Onsdagen den 17 april 2019

P8_TA(2019)0421

Förhindrande av spridning av terrorisminnehåll online ***I

Europaparlamentets lagstiftningsresolution av den 17 april 2019 om förslaget till Europaparlamentets och rådets förordning om förhindrande av spridning av terrorisminnehåll online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD))

(Ordinarie lagstiftningsförfarande: första behandlingen)

(2021/C 158/68)

Europaparlamentet utfärdar denna resolution

— med beaktande av kommissionens förslag till Europaparlamentet och rådet (COM(2018)0640),

— med beaktande av artiklarna 294.2 och 114 i fördraget om Europeiska unionens funktionssätt, i enlighet med vilka kommissionen har lagt fram sitt förslag för parlamentet (C8-0405/2018),

— med beaktande av artikel 294.3 i fördraget om Europeiska unionens funktionssätt,

— med beaktande av det motiverade yttrande från den tjeckiska deputeradekammaren som lagts fram i enlighet med protokoll nr 2 om tillämpning av subsidiaritets- och proportionalitetsprinciperna, och enligt vilket utkastet till lagstiftningsakt inte är förenligt med subsidiaritetsprincipen,

— med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande av den 12 december 2018 ([1]),

— med beaktande av artikel 59 i arbetsordningen,

— med beaktande av betänkandet från utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor och yttrandena från utskottet för kultur och utbildning och utskottet för den inre marknaden och konsumentskydd (A8-0193/2019).

1. Europaparlamentet antar nedanstående ståndpunkt vid första behandlingen.

2. Europaparlamentet uppmanar kommissionen att på nytt lägga fram ärendet för parlamentet om den ersätter, väsentligt ändrar eller har för avsikt att väsentligt ändra sitt förslag.

3. Europaparlamentet uppdrar åt talmannen att översända parlamentets ståndpunkt till rådet, kommissionen och de nationella parlamenten.

P8_TC1-COD(2018)0331

Europaparlamentets ståndpunkt fastställd vid första behandlingen den 17 april 2019 inför antagandet av Europaparlamentets och rådets förordning (EU) 2019/… om ~~förhindrande~~ *bekämpande* av spridning av terrorisminnehåll online [Ändr. 1]

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

([1]) EUT C 110, 22.3.2019, s. 67.

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Denna förordning syftar till att säkerställa att den digitala inre marknaden fungerar smidigt i ett öppet och demokratiskt samhälle, genom att ~~förhindra~~ ***motverka*** att värdtjänster missbrukas för terrorismändamål ***och bidra till den allmänna säkerheten i Europas samhällen***. Den digitala inre marknadens funktion bör förbättras genom att öka rättssäkerheten för värdtjänstleverantörer, stärka användarnas förtroende för onlinemiljön och förbättra skyddet för yttrandefriheten***, friheten att ta emot*** och ~~informationsfriheten~~ ***sprida uppgifter och tankar i ett öppet och demokratiskt samhälle samt mediernas frihet och mångfald***. **[Ändr. 2]**

(1a) Regleringen av värdtjänstleverantörer kan endast komplettera medlemsstaternas strategier för att ta itu med terrorism, som måste inriktas på åtgärder utanför nätet, såsom investeringar i socialt arbete, avradikaliseringsinitiativ och samarbete med berörda grupper för att uppnå ett hållbart förebyggande av radikalisering i samhället. **[Ändr. 3]**

(1b) Terrorisminnehåll är en del av ett bredare problem med olagligt innehåll online, vilket inbegriper andra typer av innehåll såsom sexuell exploatering av barn, olagliga affärsmetoder och överträdelser av immateriella rättigheter. Terroristorganisationer och andra kriminella organisationer ägnar sig ofta åt handel med olagligt innehåll för att tvätta och anskaffa såddpengar för att finansiera sin verksamhet. Detta problem kräver en kombination av lagstiftningsåtgärder samt icke-lagstiftningsåtgärder och frivilliga åtgärder, på grundval av samarbetet mellan myndigheter och leverantörer, med fullständig respekt för grundläggande rättigheter. Även om hotet från olagligt innehåll har mildrats genom framgångsrika initiativ såsom den industriledda uppförandekoden för att motverka olaglig hatpropaganda på nätet och initiativet WePROTECT Global Alliance to end child sexual abuse online, är det nödvändigt att inrätta en lagstiftningsram för gränsöverskridande samarbete mellan nationella tillsynsmyndigheter för att avlägsna olagligt innehåll. **[Ändr. 4]**

(2) Värdtjänstleverantörer som är aktiva på internet spelar en viktig roll i den digitala ekonomin genom att koppla samman företag och medborgare***, genom att tillhandahålla möjligheter till lärande*** samt genom att underlätta den offentliga debatten och spridningen och mottagandet av information, åsikter och idéer, vilket i hög grad bidrar till innovation, ekonomisk tillväxt och skapande av arbetstillfällen i unionen. Deras tjänster missbrukas dock i vissa fall av tredje part för att bedriva olaglig verksamhet på nätet. Särskilt oroande är att terroristgrupper och deras anhängare utnyttjar värdtjänsteleverantörer för att sprida terrorisminnehåll online i syfte att få ut sitt budskap, radikalisera och rekrytera samt att främja och styra terroristverksamhet. **[Ändr. 5]**

(3) ***Även om det inte är den enda faktorn, har*** förekomsten av terrorisminnehåll online ***visat sig vara en katalysator för radikaliseringen av personer som har begått terroristhandlingar, och*** har ***därför*** allvarliga negativa konsekvenser för användare, medborgare och samhället i stort samt för de tjänsteleverantörer som hyser sådant innehåll online, eftersom det undergräver användarnas förtroende och skadar deras affärsmodeller. Med tanke på onlinetjänsteleverantörernas centrala roll och ***i förhållande till*** de tekniska resurser och den tekniska kapacitet som förknippas med deras tjänster, har de ett särskilt samhällsansvar att skydda sina tjänster mot terroristmissbruk och ~~bidra till~~ ***hjälpa behöriga myndigheter*** att ~~förhindra att~~ ***bekämpa*** terrorisminnehåll ***som*** sprids via deras tjänster***, samtidigt som de tar hänsyn till den centrala betydelsen av yttrandefrihet och frihet att ta emot och sprida uppgifter och tankar i ett öppet och demokratiskt samhälle***. **[Ändr. 6]**

([1]) EUT C 110, 22.3.2019, s. 67.
([2]) Europaparlamentets och rådets ståndpunkt av den 17 april 2019.

Onsdagen den 17 april 2019

(4) Unionens insatser för att motverka terrorisminnehåll online inleddes 2015 genom en ram för frivilligt samarbete mellan medlemsstaterna och värdtjänstleverantörerna, som nu behöver kompletteras med en tydlig rättslig ram för att ytterligare minska tillgången till terrorisminnehåll online och på lämpligt sätt ta itu med ett snabbt växande problem. Avsikten med denna rättsliga ram är att bygga vidare på frivilliga insatser, som förstärktes genom kommissionens rekommendation (EU) 2018/334 ([3]), och tillmötesgå uppmaningarna från Europaparlamentet att vidta kraftigare åtgärder mot olagligt och skadligt innehåll ***i linje med den övergripande ram som fastställs genom direktiv 2000/31/EG*** och från Europeiska rådet att förbättra ~~den automatiska~~ upptäckten och raderingen av innehåll som uppviglar till terroristdåd. **[Ändr. 7]**

(5) Tillämpningen av denna förordning bör inte påverka tillämpningen av ~~artikel 14 i~~ direktiv 2000/31/EG ([4]). ~~I synnerhet bör inga åtgärder som en värdtjänstleverantör vidtar i enlighet med denna förordning, inte heller proaktiva åtgärder, i sig leda till att tjänsteleverantören förlorar möjligheten till det undantag från ansvarighet som föreskrivs i den artikeln.~~ Denna förordning påverkar inte de nationella myndigheternas och domstolarnas befogenheter att fastställa värdtjänstleverantörernas ansvar i specifika fall när villkoren för undantag från ansvarighet ~~i artikel 14~~ i direktiv 2000/31/EG inte är uppfyllda. **[Ändr. 8]**

(6) Regler för att ~~förhindra~~ ***motverka*** att värdtjänster missbrukas för spridning av terrorisminnehåll online anges i denna förordning i syfte att garantera att den inre marknaden fungerar smidigt, ~~med full respekt för~~ ***och de bör fullt ut respektera*** de grundläggande rättigheter som skyddas i unionens rättsordning och i synnerhet de som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna. **[Ändr. 9]**

(7) Denna förordning ~~bidrar~~ ***syftar till att bidra*** till att skydda den allmänna säkerheten, ~~samtidigt som~~ ***och bör fastställa*** lämpliga och stabila skyddsåtgärder ~~fastställs~~ för att säkerställa skyddet av de grundläggande rättigheter som berörs. Hit hör rätten till respekt för privatlivet och skydd av personuppgifter, rätten till ett effektivt rättsligt skydd, rätten till yttrandefrihet (inklusive friheten att ta emot och sprida uppgifter), näringsfriheten samt principen om icke-diskriminering. Behöriga myndigheter och värdtjänstleverantörer bör endast vidta åtgärder som är nödvändiga, lämpliga och proportionella i ett demokratiskt samhälle, med beaktande av den särskilda vikt som tillmäts yttrandefriheten och ~~informationsfriheten~~***, friheten att ta emot*** och ***sprida uppgifter och tankar***, ***rätten till skydd för privat- och familjeliv och rätten till skydd av personuppgifter*** som utgör en väsentlig grund för ett pluralistiskt, demokratiskt samhälle och är ~~ett av~~ unionens grundläggande värden. ***Man bör i samband med alla*** åtgärder ~~som utgör~~ ***undvika*** ingrepp i yttrandefriheten och informationsfriheten ~~bör vara strikt riktade, i den bemärkelsen att de måste~~ ***och åtgärderna bör*** i ***möjligaste mån*** tjäna till att ~~förhindra~~ ***bekämpa*** spridning av terrorisminnehåll ***genom en välriktad strategi***, men utan att därigenom påverka rätten att lagligen ta emot och sprida uppgifter, med beaktande av värdtjänstleverantörernas centrala roll i att främja offentlig debatt samt delande och mottagande av fakta, åsikter och idéer i enlighet med lagen. ***Verksamma åtgärder online för bekämpning av terrorism och skyddet av yttrandefriheten utgör inte motstridiga mål, utan är mål som kompletterar och ömsesidigt förstärker varandra.*** **[Ändr. 10]**

(8) Rätten till ett effektivt rättsmedel fastställs i artikel 19 i EU-fördraget och artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna. Varje fysisk eller juridisk person har rätt till ett effektivt rättsmedel inför behörig nationell domstol mot alla åtgärder som vidtas enligt denna förordning och som kan inverka negativt på den

([3]) Kommissionens rekommendation (EU) 2018/334 av den 1 mars 2018 om åtgärder för att effektivt bekämpa olagligt innehåll online (EUT L 63, 6.3.2018, s. 50).

([4]) Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”Direktiv om elektronisk handel”) (EGT L 178, 17.7.2000, s. 1).

personens rättigheter. Rätten inbegriper särskilt värdtjänstleverantörernas och innehållsleverantörernas möjlighet att effektivt bestrida avlägsnandeorder inför domstol i den medlemsstat vars myndigheter utfärdade avlägsnandeordern***, och innehållsleverantörernas möjlighet att bestrida de specifika åtgärder som vidtagits av värdtjänstleverantöre***. **[Ändr. 11]**

(9) För att ge klarhet om de åtgärder som både värdtjänstleverantörer och behöriga myndigheter bör vidta för att ~~förhindra~~ ***bekämpa*** spridning av terrorisminnehåll online, bör denna förordning innehålla en definition av terrorisminnehåll i förebyggande syfte vilken utgår från definitionen av terroristbrott i Europaparlamentets och rådets direktiv (EU) 2017/541 ([5]). Med tanke på behovet av att ~~motverka den~~ ***bekämpa det*** skadligaste ~~terroristpropagandan~~ ***terrorisminnehållet*** online bör definitionen omfatta material ~~och information~~ som uppviglar ~~till, uppmuntrar~~ eller ~~förespråkar~~ ***försöker värva till*** utförande av eller bidrag till terroristbrott, ~~ger instruktioner om utförande av sådana brott~~ eller ***som*** främjar deltagande i en terroristgrupps verksamhet ***och därigenom ger upphov till en risk för att ett eller flera sådana brott utförs uppsåtligen***. ***Definitionen bör också omfatta innehåll som ger vägledning för tillverkning och användning av sprängämnen, skjutvapen, alla andra vapen, skadliga eller farliga ämnen samt kemiska, biologiska, radiologiska och nukleära ämnen (CBRN-ämnen) och all vägledning om andra metoder och tekniker, bland annat val av mål i syfte att begå terroristbrott***. Sådan information inbegriper i synnerhet text, bilder, ljudupptagningar och videor. Vid bedömningen av huruvida innehåll utgör terrorisminnehåll i den mening som avses i denna förordning bör de behöriga myndigheterna och värdtjänstleverantörerna ta hänsyn till sådana faktorer som karaktären hos och formuleringen av uttalandena, i vilket sammanhang de gjordes samt deras potential att få skadliga konsekvenser och därigenom påverka människors säkerhet. Det faktum att materialet producerats av, kan tillskrivas eller sprids på uppdrag av en organisation eller person som är uppförd på EU:s terroristförteckning utgör en viktig faktor i bedömningen. Innehåll som sprids i utbildningssyfte, journalistiskt syfte eller forskningssyfte***, eller i syfte att höja medvetenheten om terroristverksamhet,*** bör skyddas på lämpligt sätt***. I synnerhet i fall då innehållsleverantören innehar ett redaktionellt ansvar bör man vid varje beslut angående avlägsnande av det spridda materialet ta hänsyn till de publicistiska normer som fastställts genom press- eller medieregleringen och som överensstämmer med unionens lagstiftning och stadgan om de grundläggande rättigheterna***. Dessutom bör det gå att uttrycka radikala, polemiska eller kontroversiella åsikter i den offentliga debatten om känsliga politiska frågor utan att detta ska anses vara terrorisminnehåll. **[Ändr. 12]**

(10) För att omfatta de onlinevärdtjänster där terrorisminnehåll sprids, bör denna förordning tillämpas på informationssamhällets tjänster som på begäran av en tjänstemottagare lagrar information som tillhandahållits av denna tjänstemottagare och gör den lagrade informationen tillgänglig för ~~tredje part~~ ***allmänheten***, oavsett om denna verksamhet är av rent teknisk, automatisk och passiv karaktär. Sådana leverantörer av informationssamhällets tjänster är till exempel sociala medieplattformar, direktuppspelningstjänster, video-, bild- och ljuddelningstjänster, fildelningstjänster och andra molntjänster i den mån som de gör informationen tillgänglig för ~~tredje part~~ ***allmänheten*** samt webbplatser där användarna kan kommentera eller lägga upp recensioner. Förordningen bör också tillämpas på värdtjänstleverantörer som är etablerade utanför unionen men erbjuder tjänster inom unionen, eftersom en betydande andel av de värdtjänstleverantörer som är utsatta för terrorisminnehåll på sina tjänster är etablerade i tredjeländer. Detta bör säkerställa att alla företag som är verksamma på den digitala inre marknaden uppfyller samma krav, oavsett etableringsland. För att fastställa om en tjänsteleverantör erbjuder tjänster i unionen krävs en bedömning av huruvida tjänsteleverantören gör det möjligt för juridiska eller fysiska personer i en eller flera medlemsstater att använda dess tjänster. Enbart det faktum att en tjänsteleverantörs webbplats, e-postadress och andra kontaktuppgifter är tillgängliga i en eller flera medlemsstater bör dock inte i sig vara tillräckligt för att denna förordning ska kunna tillämpas. ***Den bör inte tillämpas på molntjänster, inklusive molntjänster mellan företag, där tjänsteleverantören inte har några kontraktsenliga rättigheter beträffande vilket innehåll som lagras eller hur***

([5]) Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017, s. 6).

Onsdagen den 17 april 2019

det behandlas eller görs offentligt tillgängligt av dess kunder eller av sådana kunders slutanvändare, och där tjänsteleverantören inte har någon teknisk kapacitet att avlägsna specifikt innehåll som lagras av dess kunder eller tjänsternas slutanvändare. **[Ändr. 13]**

(11) En betydande anknytning till unionen bör vara relevant för att fastställa tillämpningsområdet för denna förordning. En sådan betydande anknytning till unionen bör anses föreligga om tjänsteleverantören har ett verksamhetsställe i unionen eller, i brist på det, på grundval av att det finns ett betydande antal användare i en eller flera medlemsstater eller att verksamheten riktas till en eller flera medlemsstater. Huruvida verksamheten är riktad till en eller flera medlemsstater kan avgöras på grundval av alla relevanta omständigheter, t.ex. faktorer som användning av ett språk eller en valuta som i allmänhet används i den medlemsstaten~~, eller möjligheten att beställa varor eller tjänster~~. Verksamheten kan även anses vara riktad till en medlemsstat om en app finns tillgänglig i den berörda nationella appbutiken, om lokal marknadsföring eller reklam görs på det språk som används i medlemsstaten eller om kundkontakter, t.ex. kundtjänst, sköts på det språk som vanligen används i den medlemsstaten. En betydande anknytning bör också antas föreligga om en tjänsteleverantör riktar sin verksamhet till en eller flera medlemsstater i den mening som avses i artikel 17.1 c i Europaparlamentets och rådets förordning (EU) nr 1215/2012 ([6]). Däremot kan det inte enbart på grund av att en tjänst tillhandahålls för att efterleva det förbud mot diskriminering som fastställs i Europaparlamentets och rådets förordning (EU) 2018/302 ([7]) anses att verksamheten riktas till ett visst territorium inom unionen. **[Ändr. 14]**

(12) Värdtjänstleverantörer bör följa vissa aktsamhetskrav för att ~~förhindra~~ ***motverka*** att terrorisminnehåll sprids på deras tjänster ***till allmänheten***. Dessa aktsamhetskrav bör inte utgöra en allmän ~~övervakningsskyldighet~~ ***skyldighet för värdtjänstleverantörer att övervaka den information de lagrar, och inte heller någon allmän skyldighet att aktivt efterforska fakta eller omständigheter som tyder på olaglig verksamhet***. Aktsamhetskraven bör omfatta att värdtjänstleverantörer, när de tillämpar denna förordning, agerar på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt med avseende på innehåll som de lagrar, i synnerhet när de tillämpar sina egna användarvillkor, i syfte att undvika att innehåll som inte är terrorisminnehåll avlägsnas. När innehåll avlägsnas eller görs oåtkomligt måste det ske med hänsyn till yttrandefriheten***, friheten att ta emot*** och ~~informationsfriheten~~ ***sprida uppgifter och tankar i ett öppet och demokratiskt samhälle samt mediernas frihet och mångfald***. **[Ändr. 15]**

(13) En harmonisering bör ske av förfarandet för och de skyldigheter som följer av ~~rättsliga beslut~~ ***avlägsnandeorder*** som ålägger värdtjänstleverantörer att avlägsna terrorisminnehåll eller göra det oåtkomligt efter en bedömning av de behöriga myndigheterna. Medlemsstaterna bör ha fortsatt frihet att välja de behöriga myndigheterna, så att de kan utse ~~administrativa,~~ ***en rättslig myndighet eller en funktionellt oberoende administrativ eller*** brottsbekämpande ~~eller rättsliga myndigheter~~ ***myndighet*** för denna uppgift. Med tanke på hur snabbt terrorisminnehåll sprids via onlinetjänster åläggs värdtjänstleverantörerna i denna förordning skyldigheter att säkerställa att det terrorisminnehåll som anges i avlägsnandeordern avlägsnas eller görs oåtkomligt inom en timme från mottagandet av avlägsnandeordern. ~~Det är upp till värdtjänstleverantörerna att besluta om de ska avlägsna innehållet i fråga eller göra det oåtkomligt för användarna i unionen.~~ **[Ändr. 16]**

(14) Den behöriga myndigheten bör översända avlägsnandeordern direkt till ~~mottagaren~~ ***värdtjänstleverantörens kontaktpunkt*** och ~~kontaktpunkten~~***, om värdtjänstleverantörens huvudsakliga verksamhetsställe är i en annan medlemsstat, till den behöriga myndigheten i den medlemsstaten*** på ett elektroniskt sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar för tjänsteleverantören att säkerställa autentisering – även att datum och tidpunkt för sändandet och mottagandet av ordern är korrekt – såsom genom säkrad e-post, säkrade

([6]) Europaparlamentets och rådets förordning (EU) nr 1215/2012 av den 12 december 2012 om domstols behörighet och om erkännande och verkställighet av domar på privaträttens område (EUT L 351, 20.12.2012, s. 1).

([7]) Europaparlamentets och rådets förordning (EU) 2018/302 av den 28 februari 2018 om åtgärder mot omotiverad geoblockering och andra former av diskriminering på grund av kunders nationalitet, bosättningsort eller etableringsort på den inre marknaden och om ändring av förordningarna (EG) nr 2006/2004 och (EU) 2017/2394 samt direktiv 2009/22/EG (EUT L 601, 2.3.2018, s. 1).

plattformar eller andra säkra kanaler, även sådana som tillhandahålls av tjänsteleverantören, i enlighet med reglerna om skydd av personuppgifter. Detta krav kan särskilt uppfyllas genom användning av en kvalificerad elektronisk tjänst för rekommenderad leverans i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 ([8]). **[Ändr. 17]**

~~(15) Anmälningar från de behöriga myndigheterna eller Europol utgör ett effektivt och snabbt sätt att göra värdtjänstleverantörer medvetna om specifikt innehåll på deras tjänster. Denna mekanism för att uppmärksamma värdtjänstleverantörer på information som kan anses vara terrorisminnehåll, så att de på frivillig basis kan bedöma om innehållet är förenligt med de egna användarvillkoren, bör förbli tillgänglig vid sidan av avlägsnandeorder. Det är viktigt att värdtjänstleverantörer bedömer dessa anmälningar som en prioriterad fråga och ger snabb återkoppling om de åtgärder som vidtagits. Det är fortsättningsvis värdtjänstleverantören som fattar det slutliga beslutet om huruvida innehållet ska avlägsnas eftersom det inte är förenligt med användarvillkoren. Europols mandat som fastställs i förordning (EU) 2016/794 ([9]) påverkas inte av tillämpningen av denna förordning när det gäller anmälningar.~~ **[Ändr. 18]**

(16) Med tanke på terrorisminnehållets omfattning och den snabbhet som krävs för att effektivt identifiera och avlägsna det, är proportionella ~~proaktiva~~ ***specifika*** åtgärder~~, även användning av automatiska metoder i vissa fall,~~ en avgörande del i bekämpandet av terrorisminnehåll online. I syfte att minska tillgången till terrorisminnehåll på värdtjänstleverantörernas tjänster, bör de bedöma om det är lämpligt att vidta ~~proaktiva~~ ***specifika*** åtgärder beroende på riskerna för och graden av utsatthet för terrorisminnehåll, samt inverkan på tredje parters rättigheter och allmänhetens intresse av ~~information~~ ***att ta emot och sprida uppgifter, särskilt då de utsätts för terrorisminnehåll och mottar avlägsnandeorder i betydande omfattning***. Därför bör värdtjänstleverantörer fastställa vilken lämplig, ***riktad,*** effektiv och proportionell ~~proaktiv~~ ***specifik*** åtgärd som bör vidtas. Detta krav bör inte innebära någon allmän övervakningsskyldighet. ***Dessa specifika åtgärder kan inbegripa regelbunden rapportering till de behöriga myndigheterna, utökning av personal som arbetar med åtgärder för att skydda tjänsterna mot offentlig spridning av terrorisminnehåll samt utbyte av bästa praxis.*** I samband med denna bedömning är det ett tecken på en låg nivå av utsatthet för terrorisminnehåll om inga avlägsnandeorder ~~och anmälningar~~ har riktats till värdtjänstleverantören. **[Ändr. 19]**

(17) När ~~proaktiva~~ ***specifika*** åtgärder införs bör värdtjänstleverantörer säkerställa att användarnas rätt till yttrandefrihet och ~~informationsfrihet – inklusive friheten~~ ***frihet*** att ta emot och sprida uppgifter – ***och tankar i ett öppet och demokratiskt samhälle*** bibehålls. Utöver de krav som fastställs i lagstiftning, även lagstiftningen om skydd av personuppgifter, bör värdtjänstleverantörer agera med vederbörlig omsorg och vidta skyddsåtgärder, framför allt mänsklig tillsyn och kontroll~~, när så är lämpligt,~~ för att undvika oavsiktliga och felaktiga beslut som leder till att innehåll som inte är terrorisminnehåll avlägsnas. ~~Detta är särskilt relevant när värdtjänstleverantörerna använder automatiska metoder för att upptäcka terrorisminnehåll. Beslut om att använda automatiska metoder, oavsett om de fattats av värdtjänstleverantören själv eller efter en begäran från den behöriga myndigheten, bör bedömas med hänsyn till den underliggande teknikens tillförlitlighet och den resulterande inverkan på de grundläggande rättigheterna.~~ **[Ändr. 20]**

(18) För att säkerställa att de värdtjänstleverantörer som utsätts för terrorisminnehåll vidtar lämpliga åtgärder för att förhindra att deras tjänster missbrukas, bör ~~de~~ ***den*** behöriga ~~myndigheterna~~ ***myndigheten*** begära att värdtjänstleverantörer som har mottagit ~~en~~ ***ett betydande antal*** avlägsnandeorder som vunnit laga kraft rapporterar om vilka ~~proaktiva~~ åtgärder som vidtagits. ~~Dessa kan bestå av åtgärder för att förhindra att terrorisminnehåll som avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder eller en anmälan laddas upp på nytt, genom en kontroll mot offentliga eller privata verktyg som omfattar känt terrorisminnehåll.~~ De får också använda tillförlitliga tekniska verktyg för att identifiera nytt terrorisminnehåll~~, antingen sådana som finns tillgängliga på marknaden eller sådana~~

([8]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

~~([9]) Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).~~

~~som värdtjänstleverantören har utvecklat~~. Tjänsteleverantören bör rapportera om de specifika ~~proaktiva~~ åtgärder som vidtagits för att göra det möjligt för den behöriga myndigheten att bedöma om åtgärderna är ***nödvändiga,*** effektiva och proportionella och, om automatiska metoder används, huruvida värdtjänstleverantören har de nödvändiga förutsättningarna för mänsklig tillsyn och kontroll. Vid bedömningen av åtgärdernas effektivitet***, nödvändighet*** och proportionalitet bör de behöriga myndigheterna beakta relevanta parametrar såsom antalet avlägsnandeorder ~~och anmälningar~~ som utfärdats till leverantören, dess ***storlek och*** ekonomiska kapacitet och tjänstens inverkan på spridningen av terrorisminnehåll (t.ex. med beaktande av antalet användare i unionen)***, såväl som de skyddsåtgärder som införts för att skydda yttrandefriheten och informationsfriheten samt antalet fall av begränsning av lagligt innehåll***. **[Ändr. 21]**

(19) Efter begäran bör den behöriga myndigheten inleda en dialog med värdtjänstleverantören om de nödvändiga ~~proaktiva~~ ***specifika*** åtgärder som ska vidtas. Vid behov bör den behöriga myndigheten ~~föreskriva~~ ***begära att värdtjänstleverantören på nytt utvärderar vilka åtgärder som krävs eller begära*** antagande av lämpliga, effektiva och proportionella ~~proaktiva~~ ***specifika*** åtgärder om den anser att de åtgärder som vidtagits inte ***följer nödvändighets- och proportionalitetsprinciperna eller inte*** är tillräckliga för att hantera riskerna. ~~Ett beslut att föreskriva~~ ***Den behöriga myndigheten bör endast begära specifika åtgärder som värdtjänstleverantören rimligen kan förväntas genomföra, med beaktande av faktorer som exempelvis värdtjänstleverantörens finansiella och andra resurser. En begäran om att genomföra*** sådana specifika ~~proaktiva~~ åtgärder bör ~~i princip~~ inte leda till införandet av en allmän övervakningsskyldighet i den mening som avses i artikel 15.1 i direktiv 2000/31/EG. ~~Med tanke på de särskilt allvarliga risker som är förknippade med spridningen av terrorisminnehåll, kan de beslut som fattas av de behöriga myndigheterna på grundval av denna förordning avvika från den metod som fastställs i artikel 15.1 i direktiv 2000/31/EG när det gäller vissa specifika, riktade åtgärder som antas av tvingande hänsyn till allmän säkerhet. Innan den behöriga myndigheten fattar sådana beslut bör den finna rätt balans mellan hänsyn till allmän säkerhet och de berörda grundläggande rättigheterna, framför allt yttrandefriheten, informationsfriheten och näringsfriheten, samt lämna en lämplig motivering.~~ **[Ändr. 22]**

(20) Värdtjänstleverantörernas skyldighet att bevara avlägsnat innehåll och relaterade data bör fastställas för specifika ändamål och tidsbegränsas till den period som är nödvändig. Det finns ett behov av att utvidga bevarandekravet till relaterade data i den mån sådana data annars skulle gå förlorade till följd av att det berörda innehållet avlägsnades. Relaterade data kan omfatta data såsom ”abonnentdata”, ~~t.ex.~~ ***särskilt*** uppgifter om innehållsleverantörens identitet, och ”åtkomstdata”, t.ex. uppgifter om datum och tidpunkt för innehållsleverantörens användning av eller inloggning till och utloggning från tjänsten, tillsammans med den ip-adress som internetleverantören har tilldelat innehållsleverantören. **[Ändr. 23]**

(21) Skyldigheten att bevara innehållet för administrativa eller rättsliga ~~prövningsförfaranden~~ ***förfaranden för prövning eller överklagande*** är nödvändig och motiverad för att säkerställa effektiv prövning för den innehållsleverantör vars innehåll har avlägsnats eller gjorts oåtkomligt samt för att säkerställa att innehållet kan återställas i samma skick beroende på resultatet av prövningsförfarandet. Skyldigheten att bevara innehåll för utrednings- och lagförings-ändamål är motiverad och nödvändig med tanke på det värde som detta material kan tillföra för att störa eller förhindra terroristverksamhet. Om företag avlägsnar material eller gör det oåtkomligt, ~~i synnerhet~~ genom egna ~~proaktiva~~ ***specifika*** åtgärder, ~~och inte informerar den berörda myndigheten eftersom de bedömer att det inte omfattas av artikel 13.4 i denna förordning, kan~~ ***bör de omgående informera*** de ***behöriga*** brottsbekämpande myndigheterna ~~vara omedvetna om att innehållet existerar. Därför~~ ***Det*** är ~~det~~ också motiverat att bevara innehåll för att förebygga, upptäcka, utreda och lagföra terroristbrott. För dessa ändamål ***bör terrorisminnehållet och relaterade data endast lagras under en viss period så att de brottsbekämpande myndigheterna kan kontrollera innehållet och besluta om det skulle behövas för dessa specifika ändamål. Perioden bör inte överstiga sex månader. För förebyggande, upptäckt, utredning och lagföring av terroristbrott*** är kravet på att bevara data begränsat till data som sannolikt har samband med terroristbrott och därmed kan bidra till att lagföra terroristbrott eller förhindra allvarliga risker för den allmänna säkerheten. **[Ändr. 24]**

(22) För att säkerställa proportionalitet bör perioden för bevarande vara begränsad till sex månader så att innehållsleverantörerna får tillräckligt med tid för att inleda prövningsförfarandet ~~och~~ ***eller*** så att brottsbekämpande myndigheter ska kunna få åtkomst till relevanta data för utredning och lagföring av terroristbrott. Denna period kan

dock förlängas med den tid som är nödvändig om ~~prövningsförfaranden~~ ***förfaranden för prövning eller överklagande*** inleds men inte avslutas inom sexmånadersperioden, på begäran av den myndighet som genomför prövningen. Denna period bör ***också*** vara tillräcklig för att de brottsbekämpande myndigheterna ska kunna bevara ~~bevis~~ ***material*** som är ~~nödvändiga~~ ***nödvändigt*** för utredningar ***och straffrättsliga förfaranden***, samtidigt som balansen i förhållande till de berörda grundläggande rättigheterna säkerställs. **[Ändr. 25]**

(23) Denna förordning påverkar inte de procedurgarantier och processuella utredningsåtgärder som rör åtkomst till innehåll och relaterade data som bevarats för att utreda och lagföra terroristbrott, vilka fastställs i medlemsstaternas nationella lagstiftning och unionslagstiftningen.

(24) Transparens i värdtjänstleverantörernas strategier för terrorisminnehåll är avgörande för att öka deras ansvarighet gentemot användarna och stärka medborgarnas förtroende för den digitala inre marknaden. ***Endast*** värdtjänstleverantörer ***som under det relevanta året är föremål för avlägsnandeorder*** bör ***vara skyldiga att*** offentliggöra årliga transparensrapporter som innehåller meningsfull information om åtgärder som vidtagits för att upptäcka, identifiera och avlägsna terrorisminnehåll. **[Ändr. 26]**

(24a) De myndigheter som är behöriga att utfärda avlägsnandeorder bör också offentliggöra transparensrapporter som innehåller information om antalet avlägsnandeorder, antalet nekade order, antalet fall med identifierat terrorisminnehåll som lett till utredning och lagföring samt antalet fall då innehåll felaktigt identifierats som terrorisminnehåll. **[Ändr. 27]**

(25) Klagomålsförfaranden utgör en nödvändig skyddsåtgärd mot felaktigt avlägsnande av innehåll som är skyddat genom yttrandefriheten och ~~informationsfriheten~~ ***friheten att ta emot och sprida uppgifter och tankar i ett öppet och demokratiskt samhälle***. Värdtjänstleverantörer bör därför upprätta användarvänliga klagomålsmekanismer och säkerställa att klagomål hanteras snabbt och med full transparens gentemot innehållsleverantören. Kravet på att värdtjänstleverantören ska återställa innehållet om det har avlägsnats felaktigt påverkar inte värdtjänstleverantörernas möjlighet att genomdriva sina egna användarvillkor på andra grunder. **[Ändr. 28]**

(26) För ett effektivt rättsligt skydd enligt artikel 19 i EU-fördraget och artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna krävs att personer ska kunna utröna av vilka orsaker det innehåll de laddat upp har avlägsnats eller gjorts oåtkomligt. För detta ändamål bör värdtjänstleverantören tillhandahålla innehållsleverantören meningsfull information ~~som~~ ***såsom orsakerna till att innehållet avlägsnades eller gjordes oåtkomligt, och den rättsliga grunden för åtgärden, vilket*** gör det möjligt för innehållsleverantören att bestrida beslutet. ~~Detta kräver dock inte nödvändigtvis en underrättelse till innehållsleverantören.~~ Beroende på omständigheterna kan värdtjänstleverantörer ersätta innehåll som anses vara terrorisminnehåll med ett meddelande om att det har avlägsnats eller gjorts oåtkomligt i enlighet med denna förordning. ~~Ytterligare information om orsakerna och innehållsleverantörens möjligheter att bestrida beslutet bör ges på begäran.~~ Om de behöriga myndigheterna beslutar att det av hänsyn till allmän säkerhet, t.ex. inom ramen för en utredning, är olämpligt eller kontraproduktivt att direkt underrätta innehållsleverantören om att innehåll har avlägsnats eller gjorts oåtkomligt, bör de informera värdtjänstleverantören. **[Ändr. 29]**

(27) För att undvika dubbelarbete och möjlig störning av utredningar ***samt minimera kostnaderna för berörda värdtjänstleverantörer***, bör de behöriga myndigheterna informera, samordna sig med och samarbeta med varandra och Europol, när så är lämpligt, när de utfärdar avlägsnandeorder ~~eller anmäler innehåll~~ till värdtjänstleverantörer. Vid genomförandet av bestämmelserna i denna förordning kan Europol tillhandahålla stöd i enlighet med dess nuvarande mandat och befintliga rättsliga ram. **[Ändr. 30]**

(27a) Anmälningar från Europol utgör ett effektivt och snabbt sätt att göra värdtjänstleverantörer medvetna om specifikt innehåll på deras tjänster. Denna mekanism för att uppmärksamma värdtjänstleverantörer på

information som kan anses vara terrorisminnehåll, så att de på frivillig basis kan bedöma om innehållet är förenligt med de egna användarvillkoren, bör förbli tillgänglig vid sidan av avlägsnandeorder. Därför är det viktigt att värdtjänstleverantörer samarbetar med Europol och bedömer Europols anmälningar som en prioriterad fråga och ger snabb återkoppling om de åtgärder som vidtagits. Det är fortsättningsvis värdtjänstleverantören som fattar det slutliga beslutet om huruvida innehållet ska avlägsnas eftersom det inte är förenligt med användarvillkoren. Europols mandat som fastställs i förordning (EU) 2016/794 ([10]) påverkas inte av tillämpningen av denna förordning. **[Ändr. 31]**

(28) I syfte att säkerställa ett effektivt och tillräckligt enhetligt genomförande av ~~proaktiva~~ åtgärder ***från värdtjänstleverantörernas sida*** bör de behöriga myndigheterna i medlemsstaterna samarbeta med varandra i fråga om de diskussioner de har med värdtjänstleverantörerna avseende ***avlägsnandeorder samt*** identifiering, genomförande och bedömning av specifika ~~proaktiva~~ åtgärder. Ett sådant samarbete behövs också i samband med antagandet av regler om påföljder, samt genomförandet och verkställandet av påföljderna. **[Ändr. 32]**

(29) Det är viktigt att den behöriga myndigheten i den medlemsstat som är ansvarig för att utdöma påföljder är fullständigt informerad om utfärdandet av avlägsnandeorder och ~~anmälningar samt~~ efterföljande utbyten mellan värdtjänstleverantören och ~~den~~ ***de*** relevanta behöriga ~~myndigheten~~ ***myndigheterna i andra medlemsstater***. För detta ändamål bör medlemsstaterna säkerställa lämpliga ***och säkra*** kommunikationskanaler och mekanismer som gör det möjligt att dela den relevanta informationen i rätt tid. **[Ändr. 33]**

(30) För att underlätta ett snabbt utbyte mellan behöriga myndigheter och värdtjänstleverantörer, och för att undvika dubbelarbete, får medlemsstaterna använda sig av de verktyg som utvecklats av Europol, såsom den befintliga *Internet Referral Management application* (IRMa) eller efterföljare till detta verktyg.

(31) Med tanke på de särskilt allvarliga konsekvenserna av visst terrorisminnehåll, bör värdtjänstleverantörer omgående informera myndigheterna i den berörda medlemsstaten eller de behöriga myndigheterna där de är etablerade eller har en rättslig företrädare om förekomsten av bevis för terroristbrott som de får kännedom om. För att säkerställa proportionalitet är denna skyldighet begränsad till terroristbrott enligt definitionen i artikel 3.1 i direktiv (EU) 2017/541. Informationsskyldigheten innebär inte att värdtjänstleverantörer är skyldiga att aktivt söka sådana bevis. Den berörda medlemsstaten är den medlemsstat som har jurisdiktion över utredning och lagföring av terroristbrott enligt direktiv (EU) 2017/541 på grundval av gärningsmannens eller det potentiella brottsoffrets nationalitet eller målplatsen för terroristdådet. I tveksamma fall får värdtjänstleverantörer överföra informationen till Europol som bör följa upp den i enlighet med sitt mandat, t.ex. genom att vidarebefordra den till de relevanta nationella myndigheterna.

(32) De behöriga myndigheterna i medlemsstaterna bör ha rätt att använda sådan information för att vidta utredningsåtgärder som föreskrivs i medlemsstaternas eller unionens lagstiftning, även att utfärda en europeisk utlämnandeorder enligt förordningen om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden ([11]).

(33) Både värdtjänstleverantörer och medlemsstaterna bör upprätta kontaktpunkter för att underlätta en snabb handläggning av avlägsnandeorder ~~och anmälningar~~. I motsats till den rättsliga företrädaren tjänar kontaktpunkten operativa syften. Värdtjänstleverantörens kontaktpunkt bör bestå av någon typ av särskilda medel som möjliggör elektronisk inlämning av avlägsnandeorder ~~och anmälningar~~ och av tekniska resurser och personalresurser som möjliggör snabb handläggning av dem. Värdtjänstleverantörens kontaktpunkt måste inte vara belägen i unionen, och värdtjänstleverantören är fri att utse en befintlig kontaktpunkt, under förutsättning att denna kontaktpunkt klarar av att fullgöra de funktioner som föreskrivs i denna förordning. I syfte att säkerställa att terrorisminnehåll avlägsnas eller görs oåtkomligt inom en timme från mottagandet av en avlägsnandeorder, bör värdtjänstleverantörerna säkerställa att kontaktpunkten kan nås dygnet runt varje dag. Informationen om kontaktpunkten bör inbegripa information om vilket språk kontaktpunkten kan kontaktas på. För att underlätta kommunikationen mellan

---

([10]) Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).

([11]) COM(2018)0225.

värdtjänstleverantörerna och de behöriga myndigheterna, uppmuntras värdtjänstleverantörer att tillåta kommunikation på ett av unionens officiella språk som deras användarvillkor finns tillgängliga på. **[Ändr. 34]**

(34) Då det inte finns något allmänt krav på att tjänsteleverantörer måste säkerställa fysisk närvaro på unionens territorium, finns det ett behov av att säkerställa klarhet om vilken medlemsstats jurisdiktion den värdtjänstleverantör som erbjuder tjänster inom unionen omfattas av. Som en allmän regel omfattas värdtjänstleverantören av jurisdiktionen i den medlemsstat där den har sitt huvudsakliga verksamhetsställe eller där den har utsett en rättslig företrädare. ~~Om en annan medlemsstat utfärdar en avlägsnandeorder bör det dock vara möjligt för dess myndigheter att genomdriva sin order genom att vidta tvångsåtgärder av en icke-bestraffande karaktär, såsom vite.~~ När det gäller en värdtjänstleverantör som inte har något verksamhetsställe i unionen och som inte utser en rättslig företrädare, bör alla medlemsstater ändå kunna utdöma påföljder, under förutsättning att principen *ne bis in idem* följs. **[Ändr. 35]**

(35) Värdtjänstleverantörer som inte är etablerade i unionen bör skriftligen utse en rättslig företrädare för att säkerställa att skyldigheterna enligt denna förordning efterlevs och verkställs. ***Värdtjänstleverantörer får använda sig av en befintlig rättslig företrädare, under förutsättning att denna rättsliga företrädare kan fullgöra de funktioner som anges i denna förordning.*** **[Ändr. 36]**

(36) Den rättsliga företrädaren bör ha rättslig befogenhet att agera på värdtjänstleverantörens vägnar.

(37) Medlemsstaterna bör utse ~~behöriga myndigheter~~ ***en enda rättslig eller funktionellt oberoende administrativ myndighet*** för tillämpningen av denna förordning. ~~Kravet på att utse behöriga myndigheter~~ ***Detta krav*** förutsätter inte ~~nödvändigtvis att nya myndigheter~~ ***att en ny myndighet*** inrättas, utan ~~de~~ ***det*** kan vara ~~befintliga~~ ***ett befintligt*** organ som ges i uppdrag att sköta de funktioner som anges i denna förordning. Denna förordning kräver att det utses ~~myndigheter~~ ***en myndighet*** som ska vara ~~behöriga~~ ***behörig*** att utfärda avlägsnandeorder ~~och anmälningar~~, övervaka ~~proaktiva~~ ***specifika*** åtgärder och fastställa påföljder. ~~Det är upp till~~ Medlemsstaterna ~~att bestämma hur många myndigheter de vill utse för dessa uppgifter~~ ***bör underrätta kommissionen om den behöriga myndighet som utsetts enligt denna förordning, och kommissionen bör offentliggöra en sammanställning online av de behöriga myndigheterna i varje medlemsstat. Onlineregistret bör vara lättillgängligt så att värdtjänstleverantörerna snabbt kan kontrollera att avlägsnandeordern är autentisk***. **[Ändr. 37]**

(38) Påföljder är nödvändiga för att säkerställa att värdtjänstleverantörerna effektivt genomför sina skyldigheter enligt denna förordning. Medlemsstaterna bör anta bestämmelser om påföljder, även riktlinjer för bötfällning när så är lämpligt. ~~Särskilt stränga~~ Påföljder ~~ska~~ ***bör*** fastställas om ~~värdtjänstleverantören~~ ***värdtjänstleverantörerna*** systematiskt ***och ständigt*** underlåter att ~~avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme från mottagandet av en avlägsnandeorder. Bristande efterlevnad i enskilda fall kan leda till påföljder, med respekt för principen *ne bis in idem* och proportionalitetsprincipen, samt med säkerställande av att påföljderna utdöms med beaktande av systematisk underlåtenhet. För att säkerställa rättssäkerhet bör det i förordningen anges i vilken utsträckning de relevanta skyldigheterna kan bli föremål för påföljder~~ ***fullgöra sina skyldigheter enligt denna förordning***. Påföljder för bristande efterlevnad av artikel 6 bör endast tillämpas i fråga om skyldigheter som följer av en begäran om ~~rapportering enligt artikel 6.2 eller ett beslut om införande~~ ***genomförande*** av ytterligare ~~proaktiva~~ ***specifika*** åtgärder enligt artikel 6.4. Vid fastställande av huruvida böter bör föreskrivas, bör vederbörlig hänsyn tas till leverantörens ekonomiska resurser. ***Den behöriga myndigheten bör dessutom ta hänsyn till om värdtjänstleverantören är ett nystartat företag eller ett litet eller medelstort företag och avgöra från fall till fall om företaget haft förmåga att på lämpligt sätt följa den utfärdade ordern.*** Medlemsstaterna ska säkerställa att påföljderna inte uppmuntrar till avlägsnande av innehåll som inte är terrorisminnehåll. **[Ändr. 38]**

(39) Användningen av standardiserade mallar underlättar samarbete och informationsutbyte mellan behöriga myndigheter och tjänsteleverantörer, och gör det möjligt för dem att kommunicera snabbare och mer effektivt. Det är särskilt viktigt att säkerställa snabba åtgärder efter mottagandet av en avlägsnandeorder. Mallarna minskar översättningskostnaderna och bidrar till en hög kvalitetsstandard. Svarsformulär bör också möjliggöra ett standardiserat informationsutbyte, vilket är särskilt viktigt om tjänsteleverantörerna inte kan följa ordern.

Autentiserade inlämningskanaler kan garantera att avlägsnandeordern är autentisk, liksom att datum och tidpunkt för sändande och mottagande av ordern är korrekt.

(40) För att vid behov möjliggöra snabba ändringar av innehållet i de mallar som ska användas vid tillämpningen av denna förordning, bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt delegeras till kommissionen med avseende på ändringar av bilagorna I, II och III till denna förordning. För att kunna ta hänsyn till den tekniska utvecklingen och utvecklingen av den relaterade rättsliga ramen, bör kommissionen också ges befogenhet att anta delegerade akter för att komplettera denna förordning med tekniska krav på de elektroniska medel som de behöriga myndigheterna ska använda för att översända avlägsnandeorder. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([12]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(41) Medlemsstaterna bör samla in information om genomförandet av lagstiftningen***, inbegripet information om antalet fall av framgångsrik upptäckt, utredning och lagföring av terroristbrott som en följd av denna förordning***. Ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter bör fastställas som underlag för en utvärdering av lagstiftningen. **[Ändr. 39]**

(42) På grundval av resultaten och slutsatserna i genomföranderapporten och resultaten av övervakningen bör kommissionen genomföra en utvärdering av denna förordning ~~tidigast tre~~ ***ett*** år efter dess ikraftträdande. Utvärderingen bör bygga på de ~~fem~~ ***sju*** kriterierna effektivitet, ***nödvändighet, proportionalitet,*** ändamålsenlighet, relevans, samstämmighet och mervärde för EU. Man ~~kommer att~~ ***bör*** bedöma hur de olika operativa och tekniska åtgärder som föreskrivs i denna förordning fungerar, bland annat effektiviteten i de åtgärder som ska förbättra upptäckt, identifiering och avlägsnande av terrorisminnehåll, skyddsmekanismernas effektivitet samt inverkan på tredje parts potentiellt påverkade ~~rättigheter och~~ ***grundläggande rättigheter, bland annat yttrandefriheten och friheten att ta emot och sprida uppgifter, mediernas frihet och mångfald, näringsfriheten och rätten till integritet och skydd av personuppgifter. Kommissionen bör också bedöma inverkan på*** intressen, inklusive en översyn av kravet på att informera innehållsleverantörerna. **[Ändr. 42]**

(43) Eftersom målet för denna förordning, nämligen att säkerställa att den digitala inre marknaden fungerar smidigt genom att förhindra spridning av terrorisminnehåll online, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och därför, på grund av begränsningens omfattning och verkningar, bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVSNITT I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. I denna förordning fastställs ***riktade*** enhetliga regler för att ~~förhindra att~~ ***bekämpa missbruk av*** värdtjänster ~~missbrukas~~ för ***offentlig*** spridning av terrorisminnehåll online. Här fastställs i synnerhet följande: **[Ändr. 41]**

([12]) EUT L 123, 12.5.2016, s. 1.

a) Regler om ***rimliga och proportionella*** aktsamhetskrav som värdtjänstleverantörer ska iaktta för att ~~förhindra~~ ***bekämpa offentlig*** spridning av terrorisminnehåll via deras tjänster och vid behov säkerställa ett snabbt avlägsnande. **[Ändr. 42]**

b) En rad åtgärder som medlemsstaterna ska vidta för att identifiera terrorisminnehåll, göra det möjligt för värdtjänstleverantörerna att snabbt avlägsna det ***i enlighet med de unionsrättsliga bestämmelser som föreskriver lämpliga skyddsåtgärder för yttrandefriheten och friheten att ta emot och sprida uppgifter och tankar i ett öppet och demokratiskt samhälle*** samt underlätta samarbete med behöriga myndigheter i andra medlemsstater, med värdtjänstleverantörer och i tillämpliga fall med relevanta unionsorgan. **[Ändr. 43]**

2. Denna förordning ska tillämpas på värdtjänstleverantörer som ***i unionen*** erbjuder tjänster ~~i unionen~~ ***till allmänheten***, oberoende av deras huvudsakliga verksamhetsställe. **[Ändr. 44]**

2a. Denna förordning ska inte tillämpas på innehåll som sprids i utbildningssyfte, konstnärligt syfte, journalistiskt syfte eller forskningssyfte, eller i syfte att öka medvetenheten om terroristverksamhet; den ska heller inte tillämpas på innehåll som är ett uttryck för polemiska eller kontroversiella åsikter i den offentliga debatten. **[Ändr. 45]**

2b. Denna förordning ska inte medföra någon ändring av skyldigheten att respektera de rättigheter, friheter och principer som avses i artikel 6 i fördraget om Europeiska unionen, och den påverkar inte tillämpningen av de grundläggande principerna i unionsrätten och nationell lagstiftning om yttrandefrihet, pressfrihet och mediernas frihet och mångfald. **[Ändr. 46]**

2c. Denna förordning påverkar inte tillämpningen av direktiv 2000/31/EG. **[Ändr. 47]**

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

-1. informationssamhällets tjänster: de tjänster som avses i artikel 2 a i direktiv 2000/31/EG. **[Ändr. 48]**

1. *värdtjänstleverantör*: en leverantör av informationssamhällets tjänster som innebär att leverantören lagrar information som tillhandahållits av innehållsleverantören på dennas begäran och gör den lagrade informationen tillgänglig för ~~tredje part~~ ***allmänheten. Detta gäller enbart tjänster som tillhandahålls allmänheten i applikationslagret. Leverantörer av molninfrastruktur och leverantörer av molntjänster betraktas inte som värdtjänstleverantörer. Elektroniska kommunikationstjänster enligt definitionen i direktiv (EU) 2018/1972 är också undantagna***. **[Ändr. 49]**

2. *innehållsleverantör*: en användare som har tillhandahållit information som lagras eller har lagrats ***och gjorts tillgänglig för allmänheten*** av en värdtjänstleverantör på användarens begäran. **[Ändr. 50]**

3. *erbjuda tjänster i unionen*: göra det möjligt för juridiska eller fysiska personer i en eller flera medlemsstater att använda de tjänster som erbjuds av en värdtjänstleverantör som har en betydande anknytning till den eller de medlemsstaterna, såsom att värdtjänstleverantören

   a) har ett verksamhetsställe i unionen,

   b) har ett betydande antal användare i en eller flera medlemsstater,

   c) riktar verksamheten till en eller flera medlemsstater.

~~4. *terroristbrott*: brott enligt definitionen i artikel 3.1 i direktiv (EU) 2017/541.~~ **[Ändr. 51]**

Onsdagen den 17 april 2019

5. *terrorisminnehåll*: ~~information~~ ***material*** som **[Ändr. 52]**

a) uppviglar till ***utförande av ett av de brott som anges i artikel 3.1 a–i i direktiv (EU) 2017/541, i fall där sådana handlingar, direkt*** eller ~~förespråkar, även~~ ***indirekt, till exempel*** genom förhärligande ***av terroristdåd***, ***förespråkar*** utförande av terroristbrott, och därigenom ger upphov till en risk för att ***ett eller flera*** sådana ~~handlingar~~ ***brott*** utförs ***uppsåtligen***, och/eller **[Ändr. 53]**

b) ~~uppmuntrar bidrag till terroristbrott~~***försöker värva en annan person eller grupp av personer för att utföra eller bidra till utförandet av något av de brott som anges i artikel 3.1 a–i i direktiv (EU) 2017/541, och därigenom ger upphov till en risk för att ett eller flera sådana brott utförs uppsåtligen***, och/eller **[Ändr. 54]**

c) ~~främjar~~***försöker värva en annan person eller grupp av personer för att delta i*** en terroristgrupps verksamhet~~, i synnerhet genom att uppmuntra till deltagande i eller stöd till en terroristgrupp~~***, inbegripet tillhandahåller information eller materiella resurser eller bidrar med någon form av finansiering av dess verksamhet,*** i den mening som avses i artikel ~~2.3~~ **4** i direktiv (EU) 2017/541 ***och därigenom ger upphov till en risk för att ett eller flera sådana brott begås uppsåtligen***, och/eller **[Ändr. 55]**

d) ~~lär ut~~***tillhandahåller instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen, eller om andra särskilda*** metoder eller tekniker för att utföra ***eller bidra till utförandet av något av de*** terroristbrott ***som anges i artikel 3.1 a–i i direktiv (EU) 2017/541***. **[Ändr. 56]**

(da) avbildar utförandet av ett eller flera av de brott som anges i artikel 3.1 a–i i direktiv (EU) 2017/541 och därigenom ger upphov till en risk för att ett eller flera sådana brott utförs uppsåtligen, och/eller **[Ändr. 57]**

6. *spridning av terrorisminnehåll*: att göra terrorisminnehåll tillgängligt för ~~tredje part~~ ***allmänheten*** via värdtjänstleverantörernas tjänster. **[Ändr. 58]**

7. *användarvillkor*: alla krav, villkor och klausuler som, oberoende av deras namn eller form, reglerar avtalsförhållandet mellan värdtjänstleverantören och dess användare.

~~8. *anmälan*: ett meddelande från en behörig myndighet, eller i tillämpliga fall ett relevant unionsorgan, till en värdtjänstleverantör om information som kan anses vara terrorisminnehåll, för att leverantören på frivillig basis ska överväga om innehållet är förenligt med dess egna användarvillkor som syftar till att förhindra spridning av terrorisminnehåll.~~ **[Ändr. 59]**

9. *huvudsakligt verksamhetsställe*: det huvudkontor eller säte där de huvudsakliga finansiella funktionerna och den operativa ledningen utövas.

(9a) behörig myndighet: en enda utsedd rättslig myndighet eller funktionellt oberoende administrativ myndighet i medlemsstaten. **[Ändr. 60]**

Onsdagen den 17 april 2019

AVSNITT II

ÅTGÄRDER FÖR ATT FÖRHINDRA SPRIDNING AV TERRORISMINNEHÅLL ONLINE

Artikel 3

Aktsamhetskrav

1. Värdtjänstleverantörer ska ~~vidta lämpliga, rimliga och proportionella åtgärder~~ ***agera*** i enlighet med denna förordning ~~för att motverka spridning av terrorisminnehåll~~ och skydda användarna mot terrorisminnehåll. ~~När de gör~~ Detta ska ~~de handla~~ ***ske*** på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt, med vederbörlig hänsyn ***under alla omständigheter*** till användarnas grundläggande rättigheter och med beaktande av den grundläggande vikten av yttrandefrihet och ~~informationsfrihet~~ ***frihet att ta emot och sprida uppgifter och tankar*** i ett öppet och demokratiskt samhälle ***och i syfte att undvika att innehåll som inte är terrorisminnehåll avlägsnas***. **[Ändr. 61]**

1a. Dessa aktsamhetskrav får inte utgöra en allmän skyldighet för värdtjänstleverantörer att övervaka den information de överför eller lagrar, och inte heller någon allmän skyldighet att aktivt efterforska fakta eller omständigheter som tyder på olaglig verksamhet. **[Ändr. 62]**

~~2. Värdtjänstleverantörer ska i sina användarvillkor inbegripa bestämmelser för att förhindra spridning av terrorisminnehåll och tillämpa dessa.~~ **[Ändr. 63]**

2a. Om värdtjänstleverantörer får kunskap eller kännedom om terrorisminnehåll på deras tjänster, ska de informera de behöriga myndigheterna om detta innehåll och snabbt avlägsna det. **[Ändr. 64]**

2b. De värdtjänstleverantörer som uppfyller kriterierna i definitionen av leverantörer av videodelningsplattformar i direktiv (EU) 2018/1808 ska vidta lämpliga åtgärder för att bekämpa spridningen av terrorisminnehåll i enlighet med artikel 28b.1 c och 28b.3 i direktiv (EU) 2018/1808. **[Ändr. 65]**

Artikel 4

Avlägsnandeorder

1. Den behöriga myndigheten ***i den medlemsstat där värdtjänstleverantörens huvudsakliga verksamhetsställe är beläget*** ska ha befogenhet att utfärda ~~ett beslut~~ ***en avlägsnandeorder*** som kräver att värdtjänstleverantören avlägsnar terrorisminnehåll eller gör det oåtkomligt ***i alla medlemsstater***. **[Ändr. 66]**

1a. Den behöriga myndigheten i en medlemsstat där värdtjänstleverantören inte har sitt huvudsakliga verksamhetsställe eller inte har en rättslig företrädare får begära att terrorisminnehållet ska göras oåtkomligt och verkställa denna begäran inom sitt territorium. **[Ändr. 67]**

1b. Om den berörda behöriga myndigheten inte tidigare har utfärdat en avlägsnandeorder till en värdtjänstleverantör, ska den kontakta värdtjänstleverantören och tillhandahålla information om förfaranden och tillämpliga tidsfrister senast tolv timmar innan avlägsnandeordern utfärdas. **[Ändr. 68]**

2. Värdtjänstleverantörer ska avlägsna terrorisminnehåll eller göra det oåtkomligt ***så snart som möjligt, dock senast*** inom en timme från mottagandet av avlägsnandeordern. **[Ändr. 69]**

3. Avlägsnandeorder ska innehålla följande uppgifter i enlighet med mallen i bilaga I:

a) ~~Uppgift om~~ ***Identifiering med hjälp av en elektronisk signatur av*** den behöriga myndighet som utfärdat avlägsnandeordern och den behöriga myndighetens autentisering av avlägsnandeordern. **[Ändr. 70]**

Onsdagen den 17 april 2019

b) En ***detlajerad*** redogörelse av orsaker till att innehållet anses vara terrorisminnehåll~~, åtminstone genom~~ ***och en särskild*** hänvisning till de kategorier av terrorisminnehåll som anges i artikel 2.5. **[Ändr. 71]**

c) En ***exakt*** webbadress (URL) och, vid behov, ytterligare information som gör det möjligt att identifiera det innehåll som anmäls. **[Ändr. 72]**

d) En hänvisning till denna förordning som rättslig grund för avlägsnandeordern.

e) Datum och tidpunkt för utfärdande.

f) ***Lättbegriplig*** information om värdtjänstleverantörens och innehållsleverantörens prövningsmöjligheter***, inbegripet prövning vid såväl den behöriga myndigheten som vid domstol samt tidsfrister för överklagande*** **[Ändr. 73]**.

g) ~~I tillämpliga fall~~***Där så är nödvändigt och proportionellt***, beslutet att inte lämna ut information om att terrorisminnehåll avlägsnats eller gjorts oåtkomligt i den mening som avses i artikel 11. **[Ändr. 74]**

~~4. På värdtjänstleverantörens eller innehållsleverantörens begäran ska den behöriga myndigheten lämna en detaljerad motivering, utan att det påverkar värdtjänstleverantörens skyldighet att följa avlägsnandeordern inom den tidsfrist som anges i punkt 2.~~ **[Ändr. 75]**

5. ~~De~~***Den*** behöriga ~~myndigheterna~~ ***myndigheten*** ska rikta avlägsnandeordern till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den juridiska företrädare som värdtjänstleverantören har utsett enligt artikel 16 och överföra den till den kontaktpunkt som avses i artikel 14.1. Sådana order ska sändas på ett elektroniskt sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar att säkerställa autentisering av avsändaren, även att datum och tidpunkt för sändandet och mottagandet av ordern är korrekt. **[Ändr. 76]**

6. Värdtjänstleverantörer ska ~~bekräfta mottagandet och~~ utan onödigt dröjsmål informera den behöriga myndigheten om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt, med angivelse av i synnerhet tidpunkten för åtgärden, med hjälp av mallen i bilaga II. **[Ändr. 77]**

7. Om värdtjänstleverantören inte kan följa avlägsnandeordern på grund av force majeure eller faktisk omöjlighet som inte kan tillskrivas värdtjänstleverantören, ***bland annat av tekniska eller operativa skäl,*** ska den utan dröjsmål informera den behöriga myndigheten och förklara orsakerna till detta med hjälp av mallen i bilaga III. Den frist som anges i punkt 2 ska tillämpas så snart de angivna orsakerna inte längre föreligger. **[Ändr. 78]**

8. ~~Om~~ Värdtjänstleverantören ~~inte kan följa~~ ***får vägra*** avlägsnandeordern ~~eftersom~~ ***om*** ordern innehåller uppenbara fel eller inte innehåller tillräcklig information ~~för att verkställa den,~~***. Värdtjänstleverantören*** ska ~~värdtjänstleverantören~~ informera den behöriga myndigheten utan dröjsmål och be om nödvändiga klargöranden med hjälp av mallen i bilaga III. Den frist som anges i punkt 2 ska tillämpas så snart klargörandet har lämnats. **[Ändr. 79]**

9. Den behöriga myndighet som utfärdade avlägsnandeordern ska informera den behöriga myndighet som övervakar genomförandet av ~~proaktiva~~ ***specifika*** åtgärder i enlighet med artikel 17.1 c när avlägsnandeordern vunnit laga kraft. En avlägsnandeorder vinner laga kraft när den inte har överklagats inom tidsfristen enligt tillämplig nationell rätt eller när den har bekräftats efter ett överklagande. **[Ändr. 80]**

Artikel 4a

Samrådsförfarande för avlägsnandeorder

1. Den behöriga myndighet som utfärdar en avlägsnandeorder enligt artikel 4.1a ska översända en kopia av denna till den behöriga myndighet som avses i artikel 17.1 a där värdtjänstleverantörens huvudsakliga verksamhetsställe är beläget samtidigt som den överförs till värdtjänstleverantören i enlighet med artikel 4.5.

2. Den behöriga myndigheten i den medlemsstat där värdtjänstleverantörens huvudsakliga verksamhetsställe är beläget ska, i fall där den har rimliga skäl att anta att avlägsnandeordern kan påverka grundläggande intressen i den medlemsstaten, underrätta den utfärdande behöriga myndigheten. Den utfärdande myndigheten ska beakta dessa omständigheter och, vid behov, dra tillbaka eller anpassa avlägsnandeordern. **[Ändr. 81]**

Artikel 4b

Samarbetsförfarande för utfärdande av en ytterligare avlägsnandeorder

1. Om en behörig myndighet har utfärdat en avlägsnandeorder enligt artikel 4.1a, får den myndigheten kontakta den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe för att begära att den sistnämnda behöriga myndigheten också utfärdar en avlägsnandeorder enligt artikel 4.1.

2. Den behöriga myndigheten i den medlemsstat där värdtjänstleverantörens huvudsakliga verksamhetsställe är beläget ska så snart som möjligt, dock senast en timme efter att den blivit kontaktad enligt punkt 1, antingen utfärda en avlägsnandeorder eller vägra att utfärda en avlägsnandeorder, och den ska underrätta den behöriga myndighet som har utfärdat den första ordern om sitt beslut.

3. Om den behöriga myndigheten i den medlemsstat där det huvudsakliga verksamhetsstället är beläget behöver mer än en timme för sin bedömning av innehållet, ska den sända en begäran till den berörda värdtjänstleverantören om att tillfälligt göra innehållet oåtkomligt i upp till 24 timmar; under denna tid ska den behöriga myndigheten ska göra sin bedömning och antingen sända avlägsnandeordern eller dra tillbaka begäran om att göra innehållet oåtkomligt. **[Ändr. 82]**

~~Artikel 5~~

~~Anmälningar~~

~~1. Den behöriga myndigheten eller det relevanta unionsorganet får göra en anmälan till en värdtjänstleverantör.~~

~~2. Värdtjänstleverantörer ska införa operativa och tekniska åtgärder som underlättar snabb utvärdering av innehåll som har anmälts av de behöriga myndigheterna, och i tillämpliga fall relevanta unionsorgan, för frivilligt övervägande.~~

~~3. Anmälan ska riktas till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den rättsliga företrädare som värdtjänstleverantören utsett enligt artikel 16 och överföras till den kontaktpunkt som avses i artikel 14.1. Sådana anmälningar ska sändas på elektronisk väg.~~

~~4. Anmälan ska innehålla tillräckligt detaljerad information, inklusive orsakerna till att innehållet anses vara terrorisminnehåll, en webbadress och, vid behov, ytterligare information som gör det möjligt att identifiera det anmälda terrorisminnehållet.~~

~~5. Värdtjänstleverantören ska, som en prioriterad fråga, bedöma det innehåll som anges i anmälan utifrån sina egna användarvillkor och besluta om den ska avlägsna innehållet eller göra det oåtkomligt.~~

Onsdagen den 17 april 2019

~~6. Värdtjänstleverantören ska skyndsamt informera den behöriga myndigheten eller det relevanta unionsorganet om resultatet av bedömningen och tidpunkten för eventuella åtgärder som vidtagits till följd av anmälan.~~

~~7. Om värdtjänstleverantören anser att anmälan inte innehåller tillräcklig information för att bedöma det anmälda innehållet, ska den utan dröjsmål informera de behöriga myndigheterna eller det relevanta unionsorganet och ange vilka ytterligare upplysningar eller klargöranden som krävs.~~ **[Ändr. 83]**

Artikel 6

~~Proaktiva~~ ***Specifika*** åtgärder **[Ändr. 84]**

1. ***Utan att det påverkar tillämpningen av direktiv (EU) 2018/1808 och direktiv 2000/31/EG får*** värdtjänstleverantörer ~~ska, när så är lämpligt,~~ vidta ~~proaktiva~~ ***särskilda*** åtgärder för att skydda sina tjänster mot ***offentlig*** spridning av terrorisminnehåll. Åtgärderna ska vara verkningsfulla***, riktade*** och proportionella, ~~med beaktande av~~ ***och ska särskilt beakta*** risken för och graden av utsatthet för terrorisminnehåll, användarnas grundläggande rättigheter och den grundläggande vikten av ***rätten till*** yttrandefrihet och ~~informationsfrihet~~ ***frihet att ta emot och sprida uppgifter och tankar*** i ett öppet och demokratiskt samhälle. **[Ändr. 85]**

~~2. När den behöriga myndighet som avses i artikel 17.1 c har informerats i enlighet med artikel 4.9, ska den begära att värdtjänstleverantören, inom tre månader efter mottagandet av begäran och därefter minst en gång om året, lämnar in en rapport om de specifika proaktiva åtgärder som den har vidtagit, även med hjälp av automatiska verktyg, i syfte att~~

~~(a) förhindra att innehåll som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det anses vara terrorisminnehåll laddas upp på nytt,~~

~~(b) upptäcka, identifiera och snabbt avlägsna terrorisminnehåll eller göra det oåtkomligt.~~

~~En sådan begäran ska sändas till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den rättsliga företrädare som värdtjänstleverantören utsett.~~

~~Rapporterna ska innehålla all relevant information som gör det möjligt för den behöriga myndighet som avses i artikel 17.1 c att bedöma om de proaktiva åtgärderna är effektiva och proportionella samt utvärdera hur eventuella automatiska verktyg och mekanismer för mänsklig tillsyn och kontroll som använts fungerar.~~ **[Ändr. 86]**

~~3. Om den behöriga myndighet som avses i artikel 17.1 c anser att de proaktiva åtgärder som vidtagits och rapporterats enligt punkt 2 är otillräckliga för att minska och hantera risken för och graden av utsatthet, får den begära att värdtjänstleverantören vidtar ytterligare specifika proaktiva åtgärder. För detta ändamål ska värdtjänstleverantören samarbeta med den behöriga myndighet som avses i artikel 17.1 c i syfte att identifiera de särskilda åtgärder som värdtjänstleverantören ska införa samt fastställa centrala mål, riktmärken och tidsfrister för genomförandet.~~ **[Ändr. 87]**

4. ~~Om en överenskommelse inte kan nås inom tre månader från begäran enligt punkt 3~~***Efter att ha fastställt att en värdtjänstleverantör har tagit emot ett betydande antal avlägsnandeorder,*** får den behöriga myndighet som avses i artikel 17.1 c ~~utfärda ett beslut~~ ***skicka en begäran*** om ~~att föreskriva~~ ***nödvändiga, proportionerliga och effektiva*** ytterligare specifika ~~nödvändiga och proportionella proaktiva~~ åtgärder~~. Beslutet~~ ***som värdtjänstleverantören måste vidta. Den behöriga myndigheten får inte ålägga en allmän övervakningsskyldighet eller göra det obligatoriskt att använda automatiska verktyg. Begäran*** ska särskilt ta hänsyn till ***åtgärdernas tekniska genomförbarhet,*** värdtjänstleverantörens ***storlek och*** ekonomiska kapacitet samt sådana åtgärders inverkan på användarnas grundläggande rättigheter och den grundläggande vikten av yttrandefrihet och ~~informationsfrihet. Ett sådant beslut~~ ***frihet att ta emot och sprida uppgifter och tankar i ett öppet och demokratiskt samhälle. En sådan begäran*** ska sändas till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till den rättsliga företrädare som tjänsteleverantören utsett. Värdtjänstleverantören ska regelbundet rapportera om genomförandet av de åtgärder som fastställts av den behöriga myndighet som avses i artikel 17.1 c. **[Ändr. 88]**

5. En värdtjänstleverantör får när som helst begära att den behöriga myndighet som avses i artikel 17.1 c prövar och, när det är lämpligt, återkallar en begäran ~~eller ett beslut~~ enligt punkt ~~2, 3 respektive~~ 4. Den behöriga myndigheten ska lämna ett motiverat beslut inom rimlig tid efter det att den har mottagit värdtjänstleverantörens begäran. **[Ändr. 89]**

Artikel 7

Bevarande av innehåll och relaterade data

1. Värdtjänstleverantörer ska bevara terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder~~, en anmälan~~ eller ~~proaktiva~~ ***specifika*** åtgärder enligt artiklarna 4~~, 5~~ och 6, samt relaterade data som avlägsnats till följd av att terrorisminnehållet har avlägsnats, och som är nödvändigt för **[Ändr. 90]**

a) administrativa eller rättsliga prövningsförfaranden ***eller rättsmedel***, **[Ändr. 91]**

b) ***brottsbekämpande myndigheters*** förebyggande, upptäckt, utredning och lagföring av terroristbrott. **[Ändr. 92]**

2. Det terrorisminnehåll och de relaterade data som avses i punkt 1 ska bevaras i sex månader ***och därefter förstöras***. Terrorisminnehållet ska, på den behöriga myndighetens eller domstolens begäran, bevaras under en ~~längre~~ ***viss ytterligare*** period***, endast*** om och så länge som det krävs för ett sådant pågående administrativt eller rättsligt prövningsförfarande ***eller rättsmedel*** som avses i punkt 1 a. ***Värdtjänstleverantörer ska bevara det terrorisminnehåll och de relaterade uppgifter som avses i punkt 1 b till dess att den brottsbekämpande myndigheten reagerar på den anmälan som värdtjänstleverantören gjort i enlighet med artikel 13.4, men aldrig längre än sex månader.*** **[Ändr. 93]**

3. Värdtjänstleverantörer ska säkerställa att terrorisminnehåll och relaterade data som bevaras enligt punkterna 1 och 2 omfattas av lämpliga tekniska och organisatoriska skyddsåtgärder.

Dessa tekniska och organisatoriska skyddsåtgärder ska säkerställa att det terrorisminnehåll och de relaterade data som bevaras endast åtkoms och behandlas för de syften som avses i punkt 1, samt säkerställa en hög säkerhetsnivå för de berörda personuppgifterna. Värdtjänstleverantörer ska vid behov se över och uppdatera dessa skyddsåtgärder.

AVSNITT III

SKYDDSÅTGÄRDER OCH ANSVARIGHET

Artikel 8

Transparenskrav ***för värdtjänstleverantörer*** **[Ändr. 94]**

1. ***I tillämpliga fall ska*** värdtjänstleverantörer ~~ska~~ i sina användarvillkor fastställa sin strategi för att förhindra spridningen av terrorisminnehåll, ~~när så är lämpligt~~ ***och i tillämpliga fall*** även ***ge*** en meningsfull förklaring av hur ~~proaktiva~~ ***specifika*** åtgärder, bland annat användningen av automatiska verktyg, fungerar. **[Ändr. 95]**

2. Värdtjänstleverantörer ***som under det relevanta året är eller har varit föremål för avlägsnandeorder*** ska offentliggöra ~~årliga transparensrapporter~~ ***en årlig transparensrapport*** om åtgärder som vidtagits för att förhindra spridningen av terrorisminnehåll. **[Ändr. 96]**

3. Transparensrapporterna ska innehålla minst följande information:

a) Information om värdtjänstleverantörens åtgärder för att upptäcka, identifiera och avlägsna terrorisminnehåll.

Onsdagen den 17 april 2019

b) Information om värdtjänstleverantörens åtgärder för att förhindra att innehåll som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det anses vara terrorisminnehåll laddas upp på nytt***, särskilt när automatisk teknik har använts***. **[Ändr. 97]**

c) Mängd terrorisminnehåll som avlägsnats eller gjorts oåtkomligt efter avlägsnandeorder~~, anmälningar respektive proaktiva~~ ***eller specifika*** åtgärder***, och antalet order där innehållet inte avlägsnats i överensstämmelse med artiklarna 4.7 och 4.8, tillsammans med skälen till nekandet***. **[Ändr. 98]**

d) ~~Översikt~~ ***Antal*** och resultat av klagomålsförfaranden ***och överklaganden, inklusive antalet ärenden i vilka det fastställts att innehållet felaktigt identifierats som terrorisminnehåll***. **[Ändr. 99]**

Artikel 8a

Transparenskrav för behöriga myndigheter

1. Värdtjänstleverantörerna ska offentliggöra årliga transparensrapporter som ska innehålla åtminstone följande information:

(a) Antal utfärdade avlägsnandeorder, antal avlägsnanden och antal nekade eller förbisedda avlägsnandeorder.

(b) Antal fall med identifierat terrorisminnehåll som lett till utredning och lagföring och antal fall då innehåll felaktigt identifierats som terrorisminnehåll.

(c) En beskrivning av åtgärder som de behöriga myndigheterna har begärt i enlighet med artikel 6.4. **[Ändr. 100]**

Artikel 9

Skyddsåtgärder avseende användningen och genomförandet av ~~proaktiva~~ ***specifika*** åtgärder **[Ändr. 101]**

1. När värdtjänstleverantörer använder automatiska verktyg ~~enligt denna förordning~~ avseende det innehåll som de lagrar, ska de tillhandahålla effektiva och lämpliga skyddsmekanismer för att säkerställa att beslut som fattas angående detta innehåll, i synnerhet beslut om att avlägsna innehåll som anses vara terrorisminnehåll eller göra det oåtkomligt, är korrekta och välgrundade. **[Ändr. 102]**

2. Skyddsåtgärderna ska särskilt omfatta mänsklig tillsyn och kontroll~~, när detta är lämpligt och i alla händelser när det krävs en detaljerad bedömning~~ av ***lämpligheten i beslut om*** ~~det relevanta sammanhanget för~~ att ***avlägsna innehåll eller neka tillgång till det, i synnerhet med tanke på rätten till yttrandefrihet och frihet att ta emot och sprida uppgifter och tankar i ett öppet och demokratiskt samhälle*** ~~avgöra om innehållet ska anses vara terrorisminnehåll eller inte~~. **[Ändr. 103]**

Artikel 9a

Effektiva rättsmedel

1. Innehållsleverantörer vars innehåll har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder, och värdtjänstleverantörer som har tagit emot en avlägsnandeorder, ska ha rätt till ett effektivt rättsmedel. Medlemsstaterna ska införa effektiva förfaranden för utövandet av denna rättighet. **[Ändr. 104]**

Artikel 10

Klagomålsmekanismer

1. Värdtjänstleverantörer ska inrätta ~~effektiva~~ ***en effektiv*** och ~~tillgängliga mekanismer~~ ***tillgänglig mekanism*** som gör det möjligt för innehållsleverantörer, vars innehåll har avlägsnats eller gjorts oåtkomligt till följd av ~~en anmälan enligt artikel 5 eller av proaktiva~~ ***specifika*** åtgärder enligt artikel 6, att lämna in ett klagomål mot värdtjänstleverantörens åtgärd och begära att innehållet återställs. **[Ändr. 105]**

2. Värdtjänstleverantörer ska omgående granska varje klagomål som de tar emot och återställa innehållet utan onödigt dröjsmål om det inte var berättigat att avlägsna innehållet eller göra det oåtkomligt. De ska informera klaganden om resultatet av granskningen ***inom två veckor från mottagandet av klagomålet, tillsammans med en förklaring i sådana fall där värdtjänstleverantören beslutar att inte återställa innehållet. Ett återställande av innehåll ska inte utesluta ytterligare rättsliga åtgärder mot värdtjänstleverantörens eller den behöriga myndighetens beslut.*** **[Ändr. 106]**

Artikel 11

Information till innehållsleverantörer

1. Om värdtjänstleverantörer ~~har avlägsnat~~ ***avlägsnar*** terrorisminnehåll eller ~~gjort~~ ***gör*** det oåtkomligt, ska de tillhandahålla ***uttömmande och saklig*** information till innehållsleverantören om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt ***och om möjligheterna att bestrida beslutet, samt på begäran ge innehållsleverantören en kopia av den avlägsnandeorder som utfärdats i överensstämmelse med artikel 4***. **[Ändr. 107]**

~~2. På innehållsleverantörens begäran ska värdtjänstleverantören informera innehållsleverantören om orsakerna till att innehållet avlägsnades eller gjordes oåtkomligt och möjligheterna att bestrida beslutet.~~ **[Ändr. 108]**

3. Skyldigheten enligt ~~punkterna~~ ***punkt*** 1 ~~och 2~~ ska inte gälla om den behöriga myndigheten beslutar***, på grundval av objektiva bevis och med beaktande av proportionaliteten i och nödvändigheten av ett sådant beslut,*** att orsakerna inte bör lämnas ut av hänsyn till allmän säkerhet, såsom förebyggande, utredning, upptäckt och lagföring av terroristbrott, under en så lång tid som det är nödvändigt, men inte längre än [fyra] veckor efter beslutet. I sådana fall ska värdtjänstleverantören inte lämna någon information om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt. **[Ändr. 109]**

AVSNITT IV

SAMARBETE MELLAN BEHÖRIGA MYNDIGHETER, UNIONSORGAN OCH VÄRDTJÄNSTLEVERANTÖRER

Artikel 12

De behöriga myndigheternas kapacitet

Medlemsstaterna ska säkerställa att deras behöriga myndigheter har den kapacitet och de resurser som krävs för att uppnå målen och fullgöra sina skyldigheter enligt denna förordning***, med starka garantier för oberoende***. **[Ändr. 110]**

Artikel 13

Samarbete mellan värdtjänstleverantörer, behöriga myndigheter och i tillämpliga fall ~~relevanta~~ ***behöriga*** unionsorgan
[Ändr. 111]

1. De behöriga myndigheterna i medlemsstaterna ska informera, samordna sig med och samarbeta med varandra, och när så är lämpligt med ~~relevanta unionsorgan såsom~~ Europol, avseende avlägsnandeorder ~~och anmälningar~~ för att undvika dubbelarbete, öka samordningen och undvika att störa utredningar i andra medlemsstater. **[Ändr. 112]**

Onsdagen den 17 april 2019

2. De behöriga myndigheterna i medlemsstaterna ska informera, samordna sig med och samarbeta med den behöriga myndighet som avses i artikel 17.1 c och 17.1 d avseende åtgärder som vidtas i enlighet med artikel 6 och verkställighetsåtgärder enligt artikel 18. Medlemsstaterna ska se till att den behöriga myndighet som avses i artikel 17.1 c och 17.1 d förfogar över all relevant information. För detta ändamål ska medlemsstaterna sörja för lämpliga ***och säkra*** kommunikationskanaler eller mekanismer för att säkerställa att den relevanta informationen delas inom rimlig tid. **[Ändr. 113]**

3. Medlemsstater ~~och värdtjänstleverantörer~~ får ~~välja att~~ använda särskilda verktyg, ~~när så är lämpligt~~ även sådana som inrättats av ~~relevanta unionsorgan som t.ex.~~ Europol, för att särskilt underlätta **[Ändr. 114]**

a) handläggning och återkoppling avseende avlägsnandeorder enligt artikel 4,

~~b) handläggning och återkoppling avseende anmälningar enligt artikel 5,~~ **[Ändr. 115]**

c) samarbete i syfte att identifiera och genomföra ~~proaktiva~~ ***specifika*** åtgärder enligt artikel 6. **[Ändr. 116]**

4. Om värdtjänstleverantörer får kännedom om ~~bevis för terroristbrott~~ ***terrorisminnehåll*** ska de omedelbart underrätta de myndigheter som är behöriga att utreda och lagföra brott i den berörda medlemsstaten ~~eller~~. ***Om det inte går att fastställa vilken medlemsstat som berörs ska värdtjänstleverantörerna underrätta*** kontaktpunkten i den mening som avses i artikel ~~14.2~~ ***17.2*** i den medlemsstat där de har sitt huvudsakliga verksamhetsställe eller en rättslig företrädare. ~~I tveksamma fall får värdtjänstleverantörerna~~***, och även*** vidarebefordra denna information till Europol för lämplig uppföljning. **[Ändr. 117]**

4a. Värdtjänstleverantörerna ska samarbeta med de behöriga myndigheterna. **[Ändr. 118]**

Artikel 14

Kontaktpunkter

1. Värdtjänstleverantörer ***som tidigare tagit emot en eller flera avlägsnandeorder*** ska inrätta en kontaktpunkt, så att de kan ta emot avlägsnandeorder ~~och anmälningar~~ på elektronisk väg och säkerställa att de handläggs snabbt i enlighet med ~~artiklarna~~ ***artikel*** 4 ~~och 5~~. De ska säkerställa att denna information offentliggörs. **[Ändr. 119]**

2. I den information som avses i punkt 1 ska det anges ~~på~~ vilket eller vilka av unionens officiella språk, i den mening som avses i förordning (EG) nr 1/58, ***som kan användas för kontakter med*** kontaktpunkten ~~kan kontaktas~~ och ***för*** ytterligare utbyten avseende avlägsnandeorder ~~och anmälningar~~ enligt ~~artiklarna~~ ***artikel*** 4 ~~och 5 ska äga rum~~. Detta ska omfatta åtminstone ett av de officiella språken i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare enligt artikel 16 är bosatt eller etablerad. **[Ändr. 120]**

~~3. Medlemsstaterna ska inrätta en kontaktpunkt för att hantera begäranden om klargöranden och återkoppling avseende avlägsnandeorder och anmälningar som de har utfärdat. Information om kontaktpunkten ska offentliggöras.~~ **[Ändr. 121]**

Onsdagen den 17 april 2019

AVSNITT V

GENOMFÖRANDE OCH VERKSTÄLLIGHET

Artikel 15

Jurisdiktion

1. Den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe ska ha jurisdiktion vid tillämpningen av artiklarna 6, 18 och 21. En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i en av medlemsstaterna ska anses lyda under jurisdiktionen i den medlemsstat där den rättsliga företrädare som avses i artikel 16 är bosatt eller etablerad.

2. Om en värdtjänstleverantör ***som inte har sitt huvudsakliga verksamhetsställe i någon av medlemsstaterna*** inte har utsett en rättslig företrädare ska samtliga medlemsstater ha jurisdiktion. ***Om en medlemsstat beslutar att utöva denna jurisdiktion ska den informera alla övriga medlemsstater.*** **[Ändr. 122]**

~~3. Om en myndighet i en annan medlemsstat har utfärdat en avlägsnandeorder enligt artikel 4.1 har den medlemsstaten jurisdiktion att vidta tvångsåtgärder i enlighet med sin nationella lagstiftning för att verkställa avlägsnandeordern.~~ **[Ändr. 123]**

Artikel 16

Rättslig företrädare

1. En värdtjänstleverantör som inte har något verksamhetsställe i unionen men som erbjuder tjänster i unionen ska skriftligen utse en juridisk eller fysisk person till sin rättsliga företrädare i unionen för mottagande, efterlevnad och verkställighet av avlägsnandeorder~~, anmälningar,~~ ***och*** begäranden ~~och beslut~~ som utfärdas av de behöriga myndigheterna på grundval av denna förordning. Den rättsliga företrädaren ska vara bosatt eller etablerad i en av de medlemsstater där värdtjänstleverantören erbjuder tjänsterna. **[Ändr. 124]**

2. Värdtjänstleverantören ska anförtro den rättsliga företrädaren mottagande, efterlevnad och verkställighet av avlägsnandeorder~~, anmälningar,~~ ***och*** begäranden ~~och beslut~~ som avses i punkt 1 på den berörda värdtjänstleverantörens vägnar. Värdtjänstleverantörer ska förse sin rättsliga företrädare med de befogenheter och resurser som krävs för att samarbeta med de behöriga myndigheterna och efterleva dessa beslut och order. **[Ändr. 125]**

3. Den utsedda rättsliga företrädaren kan hållas ansvarig för bristande efterlevnad av skyldigheter enligt denna förordning, utan att det påverkar de skadeståndskrav och rättsliga åtgärder som kan inledas mot värdtjänstleverantören.

4. Värdtjänstleverantören ska underrätta den behöriga myndighet som avses i artikel 17.1 d i den medlemsstat där den rättsliga företrädaren är bosatt eller etablerad om utseendet. Information om den rättsliga företrädaren ska offentliggöras.

AVSNITT VI

SLUTBESTÄMMELSER

Artikel 17

Utseende av behöriga myndigheter

1. Varje medlemsstat ska utse ~~den~~ ***en rättslig*** eller ~~de myndigheter~~ ***en funktionellt oberoende administrativ myndighet*** som är behörig att **[Ändr. 126]**

a) utfärda avlägsnandeorder i enlighet med artikel 4,

Onsdagen den 17 april 2019

~~b) upptäcka och identifiera terrorisminnehåll och anmäla terrorisminnehåll till värdtjänstleverantörer i enlighet med artikel 5,~~ **[Ändr. 127]**

c) övervaka genomförandet av ~~proaktiva~~ ***specifika*** åtgärder i enlighet med artikel 6, **[Ändr. 128]**

d) säkerställa att skyldigheterna enligt denna förordning efterlevs genom påföljder i enlighet med artikel 18.

1a. Medlemsstaterna ska utse en kontaktpunkt inom de behöriga myndigheterna för att hantera begäranden om klargöranden och återkoppling avseende avlägsnandeorder som de har utfärdat. Information om kontaktpunkten ska offentliggöras. **[Ändr. 129]**

2. Senast [*sex månader efter denna förordnings ikraftträdande*] ska medlemsstaterna underrätta kommissionen om de behöriga myndigheter som avses i punkt 1. Kommissionen ska ***upprätta ett onlineregister över alla dessa behöriga myndigheter och den utsedda kontaktpunkten för varje behörig myndighet. Kommissionen ska*** offentliggöra underrättelsen och eventuella ändringar därav i *Europeiska unionens officiella tidning*. **[Ändr. 130]**

Artikel 18

Påföljder

1. Medlemsstaterna ska fastställa regler om påföljder vid värdtjänstleverantörers ***systematiska och fortgående*** överträdelser av skyldigheter enligt denna förordning och ska vidta alla åtgärder som krävs för att säkerställa att de tillämpas. Sådana påföljder ska begränsas till åsidosättande av skyldigheterna enligt **[Ändr. 131]**

~~a) artikel 3.2 (värdtjänstleverantörernas användarvillkor),~~ **[Ändr. 132]**

b) artikel 4.2 och 4.6 (genomförande av och återkoppling om avlägsnandeorder),

~~c) artikel 5.5 och 5.6 (bedömning av och återkoppling om anmälningar),~~ **[Ändr. 133]**

d) artikel ~~6.2 och~~ 6.4 (rapporter om ~~proaktiva~~ ***specifika*** åtgärder och antagande av åtgärder efter ett beslut som föreskriver ***ytterligare*** specifika ~~proaktiva~~ åtgärder), **[Ändr. 134]**

e) artikel 7 (bevarande av data),

f) artikel 8 (transparens ***för värdtjänstleverantörer***), **[Ändr. 135]**

g) artikel 9 (skyddsåtgärder ~~i samband med proaktiva~~ ***avseende genomförandet av specifika*** åtgärder), **[Ändr. 136]**

h) artikel 10 (klagomålsförfaranden),

i) artikel 11 (information till innehållsleverantörer),

j) artikel 13.4 (information om ~~bevis på terroristbrott~~ ***terrorisminnehåll***), **[Ändr. 137]**

k) artikel 14.1 (kontaktpunkter),

l) artikel 16 (utseende av en rättslig företrädare).

2. Påföljderna ***enligt punkt 1*** ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska senast den [*inom sex månader efter denna förordnings ikraftträdande*] till kommissionen anmäla dessa regler och åtgärder samt utan dröjsmål eventuella ändringar som påverkar dem. **[Ändr. 138]**

3. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de fastställer påföljdernas typ och nivå, beaktar alla relevanta omständigheter, bland annat

a) överträdelsens karaktär, allvar och varaktighet,

b) om överträdelsen är avsiktlig eller har orsakats av vårdslöshet,

c) tidigare överträdelser som den juridiska person som hålls ansvarig gjort sig skyldig till,

d) den finansiella styrkan hos den juridiska person som hålls ansvarig,

e) värdtjänstleverantörens vilja att samarbeta med de behöriga myndigheterna.***,*** **[Ändr. 139]**

ea) värdtjänstleverantörernas karaktär och storlek, särskilt för mikroföretag eller småföretag i den mening som avses i kommissionens rekommendation 2003/361/EG ([13]). **[Ändr. 140]**

4. Medlemsstaterna ska säkerställa att en systematisk ***och fortgående*** underlåtenhet att uppfylla skyldigheterna enligt artikel 4.2 blir föremål för böter på upp till 4 % av värdtjänstleverantörens totala omsättning under det senaste räkenskapsåret. **[Ändr. 141]**

Artikel 19

Tekniska krav***, kriterier för bedömning av betydelsen*** och ändringar av mallarna för avlägsnandeorder **[Ändr. 142]**

1. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 20 för att komplettera denna förordning med ***nödvändiga*** tekniska krav på de elektroniska medel som de behöriga myndigheterna ska använda för översändande av avlägsnandeorder. **[Ändr. 143]**

1a. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 20 för att komplettera denna förordning med kriterier och siffror som de behöriga myndigheterna ska använda för att avgöra vad som utgör ett betydande antal obestridda avlägsnandeorder enligt denna förordning. **[Ändr. 144]**

2. Kommissionen ska ha befogenhet att anta sådana delegerade akter för att ändra bilagorna I, II och III i syfte att effektivt åtgärda eventuella behov av förbättringar av innehållet i formulären för avlägsnandeorder och formulär som ska användas för att meddela att det är omöjligt att verkställa avlägsnandeordern.

Artikel 20

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 19 ska ges till kommissionen tills vidare från och med den [*datum då denna förordning börjar tillämpas*].

3. Den delegering av befogenhet som avses i artikel 19 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt, ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.

([13]) Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

Onsdagen den 17 april 2019

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 19 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 21

Övervakning

1. Medlemsstaterna ska samla in information från sina behöriga myndigheter och värdtjänstleverantörerna under deras jurisdiktion om de åtgärder som dessa har vidtagit i enlighet med denna förordning och sända informationen till kommissionen senast den [31 mars] varje år. Denna information ska omfatta följande:

a) Information om antalet utfärdade avlägsnandeorder ~~och anmälningar~~, mängd terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt, inklusive tidsramarna för detta i enlighet med ~~artiklarna~~ ***artikel*** 4 ~~och 5~~***, samt information om antalet motsvarande fall med framgångsrik upptäckt, utredning och lagföring av terroristbrott***. **[Ändr. 145]**

b) Information om de specifika proaktiva åtgärder som vidtagits i enlighet med artikel 6, inklusive den mängd terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt och tidsramarna för detta.

ba) Information om antalet begäranden om tillgång som utfärdats av behöriga myndigheter avseende innehåll som bevaras av värdtjänstleverantörerna i enlighet med artikel 7. **[Ändr. 146]**

c) Information om det antal klagomålsförfaranden som inletts och de åtgärder som vidtagits av värdtjänstleverantörerna i enlighet med artikel 10.

d) Information om antalet prövningsförfaranden som har inletts och beslut som fattats av den behöriga myndigheten i enlighet med nationell lagstiftning.

2. Senast [*ett år efter den dag då denna förordning börjar tillämpas*] ska kommissionen upprätta ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter. I övervakningsprogrammet ska det anges indikatorer, vilka metoder som ska användas för att samla in uppgifter och andra nödvändiga belägg och med vilka intervaller detta ska ske. Det ska anges vilka åtgärder kommissionen och medlemsstaterna ska vidta för att samla in och analysera uppgifterna och andra belägg för att övervaka framstegen och utvärdera denna förordning i enlighet med artikel 23.

Artikel 22

Genomföranderapport

Senast den … [*två år efter denna förordnings ikraftträdande*] ska kommissionen lägga fram en rapport för Europaparlamentet och rådet om tillämpningen av denna förordning. Information om övervakning enligt artikel 21 och information som härrör från transparenskraven enligt artikel 8 ska beaktas i kommissionens rapport. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta denna rapport.

Artikel 23

Utvärdering

~~Tidigast [tre~~***Ett*** år ~~från och med~~ ***efter*** den dag då denna förordning börjar tillämpas] ska kommissionen göra en utvärdering av denna förordning och lägga fram en rapport för Europaparlamentet och rådet om tillämpningen av förordningen, inklusive om ***funktionen och*** effektiviteten i skyddsmekanismerna, ***samt om inverkan på grundläggande rättigheter, i synnerhet på yttrandefriheten, friheten att ta emot och sprida uppgifter och rätten till respekt för privatlivet. I samband med utvärderingen ska kommissionen även rapportera om hur nödvändigt, genomförbart och effektivt det är att inrätta en europeisk plattform om terrorisminnehåll online, som skulle ge alla medlemsstater en säker***

kommunikationskanal för att sända order om avlägsnande av terrorisminnehåll till värdtjänstleverantörer. Vid behov ska rapporten åtföljas av förslag till rättsakter. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta denna rapport. **[Ändr. 147]**

Artikel 24

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den [***6*12** månader efter ikraftträdandet]. **[Ändr. 148]**

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i …

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

Onsdagen den 17 april 2019

BILAGA I

AVLÄGSNANDEORDER FÖR TERRORISMINNEHÅLL (artikel 4 i förordning (EU) xxx)

Enligt artikel 4 i förordning (EU)… ([1]) ska den som mottar en avlägsnandeorder avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme från mottagandet av avlägsnandeordern från en behörig myndighet.

I enlighet med artikel 7 i förordning (EU) … ([2]) måste mottagarna bevara innehåll och relaterade data som har avlägsnats, eller gjorts oåtkomliga, i sex månader eller längre på begäran av behöriga myndigheter eller domstolar.

Avlägsnandeordern bör sändas på ett av de språk som mottagaren har angett i enlighet med artikel 14.2.

AVSNITT A:

Utfärdande medlemsstat: . . . . . .

ANM.: uppgifter om utfärdande myndighet ska lämnas i slutet (avsnitten E och F)

Mottagare (rättslig företrädare):

. . . . . .

Mottagare (kontaktpunkt):

. . . . . .

Medlemsstat som har jurisdiktion över mottagaren [om annan än den utfärdande staten]: . . . . . .

Tid och datum för utfärdande av avlägsnandeordern:

. . . . . .

Referensnummer för avlägsnandeordern: . . . . . .

([1]) Europaparlamentets och rådets förordning om förhindrande av spridning av terrorisminnehåll online (*EUT L…*).
([2]) Europaparlamentets och rådets förordning om förhindrande av spridning av terrorisminnehåll online (*EUT L…*).

AVSNITT B: Innehåll som ska avlägsnas eller göras oåtkomligt ~~inom en timme~~ ***utan onödigt dröjsmål*** **[Ändr. 162]**

En webbadress (URL) och all annan information som gör det möjligt att identifiera och hitta exakt plats för det anmälda innehållet:

. . . . . .

Orsaker till att innehållet anses vara terrorisminnehåll, i enlighet med artikel 2.5 i förordning (EU) xxx. Innehållet (markera relevant(a) ruta/rutor)

☐ uppviglar till~~, förespråkar eller förhärligar~~ utförande av terroristbrott ***som anges i artikel 3.1a-i i direktiv (EU) 2017/541*** (artikel 2.5 a) **[Ändr. 149]**

☐ ~~uppmuntrar bidrag~~***försöker värva en annan person eller grupp av personer för att utföra eller bidra*** till ***utförande av*** terroristbrott ***som anges i artikel 3.1 a-i i direktiv (EU) 2017/541*** (artikel 2.5 b) **[Ändr. 150]**

☐ ~~främjar~~***försöker värva en annan person eller grupp av personer till medverkan i sådan*** en terroristgrupps verksamhet~~, uppmuntrar till deltagande i eller stöd till gruppen~~ ***som anges i artikel 3.1 a-i i direktiv (EU) 2017/541***(artikel 2.5 c) **[Ändr. 151]**

☐ tillhandahåller instruktioner eller tekniker för ***tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen, eller för andra särskilda metoder eller tekniker för*** utförande av terroristbrott ***m anges i artikel 3.1 a–i i direktiv (EU) 2017/541*** (artikel 2.5 d) **[Ändr. 152]**

[] ***avbildar utförande av terroristbrott som anges i artikel 3.1a-i i direktiv (EU) 2017/541 (artikel 2.5 e).*** **[Ändr. 153]**

Ytterligare information om orsakerna till att innehållet anses vara terrorisminnehåll (frivilligt):

. . . . . .

. . . . . .

AVSNITT C: Information till innehållsleverantören

Observera att (kryssa för om det är tillämpligt)

☐ mottagaren, av hänsyn till allmän säkerhet, **inte får informera den innehållsleverantör** vars innehåll avlägsnas eller görs oåtkomligt.

I övriga fall: Uppgifter om möjligheterna att bestrida avlägsnandeordern i den utfärdande medlemsstaten (som på begäran kan vidarebefordras till innehållsleverantören) enligt nationell lagstiftning, se avsnitt G nedan.

AVSNITT D: Information till den medlemsstat som har jurisdiktion

☐ Kryssa för om den stat som har jurisdiktion över mottagaren är en annan än den utfärdande medlemsstaten:

☐ en kopia av avlägsnandeordern skickas till den relevanta behöriga myndigheten i den stat som har jurisdiktion

Onsdagen den 17 april 2019

AVSNITT E: Uppgifter om den myndighet som utfärdade avlägsnandeordern

Typ av myndighet som utfärdade denna avlägsnandeorder (kryssa för relevant ruta):

☐ domare, domstol eller undersökningsdomare

☐ brottsbekämpande myndighet

☐ annan behörig myndighet → fyll även i avsnitt F

Uppgifter om den utfärdande myndigheten och/eller dess företrädare, som intygar att avlägsnandeordern är riktig och korrekt

Myndighetens namn: . . . . . .

Myndighetens företrädare: . . . . . .

Befattning (titel/grad): . . . . . .

Dokumentnummer: . . . . . .

Adress:

Tfn: (landsnummer) (riktnummer) . . . . . .

Fax: (landsnummer) (riktnummer) . . . . . .

E-postadress: . . . . . .

Datum:

. . . . . .

Officiell stämpel (om tillämpligt) och underskrift ([1]): . . . . . .

AVSNITT F: Kontaktuppgifter för uppföljning

Kontaktuppgifter med vilka den utfärdande myndigheten kan nås för att få återkoppling om när innehållet avlägsnades eller gjordes oåtkomligt, eller för att ge ytterligare klargöranden:

. . . . . .

Kontaktuppgifter till myndigheten i den stat som har jurisdiktion över mottagaren [om annan än den utfärdande medlemsstaten]:

. . . . . .

AVSNITT G: Information om möjligheter till prövning

Information om behörigt organ eller behörig domstol, tidsfrister och förfaranden – ***inklusive formella krav*** – för bestridande av avlägsnandeordern **[Ändr. 154]**

Behörig instans eller domstol för att bestrida avlägsnandeordern:

. . . . . .

Tidsfrist för bestridande av beslutet:

Xxx månader från och med xxxx

Länk till bestämmelserna i den nationella lagstiftningen:

. . . . . .

([1]) Underskrift krävs ej vid sändning via autentiserade inlämningskanaler.

Onsdagen den 17 april 2019

BILAGA II

FORMULÄR FÖR ÅTERKOPPLING EFTER DET ATT TERRORISMINNEHÅLL AVLÄGSNATS ELLER GJORTS OÅTKOMLIGT

(artikel 4.5 i förordning (EU) xxx)

AVSNITT A:

Avlägsnandeorderns mottagare:

……

Myndighet som utfärdade avlägsnandeordern:

……

Referensnummer för den utfärdande myndigheten:

……

Referensnummer för mottagaren:

……

Tid och datum för mottagande av avlägsnandeordern:

……

AVSNITT B:

Det terrorisminnehåll som avlägsnandeordern avser har (kryssa för relevant ruta)

☐ avlägsnats

☐ gjorts oåtkomligt

Tid och datum då innehållet avlägsnades eller gjordes oåtkomligt: ……

AVSNITT C: Uppgifter om mottagaren

Namn på värdtjänstleverantören/dess rättsliga företrädare:

……

Medlemsstat där det huvudsakliga verksamhetsstället är beläget eller den rättsliga företrädaren är etablerad: ……

Namn på den bemyndigade personen:

……

Uppgifter om kontaktpunkten (e-postadress): ……

Datum:

……

Onsdagen den 17 april 2019

BILAGA III

INFORMATION OM ATT DET ÄR OMÖJLIGT ATT VERKSTÄLLA AVLÄGSNANDEORDERN (artikel 4.6 och 4.7 i förordning (EU) xxx)

AVSNITT A:

Avlägsnandeorderns mottagare:

…… . . . . . .

Myndighet som utfärdade avlägsnandeordern:

…… . . . . . .

Referensnummer för den utfärdande myndigheten:

…… . . . . . .

Referensnummer för mottagaren: ……

…….. . . . . .

Tid och datum för mottagande av avlägsnandeordern:

…… . . . . . .

AVSNITT B: Orsakerna till utebliven verkställighet

i) Avlägsnandeordern kan inte verkställas eller kan inte verkställas inom den begärda tidsfristen av följande orsaker:

☐ force majeure eller faktisk omöjlighet som inte kan tillskrivas mottagaren eller tjänsteleverantören ***, inbegripet tekniska eller driftsmässiga skäl*** **[Ändr. 155]**

☐ avlägsnandeordern innehåller uppenbara fel

☐ avlägsnandeordern innehåller inte tillräckligt med information

ii) Redogör närmare för orsakerna till utebliven verkställighet:

…… . . . . . .

iii) Om avlägsnandeordern innehåller uppenbara fel och/eller inte innehåller tillräckligt med information, precisera vilka fel och vilken ytterligare information eller vilka klargöranden som krävs:

…… . . . . . .

AVSNITT H: Uppgifter om tjänsteleverantören/dess rättsliga företrädare

Namn på tjänsteleverantören/dess rättsliga företrädare:

…… . . . . . .

Namn på den bemyndigade personen:

…… . . . . . .

Kontaktuppgifter (e-postadress):

…… . . . . . .

Underskrift:

…… . . . . . .

Tid och datum: …… . . . . . .