Europeiska unionens råd

Bryssel den 3 december 2018
(OR. en)

14978/18

Interinstitutionellt ärende:
2018/0331(COD)

CT 194
ENFOPOL 595
JAI 1232
COTER 170
CYBER 303
TELECOM 440
FREMP 216
AUDIO 112
DROIPEN 189
CODEC 2160

NOT

från:	Ordförandeskapet
till:	Rådet
Föreg. dok. nr:	14570/18
Ärende:	Förslag till Europaparlamentets och rådets förordning om förhindrande av spridning av terrorisminnehåll online – allmän riktlinje

I. INLEDNING

1. Den 12 september 2018 förelade kommissionen rådet ett förslag till förordning om förhindrande av spridning av terrorisminnehåll online[1], sedan Europeiska rådet i juni 2018 efterfrågat lagstiftning i syfte att förbättra upptäckten och raderingen av innehåll som framkallar hat och uppviglar till terroristdåd. Förslaget ingick i det säkerhetspaket som lades fram i samband med att kommissionens ordförande höll sitt tal om tillståndet i unionen.

[1] 12129/18 + ADD 1–3.

2. Den rättsliga grunden för förslaget är artikel 114 i fördraget om Europeiska unionens funktionssätt (inre marknaden). Genom den föreslagna förordningen inrättas begreppet *avlägsnandeorder*, som innebär att värdtjänstleverantörer som är verksamma på unionens territorium tvingas avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme. Bristande efterlevnad kan leda till påföljder. Det nuvarande utkastet till förslag innehåller kraftfulla skyddsåtgärder för att skydda grundläggande rättigheter och principer, i synnerhet yttrandefriheten och rätten till rättslig prövning.

3. Det nuvarande frivilliga systemet för samarbete som skapades genom EU:s internetforum, inrättat i december 2015, kommer att fortsätta.

II. ARBETET INOM RÅDET

4. Arbetsgruppen mot terrorism behandlade utkastet till förordning vid mötena den 25 september, 5 och 25 oktober samt den 6 och 15 november 2018. Efter denna grundliga behandling av utkastet till förordning på expertnivå diskuterade RIF-råden några av de kvarstående frågorna den 22 november 2018. Utkastet till förordning diskuterades dessutom i samordningskommittén på området för polissamarbete och straffrättsligt samarbete den 18 september 2018.

5. Coreper hade en första diskussion under lunchen den 26 september, diskuterade frågor om kampen mot terrorism, däribland detta förslag, med EU:s samordnare för kampen mot terrorism vid frukosten den 21 november och behandlade det senaste kompromissförslaget från ordförandeskapet den 28 november 2018, varvid ordföranden konstaterade att nödvändigt majoritetsstöd förelåg.

III. DE VIKTIGASTE FRÅGORNA

6. Med ordförandeskapets kompromissförslag införs ett antal ändringar, för att försöka lösa de flesta frågor som medlemsstaterna tagit upp. Dessa tas upp nedan i samma ordning som de förekommer i artiklarna.

– När det gäller de grundläggande rättigheterna och behovet att skydda journalistiskt innehåll har formuleringarna om grundläggande rättigheter i allmänhet och pressfriheten i synnerhet förstärkts genom att en ny punkt 3 införs i artikel 1 och genom en väsentlig ändring i slutet av skäl 9, för att ta hänsyn till publicistiska normer som fastställs genom press- eller medieregelering.

– I fråga om tillämpningsområdet har definitionen av *terrorisminnehåll* i artikel 2.5 anpassats närmare till direktivet om bekämpande av terrorism. Definitionen av *värdtjänstleverantör* har förtydligats ytterligare i skäl 10 genom att de olika beståndsdelarna i definitionen anges i detalj, det förklaras vilka tjänsteleverantörer som inte ingår i tillämpningsområdet och exempel ges på värdtjänstleverantörer som omfattas.

– Vad gäller de viktigaste instrumenten för att förhindra spridning av terrorisminnehåll online (artiklarna 4 och 5) klargörs det i artikel 4.3 a och 4.4 samt i motsvarande skäl 13a vilken information som ska lämnas till värdtjänstleverantören i avlägsnandeordern. En ny artikel 4a har lagts till om samrådsförfarandet för avlägsnandeorder. En extra hänvisning till rätten till ett effektivt rättsmedel för avlägsnandeorder har förts in i skäl 25, utöver den allmänna hänvisningen i skäl 8.

– När det gäller proaktiva åtgärder anges nu i ändringar av artikel 6.2 a och 6.4 att det är upp till medlemsstaten att välja vilken art och omfattning dessa åtgärder ska ha, när medlemsstaten beslutar om vilka proaktiva åtgärder som ska vidtas.

– Med tanke på den eventuella bördan för små och medelstora företag anges i artikel 8.2 och motsvarande skäl 24 att skyldigheten att offentliggöra transparensrapporter är begränsad till värdtjänstleverantörer som faktiskt exponeras för terrorisminnehåll.

– Enligt artikel 11.3 bör skyldigheten att lämna ut information till innehållsleverantören om att terrorisminnehåll avlägsnats inte gälla omedelbart, av hänsyn till allmän säkerhet, och den period under vilken informationen inte behöver lämnas ut har förlängts, från 4 + 4 till 6 + 6 veckor.

– I fråga om samarbete har artikel 13.3 och skälen 27 och 30 ändrats för att säkerställa samordning från medlemsstaternas sida innan de utfärdar en avlägsnandeorder och anmälningar (med förtydligande av hur dubbelarbete och störande av utredningar kan undvikas) samt uppmuntra till användning av Europols verktyg. Artikel 13.4 har ändrats för att säkerställa att anmälningar av ett allvarligt hot når rätt myndighet så snart som möjligt.

– Dessutom har ändringar införts för att minska belastningen på värdtjänstleverantörer, och det förtydligas i skäl 33 att den kontaktpunkt som föreskrivs i artikel 14 för handläggningen av avlägsnandeorder kan vara extern och att kontaktpunktens tillgänglighet dygnet runt varje dag begränsas till värdtjänstleverantörer som är exponerade för terrorisminnehåll.

– Artikel 15.3 om tvångsåtgärder och motsvarande skäl 34a har strukits.

– I artikel 24 har genomförandeperioden förlängts från sex till tolv månader.

Ett antal ändringar har gjorts i fråga om jurisdiktion och den eventuella rollen för den medlemsstat där värdtjänstleverantören är etablerad, även vad gäller rättslig prövning. I den nuvarande texten klargörs i artikel 15.1 och skäl 34 att alla medlemsstater, med hänsyn till ett effektivt genomförande, brådskande fall och allmän ordning, har jurisdiktion att utfärda avlägsnandeorder och anmälningar gentemot alla värdtjänstleverantörer, oberoende av i vilken medlemsstat värdtjänstleverantören är etablerad eller har utsett en rättslig företrädare. I skäl 27 förtydligas att dubbla avlägsnandeorder inte bör utfärdas. Dessutom har en artikel 4a lagts till om samråd med den behöriga myndigheten i den medlemsstat där värdtjänstleverantören är etablerad eller har sin rättsliga företrädare. Slutligen klargörs i skäl 38 att medlemsstaterna måste se till att de grundläggande rättigheterna respekteras fullt ut innan de utfärdar påföljder.

IV. ÖVRIGA FRÅGOR

7. Tjeckien, Danmark och Finland vidhåller en parlamentsreservation mot förslaget.

8. Europeiska ekonomiska och sociala kommittén hördes av rådet genom en skrivelse av den 24 oktober 2018 och kommer att avge sitt yttrande vid plenarsessionen i december.

9. Europaparlamentet har utsett Helga Stevens (ECR, BE), utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor (LIBE), till föredragande.

V. SLUTSATS

10. Rådet uppmanas att anta en allmän riktlinje om den bifogade texten.

11. Ändringar i förhållande till kommissionens förslag (12129/18) är markerade på följande sätt: ny text markeras med ***kursiverad fetstil,*** text som strukits i det ursprungliga kommissionsförslaget återges med [...].

BILAGA

2018/0331 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om förhindrande av spridning av terrorisminnehåll online

Ett bidrag från Europeiska kommissionen till toppmötet i Salzburg den 19–20 september 2018

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,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[2],

i enlighet med det ordinarie lagstiftningsförfarandet,

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 att värdtjänster missbrukas för terrorismändamål. Den digitala inre marknadens funktion bör förbättras genom att öka rättssäkerheten för värdtjänstleverantörer, stärka användarnas förtroende för onlinemiljön och förbättra skyddet för yttrande- och informationsfriheten.

[2] EUT C , , s. .

(2) Värdtjänstleverantörer som är aktiva på internet spelar en viktig roll i den digitala ekonomin genom att koppla samman företag och medborgare 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.

(3) Förekomsten av terrorisminnehåll online har 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 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 att förhindra att terrorisminnehåll sprids via deras tjänster.

(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 och från Europeiska rådet att förbättra den automatiska upptäckten och raderingen av innehåll som uppviglar till terroristdåd.

[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).

(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. ***Denna förordning tillämpas inte på verksamhet som rör nationell säkerhet, eftersom detta också i fortsättningen är varje medlemsstats eget ansvar.***

(6) Regler för att förhindra 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 de grundläggande rättigheter som skyddas i unionens rättsordning och i synnerhet de som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna.

---

[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).

(7) Denna förordning bidrar till att skydda den allmänna säkerheten, samtidigt som 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 yttrande- och informationsfriheten ***samt pressfriheten och mediepluralismen,*** som utgör [...] [...] en väsentlig grund för ett pluralistiskt, demokratiskt samhälle och är ett av unionens grundläggande värden. Åtgärder som utgör ingrepp i yttrande- och informationsfriheten bör vara strikt riktade, i den bemärkelsen att de måste tjäna till att förhindra spridning av terrorisminnehåll, 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.

(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 personens rättigheter. Rätten inbegriper särskilt värdtjänstleverantörernas och innehållsleverantörernas möjlighet att effektivt bestrida avlägsnandeorder inför domstol i den medlemsstat vars myndigheter utfärdade avlägsnandeordern ***och värdtjänstleverantörernas möjlighet att bestrida ett beslut om föreskrivande av proaktiva åtgärder eller påföljder inför domstol i den medlemsstat där de är etablerade eller har en rättslig företrädare***.

(9) För att ge klarhet om de åtgärder som både värdtjänstleverantörer och behöriga myndigheter bör vidta för att förhindra 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 skadligaste terroristpropagandan online bör definitionen omfatta material [...] som uppviglar till, uppmuntrar eller förespråkar utförande av eller bidrag till terroristbrott, [...] eller främjar deltagande i en terroristgrupps verksamhet. [...]***Definitionen omfattar innehåll som ger vägledning för tillverkning och användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen samt CBRN-ämnen, eller om andra metoder och tekniker, bland annat urval av objekt i syfte att begå terroristbrott.*** [...]***Sådant material*** 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, [...]***som motbudskap*** eller i forskningssyfte bör skyddas på lämpligt sätt***, samtidigt som rätt balans uppnås mellan grundläggande rättigheter, inbegripet framför allt yttrande- och informationsfrihet, och hänsyn till allmän säkerhet***. ***Om det spridda materialet offentliggörs under en innehållsleverantörs redaktionella ansvar bör man vid alla beslut att avlägsna sådant innehåll ta hänsyn till publicistiska normer, som fastställts genom press- eller medieregler och som överensstämmer med unionens lagstiftning, och rätten till yttrandefrihet samt mediernas frihet och mångfald, i enlighet med artikel 11 i 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.

---

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).

(10) För att omfatta de onlinevärdtjänster där terrorisminnehåll sprids, bör denna förordning tillämpas på informationssamhällets tjänster som på begäran av en tjänstemottagare lagrar information ***och material*** som tillhandahållits av denna tjänstemottagare och gör den lagrade informationen tillgänglig för tredje part, oavsett om denna verksamhet ***och detta material*** är av rent teknisk, automatisk och passiv karaktär. […] ***Lagring av innehåll innebär att man innehar uppgifter i minnet till en fysisk eller virtuell server. Härigenom utesluts enbart vidarebefordran och andra ekonomiska elektroniska kommunikationstjänster i den mening som avses i [europeisk kodex för elektronisk kommunikation] eller leverantörer av cachelagringstjänster från tillämpningsområdet, eller andra tjänster som tillhandahålls på andra nivåer av internetinfrastrukturen, som t.ex. register eller registratorer, DNS (domännamnssystem) eller angränsande tjänster, som t.ex. betalningstjänster eller skyddstjänster mot DDoS (samordnad överbelastningsattack). Vidare måste informationen lagras på begäran av innehållsleverantören; endast de tjänster som innehållsleverantören är direkt mottagare av omfattas av förordningen. Den lagrade informationen görs slutligen tillgänglig för tredje part, vilket avser alla tredje användare som inte är innehållsleverantören. Interpersonella kommunikationstjänster som möjliggör direkt interpersonellt och interaktivt informationsutbyte mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna, omfattas ej.*** Sådana ***värdtjänstleverantörer*** [...] är t.ex. sociala medieplattformar, direktuppspelningstjänster, video-, bild- och ljuddelningstjänster, fildelningstjänster och andra ***moln- och lagringstjänster*** […]. ***Denna förordning gäller tillhandahållandet av värdtjänster snarare än specifika leverantörer eller deras huvudverksamhet, som kan kombinera värdtjänster med andra tjänster som inte omfattas av denna förordning***.

(10a) 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.

(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.

---

[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).

(12) Värdtjänstleverantörer bör följa vissa aktsamhetskrav för att förhindra att terrorisminnehåll sprids på deras tjänster. Dessa aktsamhetskrav bör inte utgöra en allmän övervakningsskyldighet. 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 och informationsfriheten.

(13) En harmonisering bör ske av förfarandet för och de skyldigheter som följer av rättsliga beslut 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, brottsbekämpande eller rättsliga myndigheter 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. ***Utan att det påverkar skyldigheten att bevara data enligt artikel 7 i denna förordning, eller enligt [utkastet till lagstiftning om e-bevisning], <u>är det</u>*** upp till värdtjänstleverantörerna att besluta om de ska avlägsna innehållet i fråga eller göra det oåtkomligt för användarna i unionen. ***Detta bör leda till förhindrad eller åtminstone försvårad åtkomst och till att de internetanvändare som använder deras tjänster i hög grad avhålls från att få åtkomst till innehåll som har gjorts oåtkomligt***.

(13a) Avlägsnandeordern bör inbegripa en klassificering av det relevanta innehållet som terrorisminnehåll samt innehålla tillräcklig information för att lokalisera innehållet genom att tillhandahålla en webbadress och eventuell ytterligare information, som t.ex. en skärmdump av innehållet i fråga. På begäran bör den behöriga myndigheten lämna en kompletterande motivering, med en förklaring till varför innehållet anses vara terrorisminnehåll. Motiveringen bör inte innehålla känslig information som skulle kunna äventyra utredningen. Motiveringen bör dock göra det möjligt för värdtjänstleverantören, och i slutändan innehållsleverantören, att faktiskt utöva sin rätt till rättslig prövning.

(14) Den behöriga myndigheten bör översända avlägsnandeordern direkt till mottagaren och kontaktpunkten 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 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].

[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).

(15) [...] ***Anmälningsmekanismen*** för att uppmärksamma värdtjänstleverantörer på information ***och material*** som kan anses vara terrorisminnehåll, så att de på frivillig basis kan bedöma om innehållet är förenligt ***med*** de egna användarvillkoren***, utgör ett*[...] *särskilt effektivt, snabbt och proportionellt sätt att göra värdtjänstleverantörer medvetna om specifikt innehåll på deras tjänster***[…]. 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.

(16) Med tanke på terrorisminnehållets omfattning och den snabbhet som krävs för att effektivt identifiera och avlägsna det, är proportionella proaktiva 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 åtgärder beroende på riskerna för och graden av utsatthet för terrorisminnehåll, samt inverkan på tredje parters rättigheter och allmänhetens intresse av information. Därför bör värdtjänstleverantörer fastställa vilken lämplig, effektiv och proportionell proaktiv åtgärd som bör vidtas. Detta krav bör inte innebära någon allmän övervakningsskyldighet. I samband med denna bedömning är det ett tecken på en låg ***risk eller*** nivå av utsatthet för terrorisminnehåll om inga avlägsnandeorder och anmälningar har riktats till värdtjänstleverantören.

---

[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).

(17) När proaktiva åtgärder införs bör värdtjänstleverantörer säkerställa att användarnas rätt till yttrandefrihet och informationsfrihet – inklusive friheten att ta emot och sprida uppgifter – 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.

(18) För att säkerställa att de värdtjänstleverantörer som utsätts för terrorisminnehåll vidtar lämpliga åtgärder för att förhindra att deras tjänster missbrukas, bör de behöriga myndigheterna begära att värdtjänstleverantörer som har mottagit en 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 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 effektiva och proportionella och, om automatiska metoder används, huruvida värdtjänstleverantören har de nödvändiga förutsättningarna för mänsklig tillsyn och kontroll. Vid bedömningen av åtgärdernas effektivitet och proportionalitet bör de behöriga myndigheterna beakta relevanta parametrar såsom antalet avlägsnandeorder och anmälningar som utfärdats till leverantören, dess ekonomiska kapacitet och tjänstens inverkan på spridningen av terrorisminnehåll (t.ex. med beaktande av antalet användare i unionen).

(19) Efter begäran bör den behöriga myndigheten inleda en dialog med värdtjänstleverantören om de nödvändiga proaktiva åtgärder som ska vidtas. Vid behov bör den behöriga myndigheten föreskriva antagande av lämpliga, effektiva och proportionella proaktiva åtgärder om den anser att de åtgärder som vidtagits inte är tillräckliga för att hantera riskerna. Ett beslut att föreskriva 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.

(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. uppgifter om innehållsleverantörens identitet, ***”transaktionsdata” 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.

(21) Skyldigheten att bevara innehållet för administrativa eller rättsliga prövningsförfaranden 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 lagföringsändamål 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 åtgärder, och inte informerar den berörda myndigheten eftersom de bedömer att det inte omfattas av artikel 13.4 i denna förordning, kan de brottsbekämpande myndigheterna vara omedvetna om att innehållet existerar. Därför är det också motiverat att bevara innehåll för att förebygga, upptäcka, utreda och lagföra terroristbrott. För dessa ändamål 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.

(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 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 inleds men inte avslutas inom sexmånadersperioden, på begäran av den myndighet som genomför prövningen. Denna period bör vara tillräcklig för att de brottsbekämpande myndigheterna ska kunna bevara bevis som är nödvändiga för utredningar, samtidigt som balansen i förhållande till de berörda grundläggande rättigheterna säkerställs.

(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. Värdtjänstleverantörer ***som är utsatta för terrorisminnehåll*** bör offentliggöra årliga transparensrapporter som innehåller meningsfull information om åtgärder som vidtagits för att upptäcka, identifiera och avlägsna terrorisminnehåll***, såvida det inte motverkar syftet med de åtgärder som införts***.

(25) Klagomålsförfaranden utgör en nödvändig skyddsåtgärd mot felaktigt avlägsnande av innehåll***, till följd av åtgärder som vidtagits i enlighet med värdtjänstleverantörernas användarvillkor,*** som är skyddat genom yttrandefriheten och informationsfriheten. 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. ***Vidare bör innehållsleverantörer vars innehåll har avlägsnats efter en avlägsnandeorder ha rätt till ett effektivt rättsmedel i enlighet med artikel 19 i EU-fördraget och artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna***.

(26) ***Mer allmänt krävs, f***[...]ör ett effektivt rättsligt skydd enligt artikel 19 i EU-fördraget och artikel 47 i Europeiska unionens stadga om de grundläggande rättigheterna, 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 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.

(27) För att undvika dubbelarbete och möjlig störning av utredningar bör de behöriga myndigheterna informera, samordna sig med och samarbeta med varandra och Europol, när så är lämpligt, [...] ***innan*** de utfärdar avlägsnandeorder eller ***när de*** anmäler innehåll till värdtjänstleverantörer. ***När beslut fattas om att utfärda en avlägsnandeorder bör den behöriga myndigheten ta vederbörlig hänsyn till alla anmälningar om en konflikt med utredningsmässiga intressen (”konfliktlösning”). Om en behörig myndighet får information från en behörig myndighet i en annan medlemsstat om en befintlig avlägsnandeorder bör ordern inte utfärdas i två exemplar.*** Vid genomförandet av bestämmelserna i denna förordning kan Europol tillhandahålla stöd i enlighet med dess nuvarande mandat och befintliga rättsliga ram.

(28) I syfte att säkerställa ett effektivt och tillräckligt enhetligt genomförande av proaktiva åtgärder bör de behöriga myndigheterna i medlemsstaterna samarbeta med varandra i fråga om de diskussioner de har med värdtjänstleverantörerna avseende 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. ***Kommissionen bör underlätta sådan samordning och sådant samarbete.***

(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 relevanta behöriga myndigheten. För detta ändamål bör medlemsstaterna säkerställa lämpliga kommunikationskanaler och mekanismer som gör det möjligt att dela den relevanta informationen i rätt tid.

(30) För att underlätta ett snabbt utbyte mellan behöriga myndigheter och värdtjänstleverantörer, och för att undvika dubbelarbete, [...] ***uppmanas*** medlemsstaterna att använda sig av ***de särskilda*** 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[10].

(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***, interna eller externa,*** som möjliggör elektronisk inlämning av avlägsnandeorder och anmälningar och av tekniska resurser […] ***eller*** 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 ***de värdtjänstleverantörer som är exponerade för terrorisminnehåll, vilket framgår av att de har tagit emot en avlägsnandeorder,*** 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 värdtjänstleverantörerna och de behöriga myndigheterna, uppmuntras värdtjänstleverantörer att tillåta kommunikation på ett av unionens officiella språk som deras användarvillkor finns tillgängliga på.

(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. ***Med hänsyn till ett effektivt genomförande, brådskande fall och allmän ordning bör alla medlemsstater ha jurisdiktion i fråga om avlägsnandeorder och anmälningar.***

---

10 COM(2018)225 final.

(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 kan använda sig av en befintlig rättslig företrädare, under förutsättning att denna rättsliga företrädare kan fullgöra de funktioner som anges i denna förordning***.

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

(37) Medlemsstaterna bör utse behöriga myndigheter för tillämpningen av denna förordning. Kravet på att utse behöriga myndigheter förutsätter inte nödvändigtvis att nya myndigheter inrättas, utan de kan vara befintliga organ som ges i uppdrag att sköta de funktioner som anges i denna förordning. Denna förordning kräver att det utses myndigheter som ska vara behöriga att utfärda avlägsnandeorder och anmälningar, övervaka proaktiva åtgärder och fastställa påföljder. Det är upp till medlemsstaterna att bestämma hur många myndigheter de vill utse för dessa uppgifter.

(38) Påföljder är nödvändiga för att säkerställa att värdtjänstleverantörerna effektivt genomför sina skyldigheter enligt denna förordning. Medlemsstaterna bör anta bestämmelser om påföljder***, som kan vara av administrativ eller straffrättslig art, inbegripet [...]*** riktlinjer för bötfällning när så är lämpligt. Särskilt stränga påföljder ska fastställas om värdtjänstleverantören systematiskt 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. 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 av ytterligare proaktiva åtgärder enligt artikel 6.4. ***När man bedömer överträdelsens art och beslutar om tillämpning av påföljder bör de grundläggande rättigheterna, exempelvis yttrandefriheten, respekteras fullständigt***. Vid fastställande av huruvida böter bör föreskrivas, bör vederbörlig hänsyn tas till leverantörens ekonomiska resurser. Medlemsstaterna ska säkerställa att påföljderna inte uppmuntrar till avlägsnande av innehåll som inte är terrorisminnehåll.

(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 om bättre lagstiftning av den 13 april 2016[11]. 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. ***Medlemsstaterna får använda sig av värdtjänstleverantörernas transparensrapporter och, vid behov, komplettera med mer detaljerad information***. Ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter bör fastställas som underlag för en utvärdering av lagstiftningen.

---

[11] EUT L 123, 12.5.2016, s. 1.

(42) På grundval av resultaten och slutsatserna i genomföranderapporten och resultaten av övervakningen bör kommissionen genomföra en utvärdering av denna förordning tidigast tre år efter dess ikraftträdande. Utvärderingen bör bygga på de fem kriterierna effektivitet, ändamålsenlighet, relevans, samstämmighet och mervärde för EU. Man kommer att 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 intressen, inklusive en översyn av kravet på att informera innehållsleverantörerna.

(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 enhetliga regler för att förhindra att värdtjänster missbrukas för spridning av terrorisminnehåll online. Här fastställs i synnerhet följande:

   a) Regler om aktsamhetskrav som värdtjänstleverantörer ska iaktta för att förhindra spridning av terrorisminnehåll via deras tjänster och vid behov säkerställa ett snabbt avlägsnande.

   b) En rad åtgärder som medlemsstaterna ska vidta för att identifiera terrorisminnehåll, göra det möjligt för värdtjänstleverantörerna att snabbt avlägsna det samt underlätta samarbete med behöriga myndigheter i andra medlemsstater, med värdtjänstleverantörer och i tillämpliga fall med relevanta unionsorgan.

2. Denna förordning ska tillämpas på värdtjänstleverantörer som erbjuder tjänster i unionen, oberoende av deras huvudsakliga verksamhetsställe.

3. ***Denna förordning påverkar inte skyldigheten att respektera de grundläggande rättigheterna och de grundläggande rättsliga principerna i artikel 6 i fördraget om Europeiska unionen.***

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

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.

2. *innehållsleverantör*: en användare som har tillhandahållit information som lagras eller har lagrats av en värdtjänstleverantör på användarens begäran.

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 har ett verksamhetsställe i unionen.

   I avsaknad av ett sådant verksamhetsställe ska bedömningen av en betydande anknytning grundas på särskilda faktiska kriterier såsom att värdtjänstleverantören

   a) har ***ett*** betydande antal användare i en eller flera medlemsstater

   b) ***eller*** riktar verksamheten till en eller flera medlemsstater.

4. *terroristbrott*: ***en av de uppsåtliga gärningar som anges*** […] i artikel 3.1 i direktiv (EU) 2017/541.

5. *terrorisminnehåll*: […] ***material som kan bidra till utförande av de uppsåtliga gärningar som anges i artikel 3.1 a–i i direktiv (EU) 2017/541, genom***

   aa) hot om att utföra ett terroristbrott,

   a) [...] uppvigling till eller förespråkande av utförande av terroristbrott, ***t.ex.*** […] ***genom förhärligande av terroristgärningar,*** vilket innebär en risk för att sådana handlingar utförs,

   b) ***värvning av personer eller en grupp personer för att utföra eller bidra*** [...] till terroristbrott,

c) ***främjande av*** en terroristgrupps verksamhet, i synnerhet genom att ***personer eller en grupp personer värvas för att delta i eller stödja brottslig verksamhet som utövas av*** [...] en terroristgrupp i den mening som avses i artikel 2.3 i direktiv (EU) 2017/541,

utlärande av metoder eller tekniker för att utföra terroristbrott.

6. *spridning av terrorisminnehåll*:att göra terrorisminnehåll tillgängligt för tredje part via värdtjänstleverantörernas tjänster.

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.

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

AVSNITT II

Åtgärder för att förhindra spridning av terrorisminnehåll online

Artikel 3

Aktsamhetskrav

1. Värdtjänstleverantörer ska vidta lämpliga, rimliga och proportionella åtgärder i enlighet med denna förordning för att motverka spridning av terrorisminnehåll och skydda användarna mot terrorisminnehåll. När de gör detta ska de handla på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt, med vederbörlig hänsyn till användarnas grundläggande rättigheter och med beaktande av den grundläggande vikten av yttrandefrihet och informationsfrihet i ett öppet och demokratiskt samhälle.

2. Värdtjänstleverantörer ska i sina användarvillkor inbegripa ***att de inte kommer att lagra terrorisminnehåll***, och tillämpa bestämmelser för att förhindra spridning av terrorisminnehåll.

Artikel 4

Avlägsnandeorder

1. Den behöriga myndigheten ska ha befogenhet att utfärda […] **en avlägsnandeorder** som kräver att värdtjänstleverantören avlägsnar terrorisminnehåll eller gör det oåtkomligt.

2. Värdtjänstleverantörer ska avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme från mottagandet av avlägsnandeordern.

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

   a) Uppgift om den behöriga myndighet som utfärdat avlägsnandeordern och den behöriga myndighetens autentisering av avlägsnandeordern.[…] ***En bedömning av innehållet***, åtminstone genom hänvisning till de ***relevanta*** kategorier av terrorisminnehåll som anges i artikel 2.5.

b) En webbadress (URL) och, vid behov, ytterligare information som gör det möjligt att identifiera det innehåll som anmäls.

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

d) Datum och tidpunkt för utfärdande.

e) Information om värdtjänstleverantörens och innehållsleverantörens prövningsmöjligheter.

f) I tillämpliga fall, beslutet att inte lämna ut information om att terrorisminnehåll avlägsnats eller gjorts oåtkomligt i den mening som avses i artikel 11.

4. På värdtjänstleverantörens eller innehållsleverantörens begäran ska den behöriga myndigheten lämna en […] ***kompletterande*** motivering, ***med en redogörelse för varför innehållet anses vara terrorisminnehåll***, utan att det påverkar värdtjänstleverantörens skyldighet att följa avlägsnandeordern inom den tidsfrist som anges i punkt 2.

5. De behöriga myndigheterna 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.

6. ***Utan onödigt dröjsmål ska*** värdtjänstleverantörer […] bekräfta mottagandet och […] 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.

7. Om värdtjänstleverantören inte kan följa avlägsnandeordern på grund av force majeure eller faktisk omöjlighet som inte kan tillskrivas värdtjänstleverantören, 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.

8. Om värdtjänstleverantören inte kan följa avlägsnandeordern eftersom ordern innehåller uppenbara fel eller inte innehåller tillräcklig information för att verkställa den, 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.

9. Den behöriga myndighet som utfärdade avlägsnandeordern ska informera den behöriga myndighet som övervakar genomförandet av proaktiva 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.

Artikel 4a

Samrådsförfarande för avlägsnandeorder

1. Den myndighet som utfärdar avlägsnandeordern ska översända en kopia av denna till den behöriga myndighet som avses i artikel 17.1 a i den medlemsstat där värdtjänstleverantörens huvudsakliga verksamhetsställe är beläget samtidigt som den översänds 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, informera den utfärdande behöriga myndigheten.

3. Den utfärdande myndigheten ska beakta dessa omständigheter och, vid behov, dra tillbaka eller anpassa avlägsnandeordern.

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 tillräcklig […] information ***om*** 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.

6. Värdtjänstleverantören ska ***utan onödigt dröjsmål*** […] 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.

Artikel 6

Proaktiva åtgärder

1. Värdtjänstleverantörer ska […], ***beroende på risken för och graden av utsatthet för terrorisminnehåll,*** vidta proaktiva åtgärder för att skydda sina tjänster mot spridning av terrorisminnehåll. Åtgärderna ska vara verkningsfulla och proportionella, med beaktande av risken för och graden av utsatthet för terrorisminnehåll, användarnas grundläggande rättigheter och den grundläggande vikten av yttrandefrihet och informationsfrihet i ett öppet och demokratiskt samhälle.

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) […] ***effektivt åtgärda*** att innehåll som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det anses vara terrorisminnehåll […] ***dyker*** 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.

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.

4. Om en överenskommelse inte kan nås inom tre månader från begäran enligt punkt 3 får den behöriga myndighet som avses i artikel 17.1 c utfärda ett beslut om att föreskriva ytterligare specifika nödvändiga och proportionella proaktiva åtgärder. […] Beslutet ska särskilt ta hänsyn till värdtjänstleverantörens ekonomiska kapacitet samt sådana åtgärders inverkan på användarnas grundläggande rättigheter och den grundläggande vikten av yttrandefrihet och informationsfrihet. ***Det är den behöriga myndighet som avses i artikel 17.1 c som ska besluta om de proaktiva åtgärdernas karaktär och omfattning, i enlighet med målet för denna förordning.*** Ett sådant beslut 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.

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.

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 åtgärder enligt artiklarna 4, 5 och 6, samt relaterade data som avlägsnats till följd av att terrorisminnehållet har avlägsnats**,** […] som är nödvändigt för

   a) administrativa eller rättsliga prövningsförfaranden,

   b) förebyggande, upptäckt, utredning och lagföring av terroristbrott.

2. Det terrorisminnehåll och de relaterade data som avses i punkt 1 ska bevaras i sex månader. Terrorisminnehållet ska, på den behöriga myndighetens eller domstolens begäran, bevaras under en längre period om och så länge som det krävs för ett sådant pågående administrativt eller rättsligt prövningsförfarande som avses i punkt 1 a.

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

1. Värdtjänstleverantörer ska i sina användarvillkor fastställa sin strategi för att förhindra spridningen av terrorisminnehåll, när så är lämpligt även en meningsfull förklaring av hur proaktiva åtgärder, bland annat användningen av automatiska verktyg, fungerar.

2. Värdtjänstleverantörer […] ***som är utsatta för terrorisminnehåll*** ska offentliggöra årliga transparensrapporter om åtgärder som vidtagits för att förhindra spridningen av terrorisminnehåll.

3. Transparensrapporterna ska innehålla minst följande information:

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

   b) Information om värdtjänstleverantörens åtgärder för att ***på ett effektivt sätt åtgärda*** […] att innehåll som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det anses vara terrorisminnehåll ***dyker*** upp på nytt.

   c) Mängd terrorisminnehåll som avlägsnats eller gjorts oåtkomligt efter avlägsnandeorder, anmälningar respektive proaktiva åtgärder.

   d) Översikt och resultat av klagomålsförfaranden.

Artikel 9

Skyddsåtgärder avseende användningen och genomförandet av proaktiva åtgärder

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.

2. Skyddsåtgärderna ska särskilt omfatta mänsklig tillsyn och kontroll, när detta är lämpligt och i alla händelser när det krävs en detaljerad bedömning av det relevanta sammanhanget för att avgöra om innehållet ska anses vara terrorisminnehåll eller inte.

Artikel 10

Klagomålsmekanismer

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

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.

Artikel 11

Information till innehållsleverantörer

1. Om värdtjänstleverantörer har avlägsnat terrorisminnehåll eller gjort det oåtkomligt, ska de tillhandahålla information till innehållsleverantören om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

2. På innehållsleverantörens begäran ska värdtjänstleverantören informera innehållsleverantören om orsakerna till att innehållet avlägsnades eller gjordes oåtkomligt och möjligheterna att bestrida beslutet.

3. Skyldigheten enligt punkterna 1 och 2 ska inte gälla om den behöriga myndigheten beslutar 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 […] ***sex***[…] veckor efter beslutet. ***Perioden kan förlängas en gång med ytterligare sex veckor, om det är motiverat.*** I sådana fall ska värdtjänstleverantören inte lämna någon information om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

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.

Artikel 13

Samarbete mellan värdtjänstleverantörer, behöriga myndigheter och i tillämpliga fall […] ***behöriga*** *unionsorgan*

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

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 kommunikationskanaler eller mekanismer för att säkerställa att den relevanta informationen delas inom rimlig tid.

3. ***För att denna förordning ska tillämpas på ett effektivt sätt och för att undvika dubbelarbete får*** medlemsstater och värdtjänstleverantörer välja att använda särskilda verktyg, […] även sådana som inrättats av […] ***behöriga*** unionsorgan som t.ex. Europol, för att särskilt underlätta

a) handläggning och återkoppling avseende avlägsnandeorder enligt artikel 4,

b) handläggning och återkoppling avseende anmälningar enligt artikel 5,

c) samarbete i syfte att identifiera och genomföra proaktiva åtgärder enligt artikel 6.

4. Om värdtjänstleverantörer får kännedom om bevis för terroristbrott ska de omedelbart underrätta de myndigheter som är behöriga att utreda och lagföra brott i den eller de[…] berörda medlemsstat***erna***[…]. ***Om det är omöjligt att identifiera den eller de berörda medlemsstaterna ska*** värdtjänstleverantörerna […] ***underrätta kontaktpunkten i den mening som avses i artikel 14.3 i den medlemsstat där de har sitt huvudsakliga verksamhetsställe eller en rättslig företrädare och också*** vidarebefordra denna information till Europol för lämplig uppföljning.

Artikel 14

Kontaktpunkter

1. Värdtjänstleverantörer 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 4 och 5. De ska säkerställa att denna information offentliggörs.

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, kontaktpunkten kan kontaktas och ytterligare utbyten avseende avlägsnandeorder och anmälningar enligt artiklarna 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.

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.

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. ***Alla medlemsstater ska ha jurisdiktion i fråga om artiklarna 4 och 5, oberoende av var värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller var denne har utsett en rättslig företrädare.***

2. Om en värdtjänstleverantör inte har utsett en rättslig företrädare ska samtliga medlemsstater ha jurisdiktion. ***Om en medlemsstat beslutar att utöva jurisdiktion ska den informera alla övriga medlemsstater.***

3. […]

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, 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.

2. Värdtjänstleverantören ska anförtro den rättsliga företrädaren mottagande, efterlevnad och verkställighet av avlägsnandeorder, anmälningar, 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.

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 eller de myndigheter som är behörig att

   a) utfärda avlägsnandeorder i enlighet med artikel 4,

   b) upptäcka och identifiera terrorisminnehåll och anmäla terrorisminnehåll till värdtjänstleverantörer i enlighet med artikel 5,

   c) övervaka genomförandet av proaktiva åtgärder i enlighet med artikel 6,

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

2. Senast [***tolv*** […] *månader efter denna förordnings ikraftträdande*] ska medlemsstaterna underrätta kommissionen om ***den eller*** de behöriga myndigheter som avses i punkt 1. Kommissionen ska offentliggöra underrättelsen och eventuella ändringar därav i *Europeiska unionens officiella tidning*.

Artikel 18

Påföljder

1. Medlemsstaterna ska fastställa regler om påföljder vid värdtjänstleverantörers 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

   a) artikel 3.2 (värdtjänstleverantörernas användarvillkor),

   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),

d) artikel 6.2 och 6.4 (rapporter om proaktiva åtgärder och antagande av åtgärder efter ett beslut som föreskriver specifika proaktiva åtgärder),

e) artikel 7 (bevarande av data),

f) artikel 8 (transparens),

g) artikel 9 (skyddsåtgärder i samband med proaktiva åtgärder),

h) artikel 10 (klagomålsförfaranden),

i) artikel 11 (information till innehållsleverantörer),

j) artikel 13.4 (information om bevis på terroristbrott),

k) artikel 14.1 (kontaktpunkter),

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

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

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 ***eller fysiska*** person som hålls ansvarig gjort sig skyldig till,

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

e) värdtjänstleverantörens vilja att samarbeta med de behöriga myndigheterna.

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

Artikel 19

Tekniska krav och ändringar av mallarna för avlägsnandeorder

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

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.

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 4 och 5.

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.

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 år från och med 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 effektiviteten i skyddsmekanismerna. Vid behov ska rapporten åtföljas av förslag till rättsakter. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta denna rapport.

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 [***12*** […] månader efter ikraftträdandet].

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

Utfärdad i Bryssel den

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