проактивни мерки

1. […] ***В зависимост от риска и степента на излагане на терористично съдържание*** доставчиците на хостинг услуги предприемат проактивни мерки, за да предпазят своите услуги от разпространението на терористично съдържание. Мерките са ефективни и пропорционални, като отчитат риска и равнището на излагане на терористично съдържание, основните права на ползвателите и фундаменталното значение на свободата на изразяване на мнение и свободата на информация в едно отворено и демократично общество.

2. Когато е бил информиран в съответствие с член 4, параграф 9, компетентният орган, посочен в член 17, параграф 1, буква в), изисква от доставчика на хостинг услуги да представи доклад в срок от три месеца след получаване на искането и след това най-малко веднъж годишно във връзка с конкретните проактивни мерки, които е предприел, включително чрез използването на автоматизирани инструменти, с цел:

   а) […] ***ефективни мерки за справяне с*** повторното ***появяване*** […] на съдържание, което преди това е било премахнато или достъпът до което е бил блокиран, тъй като се счита за терористично съдържание;

   б) откриването, идентифицирането и експедитивното премахване на терористично съдържание или блокиране на достъпа до него.

Това искане се изпраща до основното място на стопанска дейност на доставчика на хостинг услуги или на законния представител, определен от доставчика на хостинг услуги.

Докладите включват цялата относима информация, която позволява на компетентния орган, посочен в член 17, параграф 1, буква в), да прецени дали проактивните мерки са ефективни и пропорционални, включително да оцени функционирането на всички използвани автоматизирани инструменти, както и използваните механизми за контрол и проверка от човек.

3. Когато компетентният орган, посочен в член 17, параграф 1, буква в), счита, че предприетите проактивни мерки, за които е докладвано съгласно параграф 2, не са достатъчни за ограничаването и управлението на риска и равнището на излагане, той може да поиска от доставчика на хостинг услуги да предприеме конкретни допълнителни проактивни мерки. За тази цел доставчикът на хостинг услуги си сътрудничи с компетентния орган, посочен в член 17, параграф 1, буква в), за да се определят конкретните мерки, които доставчикът на хостинг услуги да въведе, като се установяват ключови цели и критерии, както и графици за тяхното изпълнение.

4. Ако не може да бъде постигнато споразумение в рамките на три месеца от искането по параграф 3, компетентният орган, посочен в член 17, параграф 1, буква в), може да издаде решение, с което да наложи конкретни допълнителни необходими и пропорционални проактивни мерки. В решението се вземат предвид по-специално икономическият капацитет на доставчика на хостинг услуги и ефектът от такива мерки върху основните права на ползвателите и фундаменталното значение на свободата на изразяване на мнение и свободата на информация. ***Компетентният орган, посочен в член 17, параграф 1, буква в), има право на преценка относно естеството и обхвата на проактивните мерки в съответствие с целта на настоящия регламент***. Това решение се изпраща до основното място на стопанска дейност на доставчика на хостинг услуги или на законния представител, определен от доставчика на хостинг услуги. Доставчикът на хостинг услуги редовно докладва за изпълнението на тези мерки, както е определено от компетентния орган, посочен в член 17, параграф 1, буква в).

5. Доставчикът на хостинг услуги може по всяко време да поиска от компетентния орган, посочен в член 17, параграф 1, буква в), да преразгледа и при необходимост да отмени дадено искане или решение по параграфи 2, 3 и 4 съответно. Компетентният орган издава мотивирано решение в рамките на разумен срок след получаване на искането от доставчика на хостинг услуги.

Член 7

Съхраняване на съдържание и свързани с него данни

1. Доставчиците на хостинг услуги съхраняват терористичното съдържание, което е премахнато или блокирано вследствие на заповед за премахване, сигнал или проактивни мерки в съответствие с членове 4, 5 и 6, и свързаните с него данни, които са премахнати в резултат на премахването на терористичното съдържание**,** […] които са необходими за:

   а) процедури за обжалване по административен или съдебен ред,

   б) предотвратяването, разкриването, разследването или наказателното преследване на терористични престъпления;

2. Терористичното съдържание и свързаните с него данни, посочени в параграф 1, се съхраняват за срок от шест месеца. При поискване от компетентния орган или съд терористичното съдържание се съхранява за по-дълъг период, когато и докато това е необходимо за текущи процедури за обжалване по административен или съдебен ред, посочени в параграф 1, буква а).

3. Доставчиците на хостинг услуги гарантират, че терористичното съдържание и свързаните с него данни, съхранявани съгласно параграфи 1 и 2, са предмет на подходящи технически и организационни предпазни мерки.

   С тези технически и организационни предпазни мерки се гарантира, че съхраняваното терористично съдържание и свързаните с него данни са достъпни и се обработват само за целите, посочени в параграф 1, и се осигурява висока степен на сигурност на засегнатите лични данни. Доставчиците на хостинг услуги преразглеждат и актуализират тези предпазни мерки, когато е необходимо.

РАЗДЕЛ III
ПРЕДПАЗНИ МЕРКИ И ОТЧЕТНОСТ

Член 8

Задължения за прозрачност

1. Доставчиците на хостинг услуги установяват в своите условия за ползване политиката си за предотвратяване на разпространението на терористично съдържание, включително, когато е целесъобразно, с подходящо обяснение за функционирането на проактивните мерки, в това число използването на автоматизирани инструменти.

2. Доставчиците на хостинг услуги, […] ***изложени на терористично съдържание,*** публикуват годишни доклади за прозрачност относно действията, предприети срещу разпространението на терористично съдържание.

3. Докладите за прозрачност съдържат най-малко следната информация:

   а) информация относно мерките на доставчика на хостинг услуги във връзка с откриването, идентифицирането и премахването на терористично съдържание;

   б) информация относно мерките на доставчика на хостинг услуги ***за ефективни мерки за справяне*** […] с повторното […]***появяване*** на съдържание, което преди това е било премахнато или достъпът до което е бил блокиран, тъй като се счита за терористично съдържание;

   в) брой на материалите с терористично съдържание, които са били премахнати или достъпът до които е бил блокиран вследствие съответно на заповеди за премахване, сигнали или проактивни мерки;

   г) обзор и резултати от процедурите за подаване на жалби.

Член 9

Гаранции по отношение на използването и прилагането на проактивните мерки

1. Когато доставчиците на хостинг услуги използват автоматизирани средства съгласно настоящия регламент по отношение на съдържанието, което съхраняват, те предоставят ефективни и подходящи гаранции за точността и обосноваността на решенията, вземани във връзка с това съдържание, и по-специално на решенията за премахване на съдържание, което се счита за терористично, или за блокирането на достъпа до него.

2. Тези гаранции се изразяват по-конкретно в контрол и проверки от човек, когато това е целесъобразно и при всички случаи когато се изисква подробна преценка на съответния контекст, за да се определи дали съдържанието трябва да се счита за терористично.

Член 10

Процедури за подаване на жалби

1. Доставчиците на хостинг услуги установяват ефективни и достъпни механизми, позволяващи на доставчиците на съдържание, чието съдържание е било премахнато или до което е бил блокиран достъпът вследствие на сигнал съгласно член 5 или на проактивни мерки съгласно член 6, да подадат жалба срещу действието на доставчика на хостинг услуги с искане съдържанието да бъде възстановено.

2. Доставчиците на хостинг услуги разглеждат своевременно всяка получена жалба и възстановяват съдържанието без ненужно забавяне, когато премахването или блокирането на достъпа е било неоснователно. Те информират жалбоподателя за резултата от разглеждането на жалбата.

Член 11

Информация за доставчиците на съдържание

1. Когато доставчиците на хостинг услуги премахват терористично съдържание или блокират достъпа до него, те предоставят на доставчика на съдържание информация относно премахването или блокирането на достъпа до терористично съдържание.

2. При поискване от доставчика на съдържание доставчикът на хостинг услуги информира доставчика на съдържание за причините за премахването или блокирането на достъпа и за възможностите за оспорване на решението.

3. Задължението съгласно параграфи 1 и 2 не се прилага, когато компетентният орган реши, че тези дейности не бива да бъдат оповестявани поради причини, свързани с обществената сигурност, като например предотвратяването, разследването, разкриването и наказателното преследване на терористични престъпления, за толкова дълго време, колкото е необходимо, но не повече от […] ***шест***[…] седмици от това решение. ***Този срок може да бъде удължен еднократно с още шест седмици, ако това е обосновано.*** В такъв случай доставчикът на хостинг услуги не оповестява никаква информация за премахването или блокирането на достъпа до терористично съдържание.

РАЗДЕЛ IV
Сътрудничество между компетентните органи, органите на Съюза и доставчиците на хостинг услуги

Член 12

Капацитет на компетентните органи

Държавите членки гарантират, че техните компетентни органи разполагат с необходимия капацитет и с достатъчни ресурси за постигане на целите и за изпълнение на техните задълженията по настоящия регламент.

Член 13

Сътрудничество между доставчиците на хостинг услуги, компетентните органи и когато е необходимо, […] ***компетентните*** *органи на Съюза*

1. Компетентните органи в държавите членки взаимно се уведомяват и координират и си сътрудничат помежду си и, когато е целесъобразно, с […] ***компетентните*** органи на Съюза, като например Европол, по отношение на заповедите за премахване и сигналите, за да се избегне дублирането на работа, да се подобри координацията и да се избегне намесата в разследвания в различните държави членки.

2. Компетентните органи в държавите членки информират, координират и си сътрудничат с компетентния орган, посочен в член 17, параграф 1, букви в) и г), по отношение на мерките, предприети съгласно член 6, и мерките за принудително изпълнение съгласно член 18. Държавите членки гарантират, че компетентният орган, посочен в член 17, параграф 1, букви в) и г), притежава цялата необходима информация. За тази цел държавите членки предоставят подходящи канали или механизми за комуникация, за да се гарантира, че съответната информация се обменя своевременно.

3. ***С цел ефективно изпълнение на настоящия регламент, както и избягване на дублирането,*** държавите членки и доставчиците на хостинг услуги могат да решат да използват специални инструменти, включително […] създадени от […] ***компетентните*** органи на Съюза, като например Европол, за да се улеснят по-специално:

   а) обработването и обратната информация, свързани със заповеди за премахване в съответствие с член 4;

   б) обработването и обратната информация, свързани със сигнали в съответствие с член 5;

   в) сътрудничество с цел определянето и прилагането на проактивни мерки в съответствие с член 6.

4. Когато доставчиците на хостинг услуги узнаят за доказателства за терористични престъпления, те незабавно информират органите, компетентни за разследването и наказателното преследване на престъпления в […] съответната***(ите)*** държава***(и)*** членка***(и)*** […]. ***Когато е невъзможно да се установи(ят) съответната(ите) държава(и) членка(и), д***[…]оставчиците на хостинг услуги […] ***уведомяват звеното за контакт в държавата членка съгласно член 14, параграф 3, в която се намира тяхното основно място на стопанска дейност или законен представител, и*** предават […] тази информация и на Европол за съответни последващи действия.

Член 14

Звена за контакт

1. Доставчиците на хостинг услуги създават звено за контакт, което получава заповедите за премахване и сигналите по електронен път и осигурява бързото им обработване съгласно членове 4 и 5. Те гарантират, че тази информация е обществено достояние.

2. В информацията, посочена в параграф 1, се посочва официалният език или официалните езици на Съюза съгласно Регламент (ЕС) № 1/58, на който може да се общува със звеното за контакт и на който се обменя допълнителна информация във връзка със заповедите за премахване и сигналите съгласно членове 4 и 5. Това включва поне един от официалните езици на държавата членка, в която се намира основното място на стопанска дейност на доставчика на хостинг услуги или е установен или пребивава неговият законен представител съгласно член 16.

3. Държавите членки създават звено за контакт, което обработва исканията за разяснения и обратна информация във връзка с издадените от тях заповеди за премахване и подадените от тях сигнали. Информацията относно звеното за контакт се прави обществено достояние.

РАЗДЕЛ V
ИЗПЪЛНЕНИЕ И ПРИЛАГАНЕ

Член 15

Юрисдикция

1. За целите на членове 6, 18 и 21 юрисдикция има държавата членка, в която се намира основно място на стопанска дейност на доставчика на хостинг услуги. За доставчик на хостинг услуги, който няма основно място на стопанска дейност в никоя държава членка, се счита, че е под юрисдикцията на държавата членка, в която пребивава или е установен неговият законен представител, посочен в член 16. ***Всяка държава членка има юрисдикция за целите на членове 4 и 5, независимо къде е основното място на стопанска дейност на доставчика на хостинг услуги или дали той е определил законен представител.***

2. Когато доставчик на хостинг услуги не е определил свой законен представител, всички държави членки имат юрисдикция. ***Когато дадена държава членки реши да упражнява юрисдикцията си, тя информира всички други държави членки***.

[…] […]

Член 16

Законен представител

1. Доставчик на хостинг услуги, който не е установен в Съюза, но предлага услуги в Съюза, определя писмено дадено юридическо или физическо лице за свой законен представител в Съюза за целите на получаването, спазването и изпълнението на заповеди за премахване, сигнали, искания и решения, издадени от компетентните органи на основание настоящия регламент. Законният представител пребивава или е установен в една от държавите членки, в които доставчикът на хостинг услуги предлага услугите си.

2. Доставчикът на хостинг услуги възлага на законния представител получаването, спазването и изпълнението на заповедите за премахване, сигналите, исканията и решенията, посочени в параграф 1, от името на въпросния доставчик на хостинг услуги. Доставчиците на хостинг услуги предоставят на своя законен представител необходимите правомощия и ресурси, за да си сътрудничат с компетентните органи и да спазват тези решения и заповеди.

3. Определеният законен представител може да бъде подведен под отговорност за неспазване на задълженията, произтичащи от настоящия регламент, без да се засягат отговорността на доставчика на хостинг услуги и правните действия, които могат да бъдат предприети срещу него.

4. Доставчикът на хостинг услуги уведомява компетентния орган, посочен в член 17, параграф 1, буква г), на държавата членка, в която пребивава или е установен законният представител относно определянето му. Информацията относно законния представител се прави обществено достояние.

РАЗДЕЛ VI
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 17

Определяне на компетентните органи

1. Всяка държава членка определя органа или органите, които са компетентни:

   а) за издаването на заповеди за премахване в съответствие с член 4;

   б) за откриването и идентифицирането на терористично съдържание и за изпращането на сигнал за него до доставчиците на хостинг услуги в съответствие с член 5;

   в) за наблюдението на прилагането на проактивни мерки в съответствие с член 6;

   г) за налагането на принудително изпълнение на задълженията, произтичащи от настоящия регламент, посредством санкции в съответствие с член 18.

2. Най-късно до [***дванадесет*** […] *месеца след влизането в сила на настоящия регламент*] държавите членки уведомяват Комисията за компетентния ***орган или*** органи, посочени в параграф 1. Комисията публикува уведомлението и всички негови изменения в *Официален вестник на Европейския съюз*.

Член 18

Санкции

1. Държавите членки установяват правилата относно санкциите, приложими при нарушения от страна на доставчиците на хостинг услуги на задълженията, произтичащи от настоящия регламент, и предприемат всички необходими мерки за гарантиране на тяхното налагане. Тези санкции се ограничават до нарушения на задълженията, произтичащи от:

   а) член 3, параграф 2 (условия за ползване на доставчиците на хостинг услуги);

   б) член 4, параграфи 2 и 6 (изпълнение на заповеди за премахване и обратна информация);

в) член 5, параграфи 5 и 6 (оценка на сигнали и обратна информация);

г) член 6, параграфи 2 и 4 (доклади за проактивните мерки и приемането на мерки след решение за налагане на конкретни проактивни мерки);

д) член 7 (съхраняване на данни);

е) член 8 (прозрачност);

ж) член 9 (гаранции по отношение на проактивните мерки);

з) член 10 (процедури за подаване на жалби);

и) член 11 (информация за доставчиците на съдържание);

й) член 13, параграф 4 (информация за доказателства за терористични престъпления);

к) член 14, параграф 1 (звена за контакт);

л) член 16 (определяне на законен представител).

2. Предвидените санкции трябва да бъдат ефективни, пропорционални и възпиращи. Най-късно до [*... месеца от влизането в сила на настоящия регламент*] държавите членки съобщават на Комисията тези правила и мерки и ѝ съобщават незабавно всички последващи техни изменения.

3. Държавите членки гарантират, че при определянето на вида и размера на санкциите компетентните органи вземат предвид всички значими обстоятелства, в това число:

а) естеството, тежестта и продължителността на нарушението;

б) дали нарушението е умишлено или е резултат от небрежност;

в) предишни нарушения, извършени от отговорното юридическо ***или физическо*** лице;

г) финансовата стабилност на отговорното юридическо ***или физическо*** лице;

д) степента на съдействие на доставчика на хостинг услуги с компетентните органи.

4. Държавите членки гарантират, че системното неспазване на задълженията по член 4, параграф 2 подлежи на финансови санкции в размер до 4 % от общия оборот на доставчика на хостинг услуги за последната финансова година.

Член 19

Технически изисквания и изменения на образците за заповедите за премахване

1. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 20 с цел допълване на настоящия регламент с техническите изисквания за електронните средства, които да се използват от компетентните органи за връчването на заповедите за премахване.

2. На Комисията се предоставя правомощието да приема такива делегирани актове за изменение на приложения I, II и III с цел да се предприемат ефективни действия при евентуална необходимост от подобрения по отношение на съдържанието на формулярите за заповед за премахване и формулярите, които да се използват за предоставяне на информация относно невъзможността за изпълнение на заповед за премахване.

Член 20

Упражняване на делегирането

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.

2. Правомощието да приема делегирани актове, посочено в член 19, се предоставя на Комисията за неопределен срок, считано от [*датата на прилагане на настоящия регламент*].

3. Делегирането на правомощия, посочено в член 19, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. Оттеглянето поражда действие в деня след публикуването на решението в Официален вестник на Европейския съюз или на по-късна дата, посочена в решението. То не засяга действителността на делегираните актове, които вече са в сила.

4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 година.

5. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.

6. Делегиран акт, приет съгласно член 19, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражение в срок от два месеца след нотифицирането на същия акт на Европейския парламент и на Съвета, или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок може да се удължи с два месеца по инициатива на Европейския парламент или на Съвета.

Член 21

Мониторинг

1. Държавите членки събират от своите компетентни органи и от доставчиците на хостинг услуги под тяхна юрисдикция информация за действията, които те са предприели в съответствие с настоящия регламенти, и я изпращат на Комисията всяка година до [31 март]. Тази информация включва:

   а) информация относно броя на издадените заповеди за премахване и подадените сигнали, броя на материалите с терористично съдържание, които са били премахнати или достъпът до които е бил блокиран, включително съответните срокове съгласно членове 4 и 5;

б) информация относно конкретните проактивни мерки, предприети съгласно член 6, включително количеството терористично съдържание, което е било премахнато или достъпът до което е бил блокиран, и съответните срокове;

в) информация относно броя на започнатите процедури за подаване на жалби и действията, предприети от доставчиците на хостинг услуги съгласно член 10;

г) информация относно броя на започнатите процедури за правна защита и решенията, взети от компетентния орган в съответствие с националното законодателство.

2. Най-късно до [*една година от датата на прилагане на настоящия регламент*] Комисията изготвя подробна програма за мониторинг на крайните продукти, резултатите и въздействието на настоящия регламент. В програмата за мониторинг се определят показателите, средствата, чрез които се събират данните и другите необходими доказателства, и на какви интервали става това. В нея се посочват действията, които да бъдат предприети от Комисията и от държавите членки при събирането и анализирането на данните и другите доказателства с оглед на мониторинга на напредъка и на оценката на настоящия регламент съгласно член 23.

Член 22

Доклад за изпълнение

Най-късно до [*две години след влизането в сила на настоящия регламент*] Комисията докладва на Европейския парламент и на Съвета относно прилагането на настоящия регламент. В доклада на Комисията се вземат предвид информацията относно мониторинга съгласно член 21 и информацията, произтичаща от задълженията за прозрачност съгласно член 8. Държавите членки предоставят на Комисията информацията, необходима за изготвянето на доклада.

Член 23

Оценка

Не по-рано от [*три години от датата на прилагане на настоящия регламент*] Комисията извършва оценка на настоящия регламент и представя доклад на Европейския парламент и на Съвета относно прилагането на настоящия регламент, включително ефективността на предпазните механизми. Когато това е целесъобразно, докладът се придружава от законодателни предложения. Държавите членки предоставят на Комисията информацията, необходима за изготвянето на доклада.

Член 24

Влизане в сила

Настоящият регламент влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

Той се прилага от [***12*** […] месеца след влизането му в сила].

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*