III

(Förberedande akter)

RÅDET

RÅDETS STÅNDPUNKT(EU) nr 6/2021VID FÖRSTA BEHANDLINGEN

inför antagandet av Europaparlamentets och rådets förordning om åtgärder mot spridning av terrorisminnehåll online

Antagen av rådet den 16 mars 2021

(Text av betydelse för EES)

(2021/C 135/01)

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 ([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 motverka att värdtjänster missbrukas för terrorismändamål samt bidra till den allmänna säkerheten i hela unionen. Den digitala inre marknadens funktion bör förbättras genom att rättssäkerheten ökas för värdtjänstleverantörer och användarnas förtroende för onlinemiljön stärks, samt genom att skyddet för yttrandefriheten förbättras, inbegripet friheten att ta emot och sprida information och idéer i ett öppet och demokratiskt samhälle och mediernas frihet och mångfald.

(2) Regleringsåtgärder för att åtgärda spridningen av terrorisminnehåll online bör kompletteras med strategier från medlemsstaternas sida för att ta itu med terrorism, inbegripet förstärkning av mediekompetens och kritiskt tänkande, utveckling av alternativa budskap och motbudskap samt andra initiativ för att minska effekterna av och mottagligheten för terrorisminnehåll online, liksom investeringar i socialt arbete, avradikaliseringsinitiativ och fördjupade kontakter med berörda samhällsgrupper, för att på ett hållbart sätt förebygga radikalisering i samhället.

(3) Åtgärder mot terrorisminnehåll online, som är en aspekt av ett större problem med olagligt innehåll online, kräver en kombination av lagstiftningsåtgärder, andra åtgärder än lagstiftningsåtgärder samt frivilliga åtgärder som bygger på samarbete mellan myndigheter och värdtjänstleverantörer, på ett sätt som säkerställer fullständig respekt för grundläggande rättigheter.

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

([2]) Europaparlamentets ståndpunkt av den 17 april 2019 (ännu inte offentliggjord i EUT) och rådets ståndpunkt vid första behandlingen av den 16 mars 2021. Europaparlamentets ståndpunkt av den … (ännu inte offentliggjord i EUT).

(4) 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. Värdtjänstleverantörers tjänster missbrukas dock i vissa fall av tredje parter för ändamålet att bedriva olaglig verksamhet online. Särskilt oroande är att terroristgrupper och deras anhängare missbrukar dessa tjänster för att sprida terrorisminnehåll online i syfte att få ut sitt budskap, radikalisera och rekrytera följare samt för att främja och styra terroristverksamhet.

(5) Även om förekomsten av terrorisminnehåll online inte är den enda faktorn, har den visat sig vara en katalysator för radikalisering av enskilda personer som kan leda till terroristgärningar och får därför allvarliga negativa konsekvenser för användare, medborgare och samhället i stort samt för de leverantörer av onlinetjänster som hyser sådant innehåll, eftersom det undergräver användarnas förtroende och skadar deras affärsmodeller. Med tanke på värdtjänstleverantörernas centrala roll och de tekniska resurser och den tekniska kapacitet som förknippas med de tjänster de tillhandahåller har värdtjänstleverantörerna ett särskilt samhällsansvar att skydda sina tjänster mot missbruk av terrorister och att bidra till att ta itu med terrorisminnehåll som sprids online via deras tjänster, och samtidigt beakta yttrandefrihetens grundläggande betydelse, inbegripet friheten att ta emot och sprida information och idéer i ett öppet och demokratiskt samhälle.

(6) Insatser på unionsnivå för att motverka terrorisminnehåll online inleddes 2015 genom en ram för frivilligt samarbete mellan medlemsstater och värdtjänstleverantörer. Dessa insatser 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 den rättsliga ramen 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 online i överensstämmelse med den övergripande ram som inrättades genom Europaparlamentets och rådets direktiv 2000/31/EG ([4]), liksom från Europeiska rådet för att förbättra upptäckten och avlägsnandet av innehåll online som anstiftar till terroristgärningar.

(7) Denna förordning bör inte påverka tillämpningen av direktiv 2000/31/EG. I synnerhet bör inga åtgärder som en värdtjänstleverantör vidtar i enlighet med denna förordning, inbegripet specifika åtgärder, i sig leda till att den värdtjänstleverantören förlorar möjligheten till det undantag från ansvar som föreskrivs i det direktivet. Denna förordning påverkar inte de nationella myndigheternas och domstolarnas befogenheter att fastställa värdtjänstleverantörernas ansvar när villkoren för undantag från ansvar i det direktivet inte är uppfyllda.

(8) Om denna förordning står i konflikt med Europaparlamentets och rådets direktiv 2010/13/EU ([5])när det gäller bestämmelser om audiovisuella medietjänster enligt definitionen i artikel 1.1 a i det direktivet bör direktiv 2010/13/EU ha företräde. Detta bör inte påverka skyldigheterna enligt denna förordning, i synnerhet vad gäller leverantörer av videodelningsplattformar.

(9) Denna förordning bör fastställa regler som ska motverka att värdtjänster missbrukas för spridning av terrorisminnehåll online i syfte att garantera att den inre marknaden fungerar smidigt. Dessa regler bör fullt ut respektera de grundläggande rättigheter som skyddas i unionen och i synnerhet de som garanteras i Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*).

([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).

([5]) Europaparlamentets och rådets direktiv 2010/13/EU av den 10 mars 2010 om samordning av vissa bestämmelser som fastställs i medlemsstaternas lagar och andra författningar om tillhandahållande av audiovisuella medietjänster (direktiv om audiovisuella medietjänster) (EUT L 95, 15.4.2010, s. 1).

(10) Syftet med denna förordning är att bidra till att skydda den allmänna säkerheten, samtidigt som lämpliga och stabila skyddsåtgärder fastställs för att säkerställa skyddet av grundläggande rättigheter, inbegripet rätten till respekt för privatlivet, till skydd av personuppgifter, till yttrandefrihet, inklusive friheten att ta emot och sprida information, näringsfriheten samt rätten till ett effektivt rättsmedel. Dessutom är all diskriminering förbjuden. Behöriga myndigheter och värdtjänstleverantörer bör endast anta åtgärder som är nödvändiga, lämpliga och proportionella i ett demokratiskt samhälle, med beaktande av den särskilda vikt som tillmäts yttrande- och informationsfriheten samt mediernas frihet och mångfald, vilka är själva grunden för ett pluralistiskt och demokratiskt samhälle och utgör värden som unionen bygger på. Åtgärder som påverkar yttrande- och informationsfriheten bör vara strikt riktade för att åtgärda spridning av terrorisminnehåll online, samtidigt som rätten att lagligen ta emot och sprida information respekteras, med beaktande av värdtjänstleverantörernas centrala roll i att främja offentlig debatt samt delande och mottagande av fakta, åsikter och idéer, i enlighet med lagen. Effektiva åtgärder online för bekämpning av terrorisminnehåll online och skyddet av yttrande- och informationsfriheten utgör inte motstridiga mål, utan kompletterar och ömsesidigt förstärker varandra.

(11) För att ge klarhet om de åtgärder som både värdtjänstleverantörer och behöriga myndigheter ska vidta för att åtgärda spridningen av terrorisminnehåll online bör denna förordning innehålla en definition av *terrorisminnehåll* i förebyggande syfte, som överensstämmer med definitionerna av relevanta brott i Europaparlamentets och rådets direktiv (EU) 2017/541 ([6]). Med tanke på behovet av att motverka den skadligaste terroristpropagandan online bör den definitionen omfatta material som anstiftar eller värvar någon för att begå eller bidra till att terroristbrott begås, värvar någon för att delta i en terroristgrupps verksamhet, eller förhärligar terroristverksamhet inbegripet genom spridning av material som skildrar en terroristattack. Definitionen bör även omfatta material som ger instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen samt kemiska, biologiska, radiologiska och nukleära (CBRN) ämnen, eller om andra särskilda metoder eller tekniker, inbegripet val av mål i syfte att begå eller bidra till begående av terroristbrott. Sådant material inbegriper text, bilder, ljudupptagningar och videor samt direktsändning av terroristbrott, som innebär en risk för att fler sådana brott begås. Vid bedömningen av huruvida material 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 uttalanden, i vilket sammanhang uttalandena gjordes samt deras potential att få skadliga konsekvenser för människors säkerhet. Det faktum att materialet producerats av, kan tillskrivas eller sprids på uppdrag av en person, grupp eller enhet som ingår i unionens förteckning över personer, grupper och enheter som är delaktiga i terroristgärningar och föremål för restriktiva åtgärder bör utgöra en viktig faktor i bedömningen.

(12) Material som sprids i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller för att öka medvetenheten om terroristverksamhet bör inte anses vara terrorisminnehåll. Vid fastställande av huruvida material som tillhandahålls av en innehållsleverantör utgör *terrorisminnehåll* enligt definitionen i denna förordning bör rätten till yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald samt konstens och vetenskapens frihet särskilt beaktas. I synnerhet i fall där innehållsleverantören har ett redaktionellt ansvar bör varje beslut om avlägsnande av det spridda materialet beakta de publicistiska normer som fastställts genom press- eller medieregler i enlighet med unionsrätten, inbegripet stadgan. 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.

(13) För att effektivt åtgärda spridningen av terrorisminnehåll online – samtidigt som respekten för enskilda personers privatliv säkerställs – bör denna förordning tillämpas på sådana leverantörer av informationssamhällets tjänster som på begäran lagrar och till allmänheten sprider information och material som tillhandahållits en användare av tjänsten, oavsett om lagringen och spridningen till allmänheten av sådan information och sådant material är av rent teknisk,

([6]) 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).

automatisk och passiv karaktär. Begreppet *lagring* bör förstås som förvaring av data i minnet hos en fysisk eller virtuell server. Leverantörer av *vidarebefordranstjänster* eller *cachelagringstjänster* samt andra tjänster som tillhandahålls på andra nivåer av internetinfrastrukturen och som inte innefattar lagring, såsom register och registratorer samt leverantörer av domännamnssystem (DNS), betalningstjänster eller skyddstjänster mot samordnad överbelastningsattack (DdoS), bör därför inte omfattas av denna förordnings tillämpningsområde.

(14) Begreppet *spridning till allmänheten* bör innebära att information görs tillgänglig för ett potentiellt obegränsat antal personer, det vill säga att information görs lätt tillgänglig för användare i allmänhet utan att det krävs någon ytterligare åtgärd från innehållsleverantörens sida, oberoende av huruvida dessa personer verkligen tar del av informationen i fråga. Om tillgång till information kräver registrering eller tillträde till en grupp av användare bör den informationen därför anses spridd till allmänheten endast när användare som söker tillgång till informationen automatiskt registreras eller ges tillträde utan att en person beslutar om eller väljer ut vem som ska ges tillgång till informationen. Interpersonella kommunikationstjänster enligt definitionen i artikel 2.5 i Europaparlamentets och rådets direktiv (EU) 2018/1972 ([7]), såsom e-post eller privata meddelandetjänster, bör inte omfattas av denna förordnings tillämpningsområde. Information bör anses lagrad och spridd till allmänheten i den mening som avses i denna förordning endast när detta sker på direkt begäran av innehållsleverantören. Leverantörer av tjänster, såsom molninfrastruktur, vilka tillhandahålls på begäran av andra parter än innehållsleverantörerna och endast indirekt är till nytta för de sistnämnda, bör därför inte omfattas av denna förordning. Denna förordning bör exempelvis omfatta leverantörer av sociala medietjänster, video-, bild- och ljuddelningstjänster, samt fildelningstjänster och andra molntjänster, i den mån som dessa tjänster används för att göra den lagrade informationen tillgänglig för allmänheten på direkt begäran av innehållsleverantören. Om en värdtjänstleverantör tillhandahåller flera tjänster bör denna förordning endast tillämpas på de tjänster som faller inom dess tillämpningsområde.

(15) Terrorisminnehåll sprids ofta till allmänheten via tjänster som tillhandhålls av värdtjänstleverantörer etablerade i tredjeländer. För att skydda användare i unionen och säkerställa att samtliga värdtjänstleverantörer som verkar inom den digitala inre marknaden omfattas av samma krav bör denna förordning vara tillämplig på alla leverantörer av relevanta tjänster som erbjuds i unionen, oberoende av i vilket land de har sitt huvudsakliga verksamhetsställe. En värdtjänstleverantör bör anses erbjuda tjänster i unionen om den gör det möjligt för fysiska eller juridiska personer i en eller flera medlemsstater att använda dess tjänster samt har en betydande anknytning till den eller de medlemsstaterna.

(16) En betydande anknytning till unionen bör föreligga om värdtjänstleverantören har ett verksamhetsställe i unionen, om dess tjänster används av ett betydande antal användare i en eller flera medlemsstater, eller om dess verksamhet riktas till en eller flera medlemsstater. Huruvida verksamheten är riktad till en eller flera medlemsstater bör avgöras på grundval av samtliga relevanta omständigheter, inbegripet faktorer som användning av ett språk eller en valuta som i allmänhet används i den berörda medlemsstaten, eller möjligheten att beställa varor eller tjänster från medlemsstaten. En sådan riktad karaktär skulle också kunna härröra från det faktum att en app finns tillgänglig i berörd nationell appstore, att lokal marknadsföring eller reklam görs på ett språk som vanligen används i den berörda medlemsstaten eller att kundkontakter, såsom kundtjänst, sköts på ett språk som vanligen används i den medlemsstaten. En betydande anknytning bör också antas föreligga om en värdtjänstleverantör 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 ([8]). Enbart det faktum att en värdtjänstleverantörs webbplats, en e-postadress eller andra kontaktuppgifter är tillgängliga i en eller flera medlemsstater bör inte i sig vara tillräckligt för att utgöra en betydande anknytning. Dessutom bör det inte kunna anses föreligga en betydande anknytning till unionen på grund av att en tjänst tillhandahålls i det enda syftet att efterleva det förbud mot diskriminering som fastställs i Europaparlamentets och rådets förordning (EU) 2018/302 ([9]).

([7]) Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

([8]) 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).

([9]) 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 60 I, 2.3.2018, s. 1).

(17) En harmonisering bör ske av förfarandet för och de skyldigheter som följer av avlägsnandeorder som ålägger värdtjänstleverantörer att avlägsna terrorisminnehåll eller göra det oåtkomligt efter en bedömning av de behöriga myndigheterna. Med tanke på hur snabbt terrorisminnehåll sprids via onlinetjänster bör värdtjänstleverantörerna åläggas en skyldighet att säkerställa att det terrorisminnehåll som anges i avlägsnandeordern avlägsnas eller att det görs oåtkomligt i samtliga medlemsstater inom en timme från mottagandet av avlägsnandeordern. Utom i vederbörligen motiverade brådskande fall bör den behöriga myndigheten tillhandahålla värdtjänstleverantören information om förfaranden och tillämpliga tidsfrister minst tolv timmar innan en avlägsnandeorder för första gången utfärdas till den värdtjänstleverantören. Vederbörligen motiverade brådskande fall föreligger när det faktum att terrorisminnehållet avlägsnas eller görs oåtkomligt senare än en timme efter mottagandet av avlägsnandeordern skulle medföra allvarlig skada, såsom i situationer där det finns ett överhängande hot mot en persons liv eller fysiska integritet eller när sådant innehåll skildrar pågående händelseförlopp som resulterar i skada på en persons liv eller fysiska integritet. Den behöriga myndigheten bör avgöra huruvida enskilda fall utgör brådskande fall och vederbörligen motivera sitt beslut i avlägsnandeordern. Om värdtjänstleverantören på grund av force majeure eller faktisk omöjlighet inte kan följa avlägsnandeordern inom en timme från det att den mottagits, inbegripet på grund av objektivt motiverade tekniska eller operativa skäl, bör den snarast möjligt informera den utfärdande behöriga myndigheten om detta och följa avlägsnandeordern så snart situationen har lösts.

(18) Avlägsnandeordern bör innehålla en motivering som klassificerar det material som ska avlägsnas eller göras oåtkomligt som terrorisminnehåll och ge tillräcklig information för att lokalisera innehållet genom att ange den exakta webbadressen och, när så krävs, eventuell ytterligare information, såsom en skärmdump av innehållet i fråga. Den motiveringen bör göra det möjligt för värdtjänstleverantören och, i slutändan, innehållsleverantören, att faktiskt utöva sin rätt till rättslig prövning. Motiveringen bör inte innebära utlämnande av känslig information som skulle kunna äventyra pågående utredningar.

(19) Den behöriga myndigheten bör lämna avlägsnandeordern direkt till den kontaktpunkt som utsetts eller inrättats av värdtjänstleverantören för tillämpningen av denna förordning, på ett elektroniskt sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar för värdtjänstleverantören att fastställa att ordern är autentisk – även att datum och tidpunkt för sändandet och mottagandet av ordern är korrekta – såsom genom säkrad e-post eller säkrade plattformar eller andra säkra kanaler, även sådana som tillhandahålls av värdtjänstleverantören, i enlighet med unionsrätt om skydd av personuppgifter. Detta krav bör bland annat kunna uppfyllas genom användning av kvalificerade elektroniska tjänster för rekommenderad leverans i den mening som avses i Europaparlamentets och rådets förordning (EU) nr 910/2014 ([10]). Om värdtjänstleverantörens har sitt huvudsakliga verksamhetsställe, eller dess rättsliga företrädare är bosatt eller etablerad, i en annan medlemsstat än den utfärdande behöriga myndighetens medlemsstat bör en kopia av avlägsnandeordern lämnas samtidigt till den behöriga myndigheten i den medlemsstaten.

(20) Den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad bör ha möjlighet att granska den avlägsnandeorder som utfärdats av behöriga myndigheter i en annan medlemsstat för att fastställa huruvida den på ett allvarligt eller uppenbart sätt är oförenlig med denna förordning eller de grundläggande rättigheterna i stadgan. Både innehållsleverantören och värdtjänstleverantören bör ha rätt att begära att den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad ska göra en sådan granskning. När en sådan begäran görs bör den behöriga myndigheten anta ett beslut om huruvida avlägsnandeordern innefattar en sådan oförenlighet. Om en sådan oförenlighet konstateras i det beslutet bör avlägsnandeordern inte längre ha rättsverkan. Granskningen bör utföras snabbt för att säkerställa att innehåll som avlägsnats eller gjorts oåtkomligt på felaktig grund återställs så snart som möjligt.

([10]) 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).

(21) Värdtjänstleverantörer som är utsatta för terrorisminnehåll och som tillämpar användarvillkor bör i dessa inkludera bestämmelser om åtgärder mot missbruk av deras tjänster för spridning av terrorisminnehåll till allmänheten. De bör tillämpa dessa bestämmelser på ett omsorgsfullt, transparent, proportionellt och icke-diskriminerande sätt.

(22) Med tanke på problemets omfattning och den snabbhet som krävs för att effektivt identifiera och avlägsna terrorisminnehåll är effektiva och proportionella specifika åtgärder en avgörande beståndsdel i kampen mot terrorisminnehåll online. I syfte att minska tillgången till terrorisminnehåll på sina tjänster bör värdtjänstleverantörer som är exponerade för terrorisminnehåll införa specifika åtgärder med beaktande av riskerna för och graden av exponering för terrorisminnehåll samt inverkan på tredje parters rättigheter och allmänhetens intresse av information. Värdtjänstleverantörer bör fastställa vilken lämplig, ändamålsenlig och proportionell specifik åtgärd som bör införas för att identifiera och avlägsna terrorisminnehåll. Specifika åtgärder skulle kunna inbegripa lämpliga tekniska eller operativa åtgärder eller lämplig teknisk eller operativ kapacitet, såsom personal eller tekniska medel för att identifiera och snabbt avlägsna terrorisminnehåll eller göra det oåtkomligt, mekanismer varmed användare kan rapportera eller flagga föregivet terrorisminnehåll, eller varje annan åtgärd som värdtjänstleverantören finner lämplig och effektiv för att åtgärda tillgängligheten av terrorisminnehåll på dess tjänster.

(23) När specifika åtgärder införs bör värdtjänstleverantörerna säkerställa att användares rätt till yttrande- och informationsfrihet samt mediernas frihet och mångfald som skyddas i stadgan bibehålls. Utöver de krav som fastställs i lag, inbegripet lagstiftningen om skydd av personuppgifter, bör värdtjänstleverantörer agera med tillbörlig aktsamhet och vidta skyddsåtgärder, när så är lämpligt, inbegripet mänsklig tillsyn och kontroll, för att undvika oavsiktliga eller felaktiga beslut som leder till att innehåll som inte är terrorisminnehåll avlägsnas eller görs oåtkomligt.

(24) Värdtjänstleverantören bör till den behöriga myndigheten rapportera om de specifika åtgärder som införts för att göra det möjligt för den myndigheten att avgöra huruvida åtgärderna är ändamålsenliga och proportionella och, om automatiska metoder används, huruvida värdtjänstleverantören har den nödvändiga kapaciteten för mänsklig tillsyn och kontroll. Vid bedömningen av åtgärdernas ändamålsenlighet och proportionalitet bör de behöriga myndigheterna beakta relevanta parametrar, däribland det antal avlägsnandeorder som utfärdats till värdtjänstleverantören, värdtjänstleverantörens storlek och ekonomiska kapacitet och inverkan av dess tjänster på spridningen av terrorisminnehåll, till exempel på grundval av antalet användare i unionen, samt de skyddsåtgärder som införts för att åtgärda missbruk av dess tjänster för spridning av terrorisminnehåll online.

(25) Om den behöriga myndigheten anser att de specifika åtgärder som införts är otillräckliga för att hantera riskerna bör den kunna kräva att ytterligare lämpliga, ändamålsenliga och proportionella specifika åtgärder antas. Kravet på införande av sådana ytterligare specifika åtgärder bör inte medföra en allmän skyldighet att övervaka eller en skyldighet att aktivt efterforska fakta i den mening som avses i artikel 15.1 i direktiv 2000/31/EG och inte heller något krav på att använda automatiska verktyg. Värdtjänstleverantörer bör emellertid kunna besluta att använda automatiska verktyg om de anser det lämpligt och nödvändigt för att på ett effektivt sätt åtgärda missbruk av deras tjänster för spridning av terrorisminnehåll online.

(26) Värdtjänstleverantörernas skyldighet att bevara avlägsnat innehåll och därtill hörande data bör fastställas för specifika ändamål och begränsas till den tidsperiod som är nödvändig. Det finns ett behov av att utvidga bevarandekravet till därtill hörande data i den mån sådana data annars skulle gå förlorade till följd av att det berörda terrorisminnehållet avlägsnas. Därtill hörande data kan omfatta data såsom abonnentdata, särskilt uppgifter om innehållsleverantörens identitet, och åtkomstdata, inbegripet uppgifter om datum och tidpunkt för innehållsleverantörens användning av och inloggning till och utloggning från tjänsten, tillsammans med den ip-adress som internetleverantören har tilldelat innehållsleverantören.

(27) Skyldigheten att bevara innehållet för administrativa eller rättsliga prövningsförfaranden är nödvändig och motiverad med hänsyn till behovet av att säkerställa att det finns effektiva rättsmedel för innehållsleverantörer vars innehåll har avlägsnats eller gjorts oåtkomligt samt för att säkerställa att innehållet kan återställas beroende på resultatet av dessa förfaranden. Skyldigheten att bevara material för utrednings- eller lagföringsändamål är motiverad och nödvändig med tanke på det värde som materialet kan tillföra för att störa eller förhindra terroristverksamhet. Därför bör bevarande av avlägsnat terrorisminnehåll för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott också anses vara motiverat. Terrorisminnehållet och därtill hörande data bör endast lagras

under den tidsperiod som är nödvändig för att de brottsbekämpande myndigheterna ska kunna kontrollera det terrorisminnehållet och besluta om det behövs för dessa ändamål. För förebyggande, förhindrande, upptäckt, utredning och lagföring av terroristbrott bör kravet på att bevara data vara begränsat till data som sannolikt har en koppling till terroristbrott och därmed skulle kunna bidra till att lagföra terroristbrott eller förhindra allvarliga risker för den allmänna säkerheten. När värdtjänstleverantörer avlägsnar material eller gör det oåtkomligt, särskilt genom egna specifika åtgärder, bör de omgående informera de behöriga myndigheterna om innehåll som innehåller information som innefattar ett överhängande hot mot en eller flera personers liv eller ett misstänkt terroristbrott.

(28) För att säkerställa proportionalitet bör perioden för bevarande vara begränsad till sex månader så att innehållsleverantörerna får tillräckligt med tid för att inleda administrativa eller rättsliga prövningsförfaranden och för att brottsbekämpande myndigheter ska kunna få åtkomst till relevanta data för utredning och lagföring av terroristbrott. Det bör dock, på begäran av den behöriga myndigheten eller domstolen, vara möjligt att förlänga denna period med den tid som är nödvändig i fall då dessa förfaranden inleds men inte avslutas inom den sexmånadersperioden. Perioden för bevarande bör vara tillräcklig för att de brottsbekämpande myndigheterna ska kunna bevara material som är nödvändigt för utredningar och lagföring, samtidigt som balansen i förhållande till de grundläggande rättigheterna säkerställs.

(29) Denna förordning bör inte påverka de förfarandegarantier eller processuella utredningsåtgärder som rör åtkomst till innehåll och därtill hörande data som bevarats för att utreda och lagföra terroristbrott, vilka fastställs i unionsrätt eller nationell rätt.

(30) 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 har vidtagit åtgärder eller ålagts att vidta åtgärder enligt denna förordning under ett visst kalenderår bör offentliggöra årliga transparensrapporter som innehåller information om åtgärder som vidtagits för att identifiera och avlägsna terrorisminnehåll.

(31) De behöriga myndigheterna bör offentliggöra årliga transparensrapporter med information om antalet avlägsnandeorder, antalet fall där en order inte verkställdes, antalet beslut avseende specifika åtgärder, antalet fall som är föremål för administrativa eller rättsliga prövningsförfaranden och antalet beslut om att påföra sanktioner.

(32) Rätten till ett effektivt rättsmedel stadfästs i artikel 19 i fördraget om Europeiska unionen (EU-fördraget) och artikel 47 i stadgan. 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. Den rätten bör särskilt inbegripa en möjlighet för värdtjänstleverantörer och innehållsleverantörer att effektivt bestrida avlägsnandeorder eller beslut till följd av granskning av avlägsnandeorder enligt denna förordning inför domstol i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern eller fattade beslutet, och en möjlighet för värdtjänstleverantörer att effektivt bestrida ett beslut om specifika åtgärder eller sanktioner inför domstol i den medlemsstat vars behöriga myndighet fattade det beslutet.

(33) Klagomålsförfaranden utgör en nödvändig skyddsåtgärd mot att innehåll online felaktigt avlägsnas eller görs oåtkomligt när sådant innehåll är skyddat genom yttrande- 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 innehåll som felaktigt har avlägsnats eller gjorts oåtkomligt bör inte påverka värdtjänstleverantörens möjlighet att genomdriva sina egna användarvillkor.

(34) Ett effektivt rättsligt skydd i enlighet med artikel 19 i EU-fördraget och artikel 47 i stadgan förutsätter att innehållsleverantörer kan utröna av vilka orsaker det innehåll de tillhandahåller har avlägsnats eller gjorts oåtkomligt. För detta ändamål bör värdtjänstleverantören tillhandahålla innehållsleverantören information för bestridande av att innehållet avlägsnats eller gjorts oåtkomligt. Beroende på omständigheterna skulle värdtjänstleverantörer kunna ersätta innehåll som har avlägsnats eller gjorts oåtkomligt med ett meddelande om att innehållet har avlägsnats eller gjorts oåtkomligt i enlighet med denna förordning. Ytterligare information om orsakerna till att innehållet avlägsnats eller gjorts oåtkomligt samt om rättsmedel för detta bör tillhandahållas på begäran från innehållsleverantören. Om de behöriga myndigheterna beslutar att det av hänsyn till allmän säkerhet, inbegripet 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 i enlighet därmed.

(35) Medlemsstaterna bör utse behöriga myndigheter för tillämpningen av denna förordning. Detta bör inte nödvändigtvis innebära att en ny myndighet måste inrättas, och det bör vara möjligt att anförtro ett befintligt organ de funktioner som föreskrivs i denna förordning. Det bör enligt denna förordning finnas krav på att det utses myndigheter som har befogenhet att utfärda avlägsnandeorder, granska avlägsnandeorder, övervaka specifika åtgärder och påföra sanktioner, medan varje medlemsstat bör kunna bestämma hur många behöriga myndigheter som ska utses och om de ska vara administrativa, brottsbekämpande eller rättsliga. Medlemsstaterna bör säkerställa att de behöriga myndigheterna utför sina uppgifter på ett objektivt och icke-diskriminerande sätt och inte efterfrågar eller tar emot instruktioner från något annat organ när det gäller utförandet av uppgifter enligt denna förordning. Detta bör inte förhindra tillsyn i enlighet med nationell konstitutionell rätt. Medlemsstaterna bör underrätta kommissionen om de behöriga myndigheter som utsetts enligt denna förordning, och kommissionen bör offentliggöra ett register online med en förteckning över de behöriga myndigheterna. Det onlineregistret bör vara lätt tillgängligt, så att värdtjänstleverantörer snabbt kan kontrollera att en avlägsnandeorder är autentisk.

(36) För att undvika dubbelarbete och möjlig störning av utredningar samt för att minimera bördan för berörda värdtjänstleverantörer bör de behöriga myndigheterna utbyta information, samordna sig med och samarbeta med varandra och, när så är lämpligt, med Europol, innan de utfärdar avlägsnandeorder. När den fattar beslut om huruvida en avlägsnandeorder ska utfärdas bör den behöriga myndigheten ta vederbörlig hänsyn till eventuella anmälningar om en konflikt med ett utredningsmässigt intresse (konfliktlösning). Om en behörig myndighet får information från en behörig myndighet i en annan medlemsstat om en befintlig avlägsnandeorder bör den inte utfärda en avlägsnandeorder avseende samma sak. Vid genomförandet av bestämmelserna i denna förordning kan Europol tillhandahålla stöd i enlighet med dess nuvarande mandat och befintliga rättsliga ram.

(37) I syfte att säkerställa ett effektivt och tillräckligt enhetligt genomförande av specifika åtgärder som vidtas av värdtjänstleverantörer bör de behöriga myndigheterna samordna sig och samarbeta med varandra i fråga om de utbyten som de har med värdtjänstleverantörer avseende avlägsnandeorder samt identifiering, genomförande och bedömning av specifika åtgärder. Samordning och samarbete behövs också i samband med andra åtgärder för genomförande av denna förordning, inbegripet med avseende på antagande av regler om sanktioner och påförande av sanktioner. Kommissionen bör underlätta sådan samordning och sådant samarbete.

(38) Det är viktigt att den behöriga myndigheten i den medlemsstat som ansvarar för att påföra sanktioner är fullständigt informerad om utfärdandet av avlägsnandeorder och efterföljande utbyten mellan värdtjänstleverantören och behöriga myndigheter i andra medlemsstater. För det ändamålet bör medlemsstaterna säkerställa lämpliga och säkra kommunikationskanaler och mekanismer som gör det möjligt att dela relevant information i rätt tid.

(39) För att underlätta ett snabbt utbyte mellan behöriga myndigheter och med värdtjänstleverantörer, och för att undvika dubbelarbete, bör medlemsstaterna uppmuntras att använda sig av de särskilda verktyg som utvecklats av Europol, såsom den befintliga applikationen för hantering av anmälan av innehåll på internet (*Internet Referral Management application*) eller dess efterföljare.

(40) Anmälningar från medlemsstaterna och Europol har visat sig utgöra ett effektivt och snabbt sätt att öka värdtjänstleverantörers medvetenhet om specifikt innehåll som är tillgängligt via deras tjänster och göra det möjligt för dem att snabbt vidta åtgärder. Sådana anmälningar, som är en mekanism för att uppmärksamma värdtjänstleverantörer på information som skulle kunna anses utgöra terrorisminnehåll, så att de frivilligt kan bedöma om det innehållet är förenligt med deras egna användarvillkor, bör förbli tillgängliga vid sidan av avlägsnandeorder. Det är alltjämt värdtjänstleverantören som fattar det slutliga beslutet om huruvida innehållet ska avlägsnas på grund av att det är oförenligt med dess användarvillkor. Denna förordning bör inte påverka Europols mandat som fastställs i Europaparlamentets och rådets förordning (EU) 2016/794 ([11]). Ingenting i denna förordning bör därför tolkas som att det skulle hindra medlemsstaterna och Europol från att använda anmälningar som ett verktyg för åtgärdande av terrorisminnehåll online.

(41) Med tanke på de särskilt allvarliga konsekvenserna av visst terrorisminnehåll online bör värdtjänstleverantörer omgående informera de relevanta myndigheterna i den berörda medlemsstaten eller de behöriga myndigheterna i den medlemsstat där de är etablerade eller har en rättslig företrädare om terrorisminnehåll som innefattar ett överhängande hot mot en eller flera personers liv eller ett misstänkt terroristbrott. För att säkerställa proportionalitet bör den skyldigheten vara begränsad till terroristbrott enligt definitionen i artikel 3.1 i direktiv (EU) 2017/541. Den skyldigheten att informera bör inte innebära att värdtjänstleverantörer är skyldiga att aktivt söka bevis på sådana överhängande hot mot en eller flera personers liv eller ett misstänkt terroristbrott. Den berörda medlemsstaten bör förstås som den medlemsstat som har jurisdiktion över utredning och lagföring av de terroristbrotten på grundval av gärningsmannens eller det potentiella brottsoffrets nationalitet eller målplatsen för terroristgärningen. Om det råder tvivel bör värdtjänstleverantörer lämna informationen till Europol som bör tillhandahålla relevanta uppföljningsåtgärder i enlighet med sitt mandat, inbegripet genom att vidarebefordra den informationen till de relevanta nationella myndigheterna. Medlemsstaternas behöriga myndigheter bör ha rätt att använda sådan information för att vidta utredningsåtgärder som föreskrivs i unionsrätt eller nationell rätt.

(42) Värdtjänstleverantörer bör utse eller inrätta kontaktpunkter för att underlätta snabb handläggning av avlägsnandeorder. Kontaktpunkten bör endast tjäna operativa syften. Kontaktpunkten bör bestå av någon typ av särskilda medel, interna eller externa, som möjliggör elektronisk inlämning av avlägsnandeorder och av tekniska resurser eller personalresurser som möjliggör snabb handläggning av dem. Kontaktpunkten måste inte vara belägen i unionen. Värdtjänstleverantören bör vara fri att använda en befintlig kontaktpunkt vid tillämpningen av denna förordning, under förutsättning att kontaktpunkten 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 kontaktpunkten för värdtjänstleverantörer som är exponerade för terrorisminnehåll vara tillgänglig vid alla tidpunkter. 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 unionsinstitutionernas officiella språk som deras användarvillkor finns tillgängliga på.

(43) Då det inte finns något allmänt krav på att värdtjänstleverantörer måste säkerställa fysisk närvaro inom 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 dess huvudsakliga verksamhetsställe är beläget eller där dess rättsliga företrädare är bosatt eller etablerad. Detta bör inte påverka de bestämmelser om behörighet som fastställs för avlägsnandeorder och beslut som följer av granskningen av avlägsnandeorder enligt denna förordning. När det gäller en värdtjänstleverantör som inte har något verksamhetsställe i unionen och som inte utser en rättslig företrädare bör varje medlemsstat ändå ha jurisdiktion och därmed kunna påföra sanktioner, under förutsättning att principen *ne bis in idem* respekteras.

([11]) 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).

(44) 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 bör för tillämpningen av denna förordning kunna utse en rättslig företrädare som redan är utsedd för andra ändamål, under förutsättning att denna rättsliga företrädare kan fullgöra de funktioner som föreskrivs i denna förordning. Den rättsliga företrädaren bör ha befogenhet att agera på värdtjänstleverantörens vägnar.

(45) Sanktioner är nödvändiga för att säkerställa värdtjänstleverantörernas effektiva genomförande av denna förordning. Medlemsstaterna bör anta regler om sanktioner, som kan vara av administrativ eller straffrättslig art, samt riktlinjer för bötfällning när så är lämpligt. Bristande efterlevnad i enskilda fall kan bli föremål för sanktioner, med respekt för principen *ne bis in idem* och proportionalitetsprincipen, samt med säkerställande av att sådana sanktioner påförs med beaktande av systematisk underlåtenhet. Sanktioner kan ta sig olika former, inbegripet formella varningar vid smärre överträdelser eller böter vid allvarligare eller systematiska överträdelser. Särskilt stränga sanktioner bör fastställas om värdtjänstleverantören systematiskt eller fortgående underlåter att avlägsna terrorisminnehåll eller göra det oåtkomligt inom en timme från mottagandet av en avlägsnandeorder. För att säkerställa rättssäkerhet bör det i denna förordning anges vilka överträdelser som kan bli föremål för sanktioner och vilka omständigheter som är relevanta för att bedöma sanktionernas typ och nivå. Vid fastställande av huruvida böter ska åläggas bör vederbörlig hänsyn tas till värdtjänstleverantörens ekonomiska resurser. Den behöriga myndigheten bör vidare ta hänsyn till huruvida värdtjänstleverantören är ett nystartat företag eller ett mikroföretag, litet eller medelstort företag enligt definitionen i kommissionens rekommendation 2003/361/EG ([12]). Ytterligare omständigheter bör beaktas, exempelvis huruvida värdtjänstleverantörens handlande objektivt sett varit oförsiktigt eller klandervärt eller huruvida överträdelsen har orsakats av vårdslöshet eller varit avsiktlig. Medlemsstaterna bör säkerställa att de sanktioner som påförs för överträdelser av denna förordning inte uppmuntrar till avlägsnande av material som inte är terrorisminnehåll.

(46) Användningen av standardiserade mallar underlättar samarbete och informationsutbyte mellan behöriga myndigheter och värdtjänstleverantörer, 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. Mallar minskar översättningskostnaderna och bidrar till en högre standard för processen. Mallar för återkoppling möjliggör ett standardiserat informationsutbyte och är särskilt viktiga om värdtjänstleverantörerna inte kan följa avlägsnandeorder. Autentiserade inlämningskanaler kan garantera att avlägsnandeordern är autentisk, liksom att datum och tidpunkt för sändande och mottagande av ordern är korrekta.

(47) För att vid behov möjliggöra en snabb ändring 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 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, inbegripet på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([13]). 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.

(48) Medlemsstaterna bör samla in information om genomförandet av denna förordning. Medlemsstaterna bör ha möjlighet att använda sig av värdtjänstleverantörernas transparensrapporter och vid behov komplettera med mer detaljerad information, såsom deras egna transparensrapporter enligt denna förordning. Ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter bör inrättas som underlag för en utvärdering av genomförandet av denna förordning.

([12]) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

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

(49) På grundval av resultaten och slutsatserna i genomföranderapporten och resultaten av övervakningen bör kommissionen genomföra en utvärdering av denna förordning inom tre år från dagen för dess ikraftträdande. Utvärderingen bör grundas på kriterierna effektivitet, nödvändighet, ändamålsenlighet, proportionalitet, relevans, samstämmighet och mervärde för unionen. Den bör inkludera en bedömning av hur de olika operativa och tekniska åtgärder som föreskrivs i denna förordning fungerar, inbegripet ändamålsenligheten i de åtgärder som ska förbättra upptäckt, identifiering och avlägsnande av terrorisminnehåll online, skyddsmekanismernas ändamålsenlighet samt inverkan på grundläggande rättigheter som potentiellt påverkas, såsom yttrande- och informationsfriheten, inbegripet mediernas frihet och mångfald, näringsfriheten, rätten till ett privatliv och skyddet av personuppgifter. Kommissionen bör även bedöma inverkan på tredje parters potentiellt påverkade intressen.

(50) Eftersom målet för denna förordning, nämligen att säkerställa att den digitala inre marknaden fungerar smidigt genom åtgärder mot spridningen av terrorisminnehåll online, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av dess omfattning och verkningar, bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. 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

Innehåll och tillämpningsområde

1. I denna förordning fastställs enhetliga regler för att åtgärda missbruk av värdtjänster för spridning till allmänheten av terrorisminnehåll online, i synnerhet följande:

a) Rimliga och proportionella aktsamhetskrav som värdtjänstleverantörer ska iaktta för att åtgärda spridning till allmänheten av terrorisminnehåll via deras tjänster och vid behov säkerställa att sådant innehåll snabbt avlägsnas eller görs oåtkomligt.

b) Åtgärder som medlemsstaterna ska införa – i enlighet med unionsrätten och med förbehåll för lämpliga skyddsåtgärder för att skydda grundläggande rättigheter, särskilt yttrande- och informationsfriheten i ett öppet och demokratiskt samhälle – för att

   i) identifiera och göra det möjligt för värdtjänstleverantörer att snabbt avlägsna terrorisminnehåll, samt

   ii) underlätta samarbete mellan medlemsstaternas behöriga myndigheter, värdtjänstleverantörer och, när så är lämpligt, Europol.

2. Denna förordning är tillämplig på värdtjänstleverantörer som erbjuder tjänster i unionen, oberoende av deras huvudsakliga verksamhetsställe, i den mån de sprider information till allmänheten.

3. Material som sprids till allmänheten i utbildningssyfte, journalistiskt syfte, konstnärligt syfte eller forskningssyfte eller i syfte att förhindra eller bekämpa terrorism, inbegripet material som ger uttryck för polemiska eller kontroversiella åsikter inom ramen för den offentliga debatten, ska inte anses vara terrorisminnehåll. Det ska göras en bedömning för att fastställa den spridningens verkliga syfte och huruvida materialet sprids för dessa syften.

4. Denna förordning ska inte medföra någon ändring av skyldigheten att respektera de rättigheter, friheter och principer som avses i artikel 6 i EU-fördraget och ska tillämpas utan att det påverkar tillämpningen av grundläggande principer som rör yttrande- och informationsfrihet, inbegripet mediernas frihet och mångfald.

5. Denna förordning ska inte påverka tillämpningen av direktiven 2000/31/EG och 2010/13/EU. För audiovisuella medietjänster enligt definitionen i artikel 1.1 a i direktiv 2010/13/EU ska direktiv 2010/13/EU äga företräde.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *värdtjänstleverantör*: en leverantör av tjänster enligt definitionen i artikel 1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([14]) som består i att information som tillhandahållits av en innehållsleverantör lagras på dennes begäran.

2. *innehållsleverantör*: en användare som har tillhandahållit information som lagras och sprids till allmänheten eller har lagrats och spridits till allmänheten av en värdtjänstleverantör.

3. *spridning till allmänheten*: tillgängliggörande av information på begäran av en innehållsleverantör för ett potentiellt obegränsat antal personer.

4. *erbjuda tjänster i unionen*: göra det möjligt för fysiska eller juridiska 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.

5. *betydande anknytning*: en värdtjänstleverantörs anknytning till en eller flera medlemsstater som antingen följer av dennes verksamhetsställe i unionen eller särskilda faktiska kriterier, såsom att

   a) värdtjänstleverantören har ett betydande antal användare av dess tjänster i en eller flera medlemsstater, eller

   b) värdtjänstleverantörens verksamhet är riktad till en eller flera medlemsstater.

6. *terroristbrott*: brott enligt definitionen i artikel 3 i direktiv (EU) 2017/541.

7. *terrorisminnehåll*: en eller flera av följande typer av material, närmare bestämt material som

   a) anstiftar till begåendet av ett av de brott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541, om sådant material, direkt eller indirekt, såsom genom förhärligande av terroristgärningar, förespråkar utförandet av terroristbrott, och därigenom medför fara för att ett eller flera sådana brott kan begås,

   b) värvar en person eller en grupp av personer för att begå något av de brott som anges i artikel 3.1 a–i i direktiv (EU) 2017/541 eller bidra till att något av dessa brott begås,

   c) värvar en person eller en grupp av personer för att delta i en terroristgrupps verksamhet i den mening som avses i artikel 4 b i direktiv (EU) 2017/541,

   d) tillhandahåller instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen eller om andra specifika metoder eller tekniker för begående av eller bidragande till begåendet av något av de terroristbrott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541,

   e) utgör ett hot om begående av ett av de brott som avses i artikel 3.1 a–i i direktiv (EU) 2017/541.

([14]) Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

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

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

Avsnitt II

Åtgärder mot spridning av terrorisminnehåll online

Artikel 3

Avlägsnandeorder

1. Den behöriga myndigheten i varje medlemsstat ska ha befogenhet att utfärda en avlägsnandeorder med krav på att värdtjänstleverantörer avlägsnar terrorisminnehåll eller gör terrorisminnehåll oåtkomligt i samtliga medlemsstater.

2. Om en behörig myndighet inte tidigare har utfärdat en avlägsnandeorder till en värdtjänstleverantör ska den tillhandahålla den värdtjänstleverantören information om tillämpliga förfaranden och tidsfrister minst tolv timmar innan avlägsnandeordern utfärdas.

Första stycket ska inte gälla i vederbörligen motiverade brådskande fall.

3. Värdtjänstleverantörer ska avlägsna terrorisminnehåll eller göra terrorisminnehåll oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern.

4. Behöriga myndigheter ska utfärda avlägsnandeorder med användning av mallen i bilaga I. Avlägsnandeorder ska innehålla följande uppgifter:

a) Identifieringsuppgifter för den behöriga myndighet som utfärdar avlägsnandeordern och den behöriga myndighetens autentisering av avlägsnandeordern.

b) En tillräckligt detaljerad motivering till varför innehållet anses utgöra terrorisminnehåll samt en hänvisning till den relevanta typen av material enligt artikel 2.7.

c) En exakt webbadress (URL) och, vid behov, ytterligare information som gör det möjligt att identifiera terrorisminnehållet.

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

e) Datum, tidsstämpel och elektronisk signatur för den behöriga myndighet som utfärdar avlägsnandeordern.

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

g) När så är nödvändigt och proportionellt, beslutet att inte lämna ut information om att terrorisminnehåll avlägsnats eller gjorts oåtkomligt i enlighet med artikel 11.3.

5. Den behöriga myndigheten ska rikta avlägsnandeordern till värdtjänstleverantörens huvudsakliga verksamhetsställe eller till dess juridiska företrädare som utsetts i enlighet med artikel 17.

Den behöriga myndigheten ska överföra avlägsnandeordern till den kontaktpunkt som avses i artikel 15.1 på ett elektroniskt sätt som gör det möjligt att få en skriftlig uppteckning och som ger förutsättningar att säkerställa autentisering av avsändaren, inbegripet att datum och tidpunkt för sändandet och mottagandet av ordern är korrekta.

6. Värdtjänstleverantörerna ska utan onödigt dröjsmål med användning av mallen i bilaga II informera den behöriga myndigheten om att terrorisminnehållet har avlägsnats eller att terrorisminnehållet gjorts oåtkomligt i samtliga medlemsstater, med angivelse av i synnerhet tidpunkten då innehållet avlägsnades eller gjordes oåtkomligt.

7. Om värdtjänstleverantören inte kan följa avlägsnandeordern på grund av force majeure eller faktisk omöjlighet som inte kan tillskrivas värdtjänstleverantören, inbegripet av objektivt motiverade tekniska eller operativa skäl, ska den utan onödigt dröjsmål informera den behöriga myndighet som utfärdade avlägsnandeordern om dessa skäl med användning av mallen i bilaga III.

Den tidsfrist som anges i punkt 3 ska börja löpa så snart de grunder som avses i första stycket i denna punkt inte längre föreligger.

8. Om värdtjänstleverantören inte kan följa avlägsnandeordern på grund av att den innehåller uppenbara fel eller inte innehåller tillräcklig information för att verkställa den, ska värdtjänstleverantören utan onödigt dröjsmål informera den behöriga myndighet som utfärdade avlägsnandeordern och be om nödvändiga klargöranden med användning av mallen i bilaga III.

Den tidsfrist som anges i punkt 3 ska börja löpa så snart värdtjänstleverantören har mottagit de nödvändiga klargörandena.

9. En avlägsnandeorder ska bli slutgiltig vid utgången av tidsfristen för överklagande om inget överklagande har ingetts i enlighet med nationell rätt eller vid bekräftelse efter ett överklagande.

När avlägsnandeordern har blivit slutgiltig ska den behöriga myndighet som utfärdade avlägsnandeordern informera den behöriga myndighet som avses i artikel 12.1 c i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad om detta.

Artikel 4

Förfarande för gränsöverskridande avlägsnandeorder

1. Med förbehåll för vad som anges i artikel 3 ska den behöriga myndighet som utfärdade avlägsnandeordern, om värdtjänstleverantören inte har sitt huvudsakliga verksamhetsställe eller sin rättsliga företrädare i den medlemsstat där den myndigheten är belägen, samtidigt översända en kopia av avlägsnandeordern till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad.

2. Om en värdtjänstleverantör mottar en avlägsnandeorder enligt denna artikel ska den vidta de åtgärder som föreskrivs i artikel 3 och vidta de åtgärder som krävs för att kunna återställa innehållet eller åtkomsten till det i enlighet med punkt 7 i denna artikel.

3. Den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad får på eget initiativ, inom 72 timmar från mottagandet av kopian av avlägsnandeordern i enlighet med punkt 1, granska avlägsnandeorden för att fastställa huruvida den på ett allvarligt eller uppenbart sätt är oförenlig med denna förordning eller de grundläggande rättigheter och friheter som garanteras i stadgan.

Om den konstaterar oförenlighet ska den, inom samma tid, anta ett motiverat beslut om detta.

4. Värdtjänstleverantörer och innehållsleverantörer ska ha rätt att inom 48 timmar från mottagandet av antingen en avlägsnandeorder eller information enligt artikel 11.2 lämna in en motiverad begäran till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad om att den ska granska avlägsnandeordern enligt punkt 3 första stycket i denna artikel.

Den behöriga myndigheten ska inom 72 timmar från mottagandet av begäran anta ett motiverat beslut till följd av granskningen av avlägsnandeordern, med angivande av sina slutsatser om huruvida oförenlighet föreligger.

5. Innan den behöriga myndigheten antar ett beslut enligt punkt 3 andra stycket eller ett beslut om att oförenlighet föreligger enligt punkt 4 andra stycket ska den informera den behöriga myndighet som utfärdat avlägsnandeordern om att den har för avsikt anta beslutet i fråga samt ange skälen till detta.

6. Om den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad antar ett motiverat beslut i enlighet med punkt 3 eller 4 i denna artikel, ska den utan dröjsmål översända det beslutet till den behöriga myndighet som utfärdat avlägsnandeordern, värdtjänstleverantören, den innehållsleverantör som begärde granskningen enligt punkt 4 i denna artikel samt, i enlighet med artikel 14, Europol. Om det i beslutet konstateras oförenlighet enligt punkt 3 eller 4 i denna artikel, ska avlägsnandeordern inte längre ha rättsverkan.

7. När den berörda värdtjänstleverantören mottar ett beslut i vilket oförenlighet konstateras som översänts i enlighet med punkt 6 ska den omedelbart återställa det avlägsnade innehållet eller åtkomsten till det utan att det påverkar dess möjlighet att genomdriva sina egna användarvillkor i enlighet med unionsrätten och nationell rätt.

Artikel 5

Specifika åtgärder

1. En värdtjänstleverantör som är exponerad för terrorisminnehåll enligt punkt 4 ska i tillämpliga fall i sina användarvillkor inkludera samt tillämpa bestämmelser om åtgärder mot missbruk av dess tjänster för spridning till allmänheten av terrorisminnehåll.

Den ska göra detta på ett omsorgsfullt, proportionellt och icke-diskriminerande sätt och under alla omständigheter med vederbörlig hänsyn till användarnas grundläggande rättigheter och med särskilt beaktande av den grundläggande betydelsen av yttrande- och informationsfrihet i ett öppet och demokratiskt samhälle, i syfte att undvika avlägsnandet av material som inte är terrorisminnehåll.

2. En värdtjänstleverantör som är exponerad för terrorisminnehåll enligt punkt 4 ska vidta specifika åtgärder för att skydda sina tjänster mot spridning till allmänheten av terrorisminnehåll.

Det är värdtjänstleverantören som ska besluta vilka specifika åtgärder som ska vidtas. Sådana åtgärder får inbegripa en eller flera av följande åtgärder:

a) Lämpliga tekniska och operativa åtgärder eller lämplig teknisk och operativ kapacitet, såsom lämplig personalstyrka eller lämpliga tekniska medel för att identifiera och snabbt avlägsna terrorisminnehåll eller göra det oåtkomligt.

b) Lättillgängliga och användarvänliga mekanismer varmed användare till värdtjänstleverantören kan rapportera eller flagga påstått terrorisminnehåll.

c) Andra mekanismer för att öka medvetenheten om terrorisminnehåll på dess tjänster, såsom mekanismer för användarmoderering.

d) Andra åtgärder som värdtjänstleverantören anser vara lämpliga för att åtgärda tillgängligheten av terrorisminnehåll på dess tjänster.

3. Specifika åtgärder ska uppfylla samtliga följande krav:

a) De ska på ett effektivt sätt minska graden av exponering för terrorisminnehåll hos värdtjänstleverantörens tjänster.

b) De ska vara riktade och proportionella, med särskilt beaktande av hur hög graden av exponering för terrorisminnehåll är hos värdtjänstleverantörens tjänster samt värdtjänstleverantörens tekniska och operativa kapacitet och finansiella styrka samt antalet användare av värdtjänstleverantörens tjänster och den mängd innehåll som de tillhandahåller.

c) De ska tillämpas med fullständigt beaktande av användarnas rättigheter och legitima intressen, särskilt användarnas grundläggande rättigheter vad gäller yttrande- och informationsfrihet, respekt för privatlivet samt skydd av personuppgifter.

d) De ska tillämpas på ett omsorgsfullt och icke-diskriminerande sätt.

När de specifika åtgärderna innebär användning av tekniska medel ska det införas lämpliga och effektiva skyddsåtgärder, särskilt genom mänsklig tillsyn och kontroll, för att säkerställa att de är korrekta och för att undvika avlägsnande av material som inte är terrorisminnehåll.

4. En värdtjänstleverantör är exponerad för terrorisminnehåll när den behöriga myndigheten i den medlemsstat där den har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad har

a) fattat ett beslut som grundas på objektiva faktorer, såsom det faktum att värdtjänstleverantören under de föregående tolv månaderna har mottagit två eller flera avlägsnandeorder som blivit slutgiltiga, i vilket det konstateras att värdtjänstleverantören är exponerad för terrorisminnehåll, och

b) meddelat värdtjänstleverantören det beslut som avses i led a.

5. Efter att ha mottagit ett beslut som avses i punkt 4 eller, i förekommande fall, punkt 6 ska en värdtjänstleverantör till den behöriga myndigheten rapportera om de specifika åtgärder som den har vidtagit och har för avsikt att vidta för att följa punkterna 2 och 3. Den ska göra detta inom tre månader från mottagandet av beslutet och därefter årligen. Denna skyldighet ska upphöra så snart den behöriga myndigheten har beslutat, till följd av en begäran enligt punkt 7, att värdtjänstleverantören inte längre är exponerad för terrorisminnehåll.

6. Om den behöriga myndigheten – på grundval av de rapporter som avses i punkt 5 och i förekommande fall andra objektiva faktorer – anser att de specifika åtgärder som vidtagits inte uppfyller kraven i punkterna 2 och 3, ska den behöriga myndigheten rikta ett beslut till värdtjänstleverantören med krav på att denne vidtar nödvändiga åtgärder för att säkerställa att kraven i punkterna 2 och 3 uppfylls.

Värdtjänstleverantören får välja vilken typ av specifika åtgärder som ska vidtas.

7. En värdtjänstleverantör får när som helst begära att den behöriga myndigheten omprövar och, när så är lämpligt, ändrar eller återkallar ett beslut som avses i punkt 4 eller 6.

Inom tre månader från mottagandet av begäran ska den behöriga myndigheten på grundval av objektiva faktorer anta ett motiverat beslut om begäran samt meddela värdtjänstleverantören det beslutet.

8. Krav på att vidta specifika åtgärder ska inte påverka tillämpningen av artikel 15.1 i direktiv 2000/31/EG och ska varken medföra en allmän skyldighet för värdtjänstleverantörer att övervaka den information som de överför eller lagrar eller en allmän skyldighet att aktivt efterforska fakta eller omständigheter som tyder på olaglig verksamhet.

Inget krav på att vidta specifika åtgärder får innebära en skyldighet för värdtjänstleverantören att använda automatiska verktyg.

Artikel 6

Bevarande av innehåll och därtill hörande data

1. Värdtjänstleverantörer ska bevara terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder, eller specifika åtgärder enligt artikel 3 eller 5, samt därtill hörande data som har avlägsnats till följd av att sådant terrorisminnehåll har avlägsnats, som är nödvändiga för

a) administrativa eller rättsliga prövningsförfaranden eller hantering av klagomål enligt artikel 10 avseende ett beslut att avlägsna eller göra oåtkomligt terrorisminnehåll och därtill hörande data,

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

2. Det terrorisminnehåll och de därtill hörande data som avses i punkt 1 ska bevaras i sex månader från det att de avlägsnats eller gjorts oåtkomliga. Terrorisminnehållet ska på den behöriga myndighetens eller domstolens begäran bevaras under en ytterligare, specificerad period endast 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 därtill hörande data som bevaras enligt punkt 1 omfattas av lämpliga tekniska och organisatoriska skyddsåtgärder.

Dessa tekniska och organisatoriska skyddsåtgärder ska säkerställa att det terrorisminnehåll och de därtill hörande 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 7

Transparenskrav för värdtjänstleverantörer

1. Värdtjänstleverantörer ska i sina användarvillkor klart och tydligt ange sin strategi för att åtgärda spridningen av terrorisminnehåll, när så är lämpligt med en meningsfull förklaring av hur specifika åtgärder, inbegripet i förekommande fall användningen av automatiska verktyg, fungerar.

2. Varje värdtjänstleverantör som har vidtagit åtgärder för att åtgärda spridningen av terrorisminnehåll eller har ålagts att vidta åtgärder enligt denna förordning under ett visst kalenderår ska offentliggöra en transparensrapport om dessa åtgärder för det året. Den ska offentliggöra den rapporten före den 1 mars följande år.

3. Transparensrapporterna ska innehålla minst följande information:

a) Information om värdtjänstleverantörens åtgärder för att identifiera och avlägsna terrorisminnehåll eller göra det oåtkomligt.

b) Information om värdtjänstleverantörens åtgärder för att åtgärda att material som tidigare har avlägsnats eller gjorts oåtkomligt på grund av att det ansågs vara terrorisminnehåll dyker upp på nytt, särskilt när automatiska verktyg har använts.

c) Antalet inslag med terrorisminnehåll som har avlägsnats eller gjorts oåtkomligt till följd av avlägsnandeorder eller specifika åtgärder samt antalet avlägsnandeorder där innehållet inte har avlägsnats eller gjorts oåtkomligt enligt artikel 3.7 första stycket och 3.8 första stycket tillsammans med skälen till detta.

d) Antalet klagomål som behandlats av värdtjänstleverantören i enlighet med artikel 10 och resultatet av dessa.

e) Antalet administrativa eller rättsliga prövningsförfaranden som inletts av värdtjänstleverantören och resultatet av dessa.

f) Antalet fall där värdtjänstleverantören har ålagts att återställa innehåll eller åtkomsten till det till följd av administrativa eller rättsliga prövningsförfaranden.

g) Antalet fall där värdtjänstleverantören har återställt innehåll eller åtkomsten till det till följd av ett klagomål från innehållsleverantören.

Artikel 8

Behöriga myndigheters transparensrapporter

1. De behöriga myndigheterna ska offentliggöra årliga transparensrapporter över sin verksamhet enligt denna förordning. Dessa rapporter ska innehålla åtminstone följande information för kalenderåret i fråga:

a) Antalet avlägsnandeorder som har utfärdats enligt artikel 3, med angivande av antalet avlägsnandeorder enligt artikel 4.1, och det antal avlägsnandeorder som granskats enligt artikel 4 samt information om hur de berörda värdtjänstleverantörerna har genomfört dessa avlägsnandeorder, inbegripet antalet fall där terrorisminnehåll har avlägsnats eller gjorts oåtkomligt och antalet fall där terrorisminnehåll inte har avlägsnats eller gjorts oåtkomligt.

b) Antalet beslut som fattats i enlighet med artikel 5.4, 5.6 eller 5.7 samt information om hur värdtjänstleverantörerna har genomfört dessa beslut, inbegripet en beskrivning av de specifika åtgärderna.

c) Antalet fall där avlägsnandeorder och beslut som fattats i enlighet med artikel 5.4 och 5.6 har varit föremål för administrativa eller rättsliga prövningsförfaranden samt information om resultatet av de relevanta förfarandena.

d) Antalet beslut om påförande av sanktioner enligt artikel 18 och en beskrivning av typen av sanktion som påförts.

2. De årliga transparensrapporter som avses i punkt 1 får inte innehålla information som negativt kan påverka pågående verksamhet för förebyggande, förhindrande, upptäckt, utredning eller lagföring av terroristbrott eller nationella säkerhetsintressen.

Artikel 9

Rättsmedel

1. Värdtjänstleverantörer som har mottagit en avlägsnandeorder som utfärdats enligt artikel 3.1 eller ett beslut enligt artikel 4.4 eller artikel 5.4, 5.6 eller 5.7 ska ha rätt till ett effektivt rättsmedel. Denna rätt ska inbegripa rätten att bestrida en sådan avlägsnandeorder inför domstolarna i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern och rätten att bestrida beslutet enligt artikel 4.4 eller artikel 5.4, 5.6 eller 5.7 inför domstolarna i den medlemsstat vars behöriga myndighet fattade beslutet.

2. Innehållsleverantörer vars innehåll har avlägsnats eller gjorts oåtkomligt till följd av en avlägsnandeorder ska ha rätt till ett effektivt rättsmedel. Denna rätt ska inbegripa rätten att bestrida en avlägsnandeorder som har utfärdats enligt artikel 3.1 inför domstolarna i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern och rätten att bestrida ett beslut enligt artikel 4.4 inför domstolarna i den medlemsstat vars behöriga myndighet utfärdade avlägsnandeordern eller fattade beslutet.

3. Medlemsstaterna ska införa effektiva förfaranden för utövandet av de rättigheter som avses i denna artikel.

Artikel 10

Klagomålsmekanismer

1. Varje värdtjänstleverantör ska inrätta en effektiv och tillgänglig mekanism som gör det möjligt för innehållsleverantörer att, när deras innehåll har avlägsnats eller gjorts oåtkomligt till följd av specifika åtgärder enligt artikel 5, lämna in ett klagomål mot att innehållet avlägsnats eller gjorts oåtkomligt med en begäran om att det avlägsnade innehållet eller åtkomsten till det återställs.

2. Varje värdtjänstleverantör ska snabbt granska alla klagomål som den tar emot genom den mekanism som avses i punkt 1 och utan onödigt dröjsmål återställa innehållet eller åtkomsten till det om det inte var berättigat att avlägsna innehållet eller göra det oåtkomligt. Den ska informera klaganden om resultatet av klagomålet inom två veckor från det att det mottagits.

Om klagomålet avslås ska värdtjänstleverantören underrätta klaganden om skälen till dess beslut.

Ett återställande av innehåll eller åtkomsten till det ska inte utesluta administrativa eller rättsliga förfaranden för prövning av värdtjänstleverantörens eller den behöriga myndighetens beslut.

Artikel 11

Information till innehållsleverantörer

1. Om en värdtjänstleverantör avlägsnar terrorisminnehåll eller gör det oåtkomligt ska den ge innehållsleverantören information om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

2. På innehållsleverantörens begäran ska värdtjänstleverantören antingen informera innehållsleverantören om skälen till att innehållet avlägsnades eller gjordes oåtkomligt och dess rätt att bestrida avlägsnandeordern eller tillhandahålla innehållsleverantören en kopia av avlägsnandeordern.

3. Skyldigheten enligt punkterna 1 och 2 ska inte gälla om den behöriga myndighet som utfärdar avlägsnandeordern beslutar att det är nödvändigt och proportionellt att skälen inte lämnas ut av hänsyn till allmän säkerhet, såsom förebyggande, förhindrande, utredning, upptäckt och lagföring av terroristbrott, under så lång tid som det är nödvändigt, men inte längre än sex veckor efter det beslutet. I ett sådant fall ska värdtjänstleverantören inte lämna någon information om att terrorisminnehållet har avlägsnats eller gjorts oåtkomligt.

Den behöriga myndigheten får förlänga den perioden med ytterligare sex veckor, om det fortfarande finns motiverade skäl till att inte lämna ut skälen.

Avsnitt IV

Behöriga myndigheter och samarbete

Artikel 12

Utseende av behöriga myndigheter

1. Varje medlemsstat ska utse den eller de myndigheter som är behöriga att

a) utfärda avlägsnandeorder enligt artikel 3,

b) granska avlägsnandeorder enligt artikel 4,

c) övervaka genomförandet av specifika åtgärder enligt artikel 5,

d) påföra sanktioner enligt artikel 18.

2. Varje medlemsstat ska säkerställa att en kontaktpunkt utses eller inrättas inom den behöriga myndighet som avses i punkt 1 a för att hantera begäranden om klargöranden och återkoppling avseende avlägsnandeorder som har utfärdats av den behöriga myndigheten.

Medlemsstaterna ska säkerställa att information om kontaktpunkten offentliggörs.

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

4. Senast den … *[tolv månader efter denna förordnings ikraftträdande]* ska kommissionen upprätta ett onlineregister med en förteckning över de behöriga myndigheter som avses i punkt 1 och den kontaktpunkt som utsetts eller inrättats enligt punkt 2 för varje behörig myndighet. Kommissionen ska regelbundet offentliggöra eventuella ändringar avseende dessa.

Artikel 13

Behöriga myndigheter

1. Medlemsstaterna ska säkerställa att deras behöriga myndigheter har de befogenheter och resurser som krävs för att uppnå målen och fullgöra sina skyldigheter enligt denna förordning.

2. Medlemsstaterna ska säkerställa att deras behöriga myndigheter utför sina uppgifter enligt denna förordning på ett objektivt och icke-diskriminerande sätt med fullständig respekt för grundläggande rättigheter. De behöriga myndigheterna får inte efterfråga eller ta emot instruktioner från något annat organ när det gäller utförandet av uppgifter enligt artikel 12.1.

Första stycket i denna punkt ska inte förhindra tillsyn i enlighet med nationell konstitutionell rätt.

Artikel 14

Samarbete mellan värdtjänstleverantörer, behöriga myndigheter och Europol

1. De behöriga myndigheterna ska utbyta information, samordna sig med och samarbeta med varandra och, när så är lämpligt, med Europol, avseende avlägsnandeorder, i synnerhet för att undvika dubbelarbete, förbättra samordningen och undvika att störa utredningar i andra medlemsstater.

2. Medlemsstaternas behöriga myndigheter ska utbyta information, samordna sig med och samarbeta med de behöriga myndigheter som avses i artikel 12.1 c och d avseende specifika åtgärder som vidtas enligt artikel 5 och sanktioner som påförs enligt artikel 18. Medlemsstaterna ska säkerställa att de behöriga myndigheter som avses i artikel 12.1 c och d förfogar över all relevant information.

3. Vid tillämpningen av punkt 1 ska medlemsstaterna sörja för lämpliga och säkra kommunikationskanaler eller mekanismer för att säkerställa att den relevanta informationen utbyts i rätt tid.

4. För en effektiv tillämpning av denna förordning och för att undvika dubbelarbete får medlemsstater och värdtjänstleverantörer använda särskilda verktyg, inbegripet sådana som inrättats av Europol, för att särskilt underlätta

a) handläggning och återkoppling avseende avlägsnandeorder enligt artikel 3, och

b) samarbete i syfte att identifiera och genomföra specifika åtgärder enligt artikel 5.

5. Om värdtjänstleverantörer får kännedom om terrorisminnehåll som medför ett överhängande hot mot en eller flera personers liv ska de omgående underrätta de myndigheter som är behöriga att utreda och lagföra brott i de berörda medlemsstaterna. Om det är omöjligt att identifiera de berörda medlemsstaterna ska värdtjänstleverantörerna underrätta kontaktpunkten enligt artikel 12.2 i den medlemsstat där de har sitt huvudsakliga verksamhetsställe eller där deras rättsliga företrädare är bosatt eller etablerad och vidarebefordra information om det terrorisminnehållet till Europol för lämplig uppföljning.

6. De behöriga myndigheterna uppmanas att skicka kopior av avlägsnandeorder till Europol så att Europol kan tillhandahålla en årlig rapport med en analys av vilka typer av terrorisminnehåll som har varit föremål för en avlägsnandeorder eller en order om att göra det oåtkomligt enligt denna förordning.

Artikel 15

Värdtjänstleverantörers kontaktpunkter

1. Varje värdtjänstleverantör ska utse eller inrätta en kontaktpunkt för mottagande av avlägsnandeorder på elektronisk väg och snabb handläggning av dem enligt artiklarna 3 och 4. Värdtjänstleverantören ska säkerställa att information om kontaktpunkten offentliggörs.

2. I den information som avses i punkt 1 i denna artikel ska det anges på vilka av unionsinstitutionernas officiella språk, i den mening som avses i förordning 1/58 ([15]), som kontaktpunkten kan kontaktas och ytterligare utbyten avseende avlägsnandeorder enligt artikel 3 äga rum. Dessa språk ska omfatta åtminstone ett av de officiella språken i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad.

([15]) Förordning nr 1 om vilka språk som skall användas i Europeiska ekonomiska gemenskapen (EGT 17, 6.10.1958, s. 385).

Avsnitt V

Genomförande och verkställighet

Artikel 16

Jurisdiktion

1. Den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe ska ha jurisdiktion vid tillämpningen av artiklarna 5, 18 och 21. En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen ska anses lyda under jurisdiktionen i den medlemsstat där dess rättsliga företrädare är bosatt eller etablerad.

2. Om en värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen inte har utsett en rättslig företrädare ska samtliga medlemsstater ha jurisdiktion.

3. Om en behörig myndighet i en medlemsstat utövar jurisdiktion enligt punkt 2 ska den informera de behöriga myndigheterna i alla övriga medlemsstater.

Artikel 17

Rättslig företrädare

1. En värdtjänstleverantör som inte har sitt huvudsakliga verksamhetsställe i unionen ska skriftligen utse en fysisk eller juridisk person till sin rättsliga företrädare i unionen för mottagande, efterlevnad och verkställighet av avlägsnandeorder och beslut som utfärdas av de behöriga myndigheterna.

2. Värdtjänstleverantören ska förse sin rättsliga företrädare med de befogenheter och resurser som krävs för att följa dessa avlägsnandeorder och beslut och för att samarbeta med de behöriga myndigheterna.

Den rättsliga företrädaren ska vara bosatt eller etablerad i en av de medlemsstater där värdtjänstleverantören erbjuder sina tjänster.

3. Den rättsliga företrädaren får hållas ansvarig för överträdelser av denna förordning, utan att det påverkar värdtjänstleverantörens eventuella ansvarighet eller eventuella rättsliga åtgärder mot denne.

4. Värdtjänstleverantören ska underrätta den behöriga myndighet som avses i artikel 12.1 d i den medlemsstat där dess rättsliga företrädare är bosatt eller etablerad om utseendet.

Informationen om den rättsliga företrädaren ska offentliggöras av värdtjänstleverantören.

Avsnitt VI

Slutbestämmelser

Artikel 18

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för värdtjänstleverantörers överträdelser av bestämmelserna i denna förordning och vidta alla åtgärder som krävs för att säkerställa att de tillämpas. Sådana sanktioner ska vara begränsade till överträdelser av artiklarna 3.3 och 3.6, 4.2 och 4.7, 5.1, 5.2, 5.3, 5.5 och 5.6, 6, 7, 10 och 11, 14.5, 15.1 och 17.

De sanktioner som avses i första stycket ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den … *[tolv månader efter denna förordnings ikraftträdande]* samt utan dröjsmål eventuella ändringar som berör dem.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de beslutar huruvida en sanktion ska påföras och när de fastställer sanktioneras typ och nivå, beaktar alla relevanta omständigheter, inbegripet

a) överträdelsens karaktär, allvar och varaktighet,

b) om överträdelsen var avsiktlig eller orsakades av vårdslöshet,

c) tidigare överträdelser som värdtjänstleverantören har gjort sig skyldig till,

d) värdtjänstleverantörens finansiella styrka,

e) graden av tjänsteleverantörens samarbete med de behöriga myndigheterna,

f) värdtjänstleverantörens karaktär och storlek, i synnerhet huruvida det är ett mikroföretag, litet eller medelstort företag,

g) graden av skuld hos värdtjänstleverantören, med beaktande av de tekniska och organisatoriska åtgärder som den har vidtagit för att följa denna förordning.

3. Medlemsstaterna ska säkerställa att en systematisk eller fortgående underlåtenhet att fullgöra skyldigheterna enligt artikel 3.3 blir föremål för böter på upp till 4 % av värdtjänstleverantörens totala omsättning under det föregående räkenskapsåret.

Artikel 19

Tekniska krav och ändringar av bilagorna

1. Kommissionen ges 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.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 20 för att ändra bilagorna i syfte att effektivt åtgärda eventuella behov av förbättringar av innehållet i mallarna för avlägsnandeorder och för att meddela att det är omöjligt att verkställa avlägsnandeorder.

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 ges till kommissionen tills vidare från och med den … *[ett år efter dagen för denna förordnings ikraftträdande]*.

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 av den 13 april 2016 om bättre lagstiftning.

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 värdtjänstleverantörer under deras jurisdiktion om de åtgärder som dessa under det föregående kalenderåret har vidtagit i enlighet med denna förordning och sända informationen till kommissionen senast den 31 mars varje år. Denna information ska omfatta följande:

a) Antalet utfärdade avlägsnandeorder och antalet inslag med terrorisminnehåll som har avlägsnats eller gjorts oåtkomliga, och hur fort de har avlägsnats eller gjorts oåtkomliga.

b) De specifika åtgärder som har vidtagits enligt artikel 5, inklusive antalet inslag med terrorisminnehåll som har avlägsnats eller gjorts oåtkomliga, och hur fort de har avlägsnats eller gjorts oåtkomliga.

c) Antalet begäranden om åtkomst som har utfärdats av behöriga myndigheter avseende innehåll som bevaras av värdtjänstleverantörer enligt artikel 6.

d) Antalet klagomålsförfaranden som har inletts och de åtgärder som vidtagits av värdtjänstleverantörerna enligt artikel 10.

e) Antalet administrativa eller rättsliga prövningsförfaranden som har inletts och beslut som fattats av den behöriga myndigheten i enlighet med nationell rätt.

2. Senast den … *[två år efter dagen för denna förordnings ikraftträdande]* ska kommissionen inrätta ett detaljerat program för övervakning av denna förordnings utfall, resultat och effekter. I övervakningsprogrammet ska de indikatorer och metoder som ska användas för att samla in uppgifter och andra nödvändiga belägg anges samt med vilka intervaller insamlingen 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 enligt 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. Den rapporten ska inkludera information om övervakning enligt artikel 21 och information som härrör från transparenskraven enligt artikel 8. Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta rapporten.

Artikel 23

Utvärdering

Senast den … *[tre år efter dagen för denna förordnings ikraftträdande]* ska kommissionen göra en utvärdering av denna förordning och lägga fram en rapport för Europaparlamentet och rådet om dess tillämpning, inklusive

a) funktionen hos och ändamålsenligheten i skyddsmekanismerna, särskilt de som föreskrivs i artikel 4.4, 6.3 och artiklarna 7–11,

b) den inverkan som tillämpningen av denna förordning har på de grundläggande rättigheterna, särskilt yttrande- och informationsfriheten, respekten för privatlivet och skyddet av personuppgifter, samt

c) denna förordnings bidrag till att skydda den allmänna säkerheten.

Vid behov ska rapporten åtföljas av lagstiftningsförslag.

Medlemsstaterna ska förse kommissionen med den information som är nödvändig för att utarbeta rapporten.

Kommissionen ska även bedöma hur nödvändigt och genomförbart det är att inrätta en europeisk plattform om terrorisminnehåll online för att underlätta kommunikation och samarbete enligt denna förordning.

Artikel 24

Ikraftträdande och tillämpning

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 … *[tolv månader efter denna förordnings ikraftträdande]*.

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

Utfärdad i …

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

BILAGA I

AVLÄGSNANDEORDER

(artikel 3 i Europaparlamentets och rådets förordning (EU) 2021/… ([1]) ([*]))

Enligt artikel 3 i förordning (EU) 2021/… ([*]) (*förordningen*) ska den som mottar denna avlägsnandeorder avlägsna terrorisminnehåll eller göra terrorisminnehåll oåtkomligt i samtliga medlemsstater så snart som möjligt och i alla händelser inom en timme från mottagandet av avlägsnandeordern.

Enligt artikel 6 i förordningen ska mottagaren bevara innehåll och därtill hörande data som har avlägsnats eller gjorts oåtkomliga i sex månader eller längre på begäran av behöriga myndigheter eller domstolar.

Enligt artikel 15.2 i förordningen ska denna avlägsnandeorder sändas på ett av de språk som mottagaren har angett.

AVSNITT A:

Den utfärdande behöriga myndighetens medlemsstat:

……

Anm.: uppgifter om den utfärdande behöriga myndigheten ska lämnas i avsnitten E och F

Mottagare och, om tillämpligt, rättslig företrädare:

……

Kontaktpunkt:

……

Medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad:

……

Tid och datum för utfärdande av avlägsnandeordern:

……

Referensnummer för avlägsnandeordern:

……

([1]) Europaparlamentets och rådets förordning (EU) 2021/…([*]) om åtgärder mot spridning av terrorisminnehåll online (EUT L …).

([*]) Numret på förordningen i dokument ST 14308/20 (2018/0331 (COD))

AVSNITT B: Terrorisminnehåll som ska avlägsnas eller göras oåtkomligt i alla medlemsstater så snart som möjligt och i alla händelser inom en timme efter mottagandet av avlägsnandeordern:

Webbadress (URL) och eventuell annan information som gör det möjligt att identifiera och hitta exakt plats för terrorisminnehållet:

……

Orsaker till att materialet anses vara terrorisminnehåll, i enlighet med artikel 2.7 i förordningen.

Materialet (kryssa för relevant(a) ruta/rutor)

☐ anstiftar andra till att begå terroristbrott, exempelvis genom att förhärliga terroristgärningar, genom att förespråka att sådana brott begås (artikel 2.7 a i förordningen)

☐ värvar andra för att begå eller bidra till begåendet av terroristbrott (artikel 2.7 b i förordningen)

☐ värvar andra för att delta i en terroristgrupps verksamhet (artikel 2.7 c i förordningen)

☐ tillhandahåller instruktioner om tillverkning eller användning av sprängämnen, skjutvapen eller andra vapen eller skadliga eller farliga ämnen, eller om andra specifika metoder eller tekniker för begående av eller bidragande till begående av terroristbrott (artikel 2.7 d i förordningen)

☐ utgör ett hot om begående av ett av terroristbrotten (artikel 2.7 e i förordningen)

Ytterligare information om orsakerna till att materialet anses vara terrorisminnehåll:

……

……

……

AVSNITT C: Information till innehållsleverantören

Observera att (kryssa för rutan, om det är tillämpligt)

☐ mottagaren **får** av hänsyn till allmän säkerhet **inte informera innehållsleverantören** om att innehållet avlägsnas eller görs oåtkomligt

Om rutan inte är relevant, se avsnitt G för uppgifter om möjligheterna enligt nationell rätt att bestrida avlägsnandeordern i den utfärdande behöriga myndighetens medlemsstat (en kopia av avlägsnandeordern måste på begäran skickas till innehållsleverantören).

AVSNITT D: Information till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad

Kryssa för relevant(a) ruta/rutor

☐ Den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad är en annan än den utfärdande behöriga myndighetens medlemsstat

☐ En kopia av avlägsnandeordern skickas till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad

AVSNITT E: Uppgifter om den utfärdande behöriga myndigheten

Typ (kryssa för relevant ruta)

☐ domare, domstol eller undersökningsdomare

☐ brottsbekämpande myndighet

☐ annan behörig myndighet → fyll även i avsnitt F

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

Den utfärdande behöriga myndighetens namn:

……

Namn på myndighetens företrädare och dennes befattning (titel och grad):

……

Dokumentnummer: ……

Adress: ……

Tfn: (landsnummer) (riktnummer) ……

Fax: (landsnummer) (riktnummer) ……

E-postadress: ……

Datum: ……

Officiell stämpel (om tillämpligt) och underskrift ([2]) : ……

([2]) En underskrift är inte nödvändig om avlägsnandeordern sänds via autentiserade inlämningskanaler som kan garantera att avlägsnandeordern är autentisk.

AVSNITT F: Kontaktuppgifter för uppföljning

Kontaktuppgifter till den utfärdande behöriga myndigheten för återkoppling om den tidpunkt då innehållet avlägsnades eller gjordes oåtkomligt, eller för att lämna ytterligare klargöranden:

……

Kontaktuppgifter till den behöriga myndigheten i den medlemsstat där värdtjänstleverantören har sitt huvudsakliga verksamhetsställe eller där dess rättsliga företrädare är bosatt eller etablerad:

……

AVSNITT G: Information om möjligheter till prövning

Information om behörigt organ eller behörig domstol, tidsfrister och förfaranden för bestridande av avlägsnandeordern

Behörigt organ eller behörig domstol vid vilken avlägsnandeordern kan bestridas:

……

Tidsfrist för bestridande av avlägsnandeordern:

[dagar/månader från och med]

……

Länk till bestämmelser i nationell lagstiftning:

……

BILAGA II

ÅTERKOPPLING EFTER DET ATT TERRORISMINNEHÅLL HAR AVLÄGSNATS ELLER GJORTS OÅTKOMLIGT

(artikel 3.6 i Europaparlamentets och rådets förordning (EU) 2021/ … ([1]) ([*]))

AVSNITT A:

Avlägsnandeorderns mottagare:

……

Behörig myndighet som utfärdade avlägsnandeordern:

……

Referensnummer för den behöriga myndighet som utfärdade avlägsnandeordern:

……

Referensnummer för mottagaren:

……

Tid och datum för mottagande av avlägsnandeordern:

……

AVSNITT B: Åtgärder som vidtagits i enlighet med avlägsnandeordern

(Kryssa för relevant ruta)

☐ terrorisminnehållet har avlägsnats

☐ terrorisminnehållet har gjorts oåtkomligt i alla medlemsstater

Tid och datum då åtgärden vidtogs:

……

([1]) Europaparlamentets och rådets förordning (EU) 2021/ … ([*]) om åtgärder mot spridning av terrorisminnehåll online (EUT L …).

([*]) Numret på förordningen i dokument ST 14308/20 (2018/0331 (COD)).

AVSNITT C: Uppgifter om mottagaren

Namn på värdtjänstleverantören:

……

ELLER

Namn på värdtjänstleverantörens rättsliga företrädare:

……

Medlemsstat där värdtjänstleverantörens har sitt huvudsakliga verksamhetsställe:

……

ELLER

Medlemsstat där värdtjänstleverantörens rättsliga företrädare är bosatt eller etablerad:

……

Namn på den bemyndigade personen:

……

Kontaktpunktens e-postadress:

……

Datum:

……

BILAGA III

INFORMATION OM ATT DET ÄR OMÖJLIGT ATT VERKSTÄLLA AVLÄGSNANDEORDERN

(artikel 3.7 och 3.8 i Europaparlamentets och rådets förordning (EU) 2021/ … ([1]) ([*]))

AVSNITT A:

Avlägsnandeorderns mottagare:

……

Behörig myndighet som utfärdade avlägsnandeordern:

……

Referensnummer för den behöriga myndighet som utfärdade avlägsnandeordern:

……

Referensnummer för mottagaren:

……

Tid och datum för mottagande av avlägsnandeordern:

……

AVSNITT B: Utebliven verkställighet

1. Avlägsnandeordern kan inte verkställas inom tidsfristen av följande orsaker (kryssa för relevant(a) ruta/rutor):

   ☐ force majeure eller faktisk omöjlighet som inte kan tillskrivas värdtjänstleverantören, inbegripet av objektivt motiverade tekniska eller operativa skäl

   ☐ avlägsnandeordern innehåller uppenbara fel

   ☐ avlägsnandeordern innehåller inte tillräckligt med information

2. Redogör närmare för orsakerna till utebliven verkställighet:

   ……

3. Om avlägsnandeordern innehåller uppenbara fel och/eller inte innehåller tillräckligt med information, precisera felen och den ytterligare information eller de ytterligare klargöranden som krävs:

   ……

([1]) Europaparlamentets och rådets förordning (EU) 2021/ …([*]) om åtgärder mot spridning av terrorisminnehåll online (EUT L …).

([*]) Numret på förordningen i dokument ST 14308/20 (2018/0331 (COD)).

AVSNITT C: Uppgifter om värdtjänstleverantören eller dess rättsliga företrädare

Namn på värdtjänstleverantören:

……

ELLER

Namn på värdtjänstleverantörens rättsliga företrädare:

……

Namn på den bemyndigade personen:

……

Kontaktuppgifter (e-postadress):

……

Underskrift:

……

Tid och datum:

……