VERORDENING (EU) 2021/784 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 29 april 2021

inzake het tegengaan van de verspreiding van terroristische online-inhoud

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité ([1]),

Handelend volgens de gewone wetgevingsprocedure ([2]),

Overwegende hetgeen volgt:

(1) Deze verordening heeft tot doel te zorgen voor de goede werking van de digitale eengemaakte markt in een open en democratische samenleving, door misbruik van hostingdiensten voor terroristische doeleinden tegen te gaan en bij te dragen tot de openbare veiligheid in de Unie. De werking van de digitale eengemaakte markt moet worden verbeterd door aanbieders van hostingdiensten meer rechtszekerheid te bieden, het vertrouwen van de gebruikers in de online-omgeving te vergroten en de waarborgen voor de vrijheid van meningsuiting, inclusief de vrijheid om inlichtingen of denkbeelden te ontvangen en door te geven in een open en democratische samenleving, evenals de waarborgen voor de vrijheid en het pluralisme van de media, solider te maken.

(2) Regelgeving om de verspreiding van terroristische online-inhoud tegen te gaan, moet worden aangevuld met strategieën van de lidstaten voor terrorismebestrijding, met inbegrip van het vergroten van mediawijsheid en het verbeteren van kritisch denken, het ontwikkelen van alternatieve en tegenverhalen, en andere initiatieven om het effect van en de kwetsbaarheid voor terroristische online-inhoud te verminderen, alsook het investeren in maatschappelijk werk, deradicaliseringsinitiatieven en contacten met getroffen gemeenschappen om radicalisering in de samenleving duurzaam te voorkomen.

(3) Het tegengaan van terroristische online-inhoud, wat een onderdeel is van een breder probleem van illegale online-inhoud, vergt een combinatie van wetgevende, niet-wetgevende en vrijwillige maatregelen op basis van samenwerking tussen autoriteiten en aanbieders van hostingdiensten, op een manier die de grondrechten ten volle eerbiedigt.

(4) Aanbieders van hostingdiensten die op het internet actief zijn, spelen een essentiële rol in de digitale economie doordat zij ondernemingen en burgers met elkaar verbinden en het publieke debat en de verspreiding en ontvangst van informatie, meningen en ideeën faciliteren, wat een aanzienlijke bijdrage levert aan innovatie, economische groei en banencreatie in de Unie. De diensten van de aanbieders van hostingdiensten worden echter in bepaalde gevallen door derden misbruikt met als doel online illegale activiteiten uit te voeren. Bijzonder zorgwekkend is het misbruik van die diensten door terroristische groeperingen en hun aanhangers met als doel terroristische online-inhoud te verspreiden om hun boodschap uit te dragen, volgelingen te radicaliseren en te werven, en terroristische activiteiten te faciliteren en aan te sturen.

([1]) PB C 110 van 22.3.2019, blz. 67.

([2]) Standpunt van het Europees Parlement van 17 april 2019 (nog niet bekendgemaakt in het Publicatieblad) en standpunt van de Raad in eerste lezing van 16 maart 2021 (PB C 135 van 16.4.2021, blz. 1). Standpunt van het Europees Parlement van 28 april 2021 (nog niet bekendgemaakt in het Publicatieblad).

(5) De aanwezigheid van terroristische online-inhoud is weliswaar niet de enige factor, maar is een katalysator gebleken voor de radicalisering van personen die kan leiden tot terroristische daden, en heeft derhalve ernstige negatieve gevolgen voor de gebruikers, de burgers en de samenleving in het algemeen alsook voor de aanbieders van onlinediensten die zulke inhoud hosten, omdat hierdoor het vertrouwen van hun gebruikers wordt ondermijnd en hun bedrijfsmodellen worden geschaad. Aanbieders van hostingdiensten hebben, gezien hun centrale rol en de technologische middelen en mogelijkheden die met de door hen verleende diensten gepaard gaan, een bijzondere maatschappelijke verantwoordelijkheid om hun diensten te beschermen tegen misbruik door terroristen en om te helpen bij het tegengaan van de verspreiding van terroristische inhoud die via hun diensten online wordt verspreid, zonder het fundamentele belang van de vrijheid van meningsuiting, inclusief de vrijheid kennis te nemen en te geven van informatie en ideeën in een open en democratische samenleving, uit het oog te verliezen.

(6) De inspanningen op Unieniveau om terroristische online-inhoud te bestrijden, zijn in 2015 opgestart met een kader voor vrijwillige samenwerking tussen lidstaten en aanbieders van hostingdiensten. Die inspanningen moeten worden aangevuld met een duidelijk wetgevend kader teneinde terroristische online-inhoud nog minder toegankelijk te maken en een zich snel ontwikkelend probleem adequaat aan te pakken. Het wetgevend kader moet voortbouwen op de vrijwillige inspanningen, die zijn versterkt door Aanbeveling (EU) 2018/334 van de Commissie ([3]), en biedt een antwoord op de oproep van het Europees Parlement om de maatregelen tegen illegale en schadelijke online-inhoud aan te scherpen, overeenkomstig het bij Richtlijn 2000/31/EG van het Europees Parlement en de Raad ([4]) vastgestelde horizontale kader, en de oproep van de Europese Raad om de opsporing en verwijdering van online-inhoud die tot terroristische daden aanzet, te verbeteren.

(7) Deze verordening mag geen afbreuk doen aan de toepassing van Richtlijn 2000/31/EG. Met name mogen maatregelen die een aanbieder van hostingdiensten ter naleving van deze verordening heeft genomen, inclusief specifieke maatregelen, er op zich niet toe leiden dat die aanbieder van hostingdiensten de vrijstelling van aansprakelijkheid verliest waarin die richtlijn voorziet. De bevoegdheden van nationale autoriteiten en rechterlijke instanties om aanbieders van hostingdiensten aansprakelijk te stellen indien niet is voldaan aan de in die richtlijn vastgestelde voorwaarden voor vrijstelling van aansprakelijkheid, worden door deze verordening bovendien onverlet gelaten.

(8) In geval van strijdigheid tussen deze verordening en Richtlijn 2010/13/EU van het Europees Parlement en de Raad ([5]) met betrekking tot bepalingen betreffende audiovisuele mediadiensten in de zin van artikel 1, lid 1, punt a), van die richtlijn, moet Richtlijn 2010/13/EU voorrang hebben. Dat moet de verplichtingen uit hoofde van deze verordening, met name ten aanzien van aanbieders van videoplatforms, onverlet laten.

(9) In deze verordening moeten regels worden vastgesteld om het misbruik van hostingdiensten voor de verspreiding van terroristische online-inhoud tegen te gaan teneinde de goede werking van de interne markt te waarborgen. Die regels moeten de in de Unie beschermde grondrechten ten volle eerbiedigen, met name die welke zijn verankerd in het Handvest van de grondrechten van de Europese Unie ("het Handvest").

(10) Doel van deze verordening is bij te dragen aan de bescherming van de openbare veiligheid en tegelijk passende en solide waarborgen te bieden om de bescherming van de grondrechten te garanderen, waaronder het recht op eerbiediging van het privéleven, het recht op de bescherming van persoonsgegevens, het recht op vrijheid van meningsuiting, waaronder de vrijheid kennis te nemen en te geven van informatie, de vrijheid van ondernemerschap en het recht op een doeltreffende voorziening in rechte. Bovendien is iedere discriminatie verboden. De bevoegde autoriteiten en de aanbieders van hostingdiensten mogen alleen maatregelen vaststellen die noodzakelijk, geschikt en proportioneel zijn in een democratische samenleving, waarbij zij rekening houden met het bijzondere belang van de vrijheid van meningsuiting en van informatie, en de vrijheid en het pluralisme van de media, die essentiële fundamenten zijn van een pluralistische en democratische samenleving en de waarden zijn waarop de Unie is gegrondvest. Maatregelen die de vrijheid van meningsuiting en van informatie aantasten moeten strikt afgebakend zijn om de verspreiding van terroristische online-inhoud tegen te gaan, en tegelijk het recht om op rechtmatige wijze kennis te nemen en te geven van informatie te eerbiedigen, rekening houdend met de centrale rol van aanbieders van hostingdiensten bij het faciliteren van het publieke debat en het verspreiden en kennis nemen van feiten, meningen en ideeën, overeenkomstig het recht. Doeltreffende maatregelen om terroristische online-inhoud tegen te gaan en de bescherming van de vrijheid van meningsuiting en van informatie zijn geen tegenstrijdige doelstellingen, maar vullen elkaar juist aan en versterken elkaar.

([3]) Aanbeveling (EU) 2018/334 van de Commissie van 1 maart 2018 over maatregelen om illegale online-inhoud effectief te bestrijden (PB L 63 van 6.3.2018, blz. 50).

([4]) Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel") (PB L 178 van 17.7.2000, blz. 1).

([5]) Richtlijn 2010/13/EU van het Europees Parlement en de Raad van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten) (PB L 95 van 15.4.2010, blz. 1).

(11) Om duidelijkheid te verschaffen over de maatregelen die zowel aanbieders van hostingdiensten als bevoegde autoriteiten moeten nemen om de verspreiding van terroristische online-inhoud tegen te gaan, moet deze verordening met het oog op preventie een definitie van "terroristische inhoud" vaststellen die spoort met de definities van de relevante misdrijven van Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad ([6]). Omdat de schadelijkste terroristische onlinepropaganda moet worden aangepakt, moet die eerste definitie ook materiaal omvatten dat iemand aanzet of aanspoort tot het plegen van, of tot het leveren van een bijdrage aan het plegen van, terroristische misdrijven, dat iemand aanspoort om deel te nemen aan activiteiten van een terroristische groepering, of dat terroristische activiteiten verheerlijkt, met inbegrip van materiaal waarop een terroristische aanslag wordt afgebeeld. De definitie moet ook materiaal omvatten dat instructies geeft voor het maken of gebruiken van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, evenals chemische, biologische, radiologische en nucleaire stoffen (CBRN-stoffen), of voor andere specifieke methoden of technieken, met inbegrip van het selecteren van doelwitten, voor het plegen of het bijdragen aan het plegen van terroristische misdrijven. Dergelijk materiaal omvat tekst, beelden, geluidsopnamen en video's, alsmede het rechtstreeks uitzenden van terroristische misdrijven, waardoor het gevaar ontstaat dat nog meer zulke misdrijven worden gepleegd. Bij de beoordeling of materiaal terroristische inhoud in de zin van deze verordening uitmaakt, moeten bevoegde autoriteiten en aanbieders van hostingdiensten rekening houden met factoren zoals de aard en de bewoordingen van verklaringen, de context waarin de verklaringen zijn afgelegd en hun potentieel om schadelijke gevolgen voor de veiligheid en beveiliging van personen teweeg te brengen. Het feit dat het materiaal geproduceerd is door, toe te rekenen is aan of verspreid is namens een persoon, groep of entiteit die opgenomen is in de Unielijst van personen, groepen en entiteiten die betrokken zijn bij terroristische activiteiten en aan beperkende maatregelen onderworpen zijn, moet een belangrijke factor in de beoordeling zijn.

(12) Materiaal dat voor educatieve, journalistieke, artistieke of onderzoeksdoeleinden of bij voorlichtingsactiviteiten op het gebied van de bestrijding van terroristische activiteiten wordt verspreid, mag niet als terroristische inhoud worden beschouwd. Bij het bepalen of het door een aanbieder van inhoud verstrekt materiaal "terroristische inhoud" is als omschreven in deze verordening, moet met name rekening worden gehouden met het recht op vrijheid van meningsuiting en van informatie, waaronder de vrijheid en het pluralisme van de media, en de vrijheid van kunsten en wetenschappen. In het bijzonder in gevallen waarin de aanbieder van inhoud redactionele verantwoordelijkheid draagt, moet bij elk besluit over de verwijdering van het verspreide materiaal rekening worden gehouden met de journalistieke normen die in overeenstemming met het Unierecht, met inbegrip van het Handvest, zijn vastgesteld in de pers- of mediaregelgeving. Voorts mag de uiting van radicale, polemische of controversiële standpunten in het publieke debat over gevoelige politieke vraagstukken niet als terroristische inhoud worden beschouwd.

(13) Om de verspreiding van terroristische online-inhoud effectief aan te pakken en tegelijk de eerbiediging van het privéleven van personen te garanderen, moet deze verordening van toepassing zijn op aanbieders van diensten van de informatiemaatschappij die door een gebruiker van de dienst verstrekte informatie en verstrekt materiaal op zijn verzoek opslaan en onder het publiek verspreiden, ongeacht of de opslag van dergelijke informatie en dergelijk materiaal en de verspreiding ervan onder het publiek louter technisch, automatisch en passief van aard is. Onder het begrip "opslag" wordt verstaan het bewaren van gegevens in het geheugen van een fysieke of virtuele server. Aanbieders van "mere conduit" of "caching"-diensten en van andere diensten die in andere lagen van de internetinfrastructuur worden aangeboden en die geen opslag omvatten, zoals registers en registrators, alsook aanbieders van domeinnaamsystemen (DNS), betalingsdiensten of diensten die bescherming bieden tegen distributed-denial-of-service (DdoS), moeten derhalve buiten het toepassingsgebied van deze verordening vallen.

(14) Het begrip "onder het publiek verspreiden" moet inhouden dat informatie beschikbaar wordt gesteld aan een mogelijk onbeperkt aantal personen, namelijk dat de informatie gemakkelijk toegankelijk wordt gemaakt voor gebruikers in het algemeen, zonder dat de aanbieder van inhoud verdere maatregelen hoeft te nemen, ongeacht of die personen zich daadwerkelijk toegang verschaffen tot de betrokken informatie. Wanneer voor de toegang tot informatie registratie of toelating tot een groep gebruikers vereist is, mag die informatie dan ook alleen worden geacht onder het publiek te worden verspreid wanneer gebruikers die toegang tot de informatie wensen, automatisch worden geregistreerd of toegelaten zonder menselijke beslissing of selectie van wie toegang krijgt. Interpersoonlijke communicatiediensten, als omschreven in artikel 2, punt 5), van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad ([7]), zoals e-mails of particuliere berichtendiensten, moeten buiten het toepassingsgebied van deze verordening vallen. Informatie mag alleen worden beschouwd als opgeslagen en verspreid onder

([6]) Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad (PB L 88 van 31.3.2017, blz. 6).

([7]) Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (PB L 321 van 17.12.2018, blz. 36).

het publiek in de zin van deze verordening wanneer dergelijke activiteiten op rechtstreeks verzoek van de aanbieder van inhoud worden verricht. Bijgevolg mogen aanbieders van diensten, zoals cloudinfrastructuur, die op verzoek van andere partijen dan de aanbieders van inhoud worden verleend en alleen indirect ten goede komen aan laatstgenoemden, niet onder deze verordening vallen. Deze verordening moet bijvoorbeeld aanbieders van socialemedia-, video-, image- en audio-sharing-diensten omvatten, alsook filesharingdiensten en andere clouddiensten, voor zover die diensten worden gebruikt om de opgeslagen informatie op rechtstreeks verzoek van de aanbieder van inhoud aan het publiek beschikbaar te stellen. Wanneer een aanbieder van hostingdiensten meerdere diensten aanbiedt, mag deze verordening alleen van toepassing zijn op de diensten die onder haar toepassingsgebied vallen.

(15) Terroristische inhoud wordt vaak onder het publiek verspreid via diensten van in derde landen gevestigde aanbieders van hostingdiensten. Om gebruikers in de Unie te beschermen en ervoor te zorgen dat voor alle aanbieders van hostingdiensten die actief zijn op de digitale eengemaakte markt dezelfde voorschriften gelden, moet deze verordening van toepassing zijn op alle aanbieders van de betreffende diensten die in de Unie worden aangeboden, ongeacht in welk land zij hun hoofdvestiging hebben. Een aanbieder van hostingdiensten moet geacht worden diensten aan te bieden in de Unie, als hij natuurlijke personen of rechtspersonen in een of meer lidstaten in staat stelt gebruik te maken van zijn diensten en een wezenlijke band heeft met die lidstaat of lidstaten.

(16) Een wezenlijke band met de Unie moet bestaan wanneer de aanbieder van hostingdiensten een vestiging in de Unie heeft, wanneer zijn diensten gebruikt worden door een aanzienlijk aantal gebruikers in een of meer lidstaten, of wanneer zijn activiteiten op een of meer lidstaten gericht zijn. Of de activiteiten op een of meer lidstaten gericht zijn, moet worden bepaald aan de hand van alle relevante omstandigheden, waaronder factoren zoals het gebruik van een taal of een munteenheid die in de betrokken lidstaat gangbaar is, of de mogelijkheid goederen of diensten vanuit die lidstaat te bestellen. Of de activiteiten op een lidstaat gericht zijn, kan ook afgeleid worden uit de beschikbaarheid van een applicatie in de betrokken nationale appstore, uit het maken van lokale reclame of reclame in een taal die in de betrokken lidstaat gangbaar is, of uit het onderhouden van klantenrelaties, bijvoorbeeld door het bieden van klantenservice in een taal die in die lidstaat gangbaar is. Een wezenlijke band moet ook worden verondersteld wanneer een aanbieder van hostingdiensten zijn activiteiten op een of meer lidstaten richt zoals bepaald in artikel 17, lid 1, punt c), van Verordening (EU) nr. 1215/2012 van het Europees Parlement en de Raad ([8]). De loutere toegankelijkheid van de website van een aanbieder van hostingdiensten, van een e-mailadres of van andere contactgegevens in een of meer lidstaten, mag op zichzelf niet volstaan om van een wezenlijke band te kunnen spreken. Bovendien mag het aanbieden van een dienst met het oog op de loutere naleving van het discriminatieverbod dat in Verordening (EU) 2018/302 van het Europees Parlement en de Raad ([9]) is opgenomen, op die grond alleen niet worden beschouwd als een wezenlijke band met de Unie uitmakend.

(17) De procedure en verplichtingen die voortvloeien uit verwijderingsbevelen waarbij van aanbieders van hostingdiensten na een beoordeling door de bevoegde autoriteiten wordt geëist dat ze terroristische inhoud verwijderen of de toegang daartoe blokkeren, moeten worden geharmoniseerd. Gezien de snelheid waarmee terroristische inhoud via onlinediensten wordt verspreid, moet aan aanbieders van hostingdiensten een verplichting worden opgelegd om de in het verwijderingsbevel geïdentificeerde terroristische inhoud binnen één uur na ontvangst van het verwijderingsbevel te verwijderen of de toegang daartoe in alle lidstaten te blokkeren. Behalve in terdege gemotiveerde noodgevallen moet de bevoegde autoriteit aan de aanbieder van hostingdiensten ten minste 12 uur voordat een verwijderingsbevel voor de eerste keer aan die aanbieder van hostingdiensten werd uitgevaardigd, informatie verstrekken over de procedures en toepasselijke termijnen. Terdege gemotiveerde noodgevallen doen zich voor wanneer het verwijderen van of het blokkeren van de toegang tot de terroristische inhoud later dan één uur na de ontvangst van het verwijderingsbevel tot ernstige schade zou leiden, bijvoorbeeld in situaties van een onmiddellijke bedreiging voor het leven of de fysieke integriteit van een persoon of wanneer die inhoud lopende gebeurtenissen afbeeldt die schade aan het leven of de fysieke integriteit van een persoon teweegbrengen. Het is aan de bevoegde autoriteit om te bepalen of gevallen dergelijke noodgevallen uitmaken en om haar besluit terdege te motiveren in het verwijderingsbesluit. Indien de aanbieder van hostingdiensten het verwijderingsbevel niet binnen een uur na de ontvangst ervan kan uitvoeren, vanwege overmacht of omdat het feitelijk onmogelijk is, met inbegrip van objectief te motiveren technische of operationele redenen, moet hij de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd daarvan zo spoedig mogelijk in kennis stellen en het verwijderingsbevel naleven zodra de situatie opgelost is.

([8]) Verordening (EU) nr. 1215/2012 van het Europees Parlement en de Raad van 12 december 2012 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken (PB L 351 van 20.12.2012, blz. 1).

([9]) Verordening (EU) 2018/302 van het Europees Parlement en de Raad van 28 februari 2018 inzake de aanpak van ongerechtvaardigde geoblocking en andere vormen van discriminatie van klanten op grond van nationaliteit, verblijfplaats of plaats van vestiging in de interne markt, en tot wijziging van Verordeningen (EG) nr. 2006/2004 en (EU) 2017/2394 en Richtlijn 2009/22/EG (PB L 60I van 2.3.2018, blz. 1).

(18) Het verwijderingsbevel moet een motivering bevatten waarom het materiaal dat verwijderd moet worden of waartoe de toegang geblokkeerd moet worden, als terroristische inhoud wordt aangemerkt, en het moet voldoende informatie bevatten om die inhoud te kunnen vinden, en wel door de exacte URL en indien nodig alle andere bijkomende informatie te verstrekken, zoals een screenshot van de betrokken inhoud. Die motivering moet de aanbieder van hostingdiensten en, uiteindelijk, de aanbieder van inhoud in staat stellen hun recht op voorziening in rechte doeltreffend uit te oefenen. De motivering mag geen gevoelige informatie openbaar maken die lopende onderzoeken in het gedrang kan brengen.

(19) De bevoegde autoriteit moet het verwijderingsbevel rechtstreeks bij het voor de toepassing van deze verordening door de aanbieder van hostingdiensten aangegeven of opgerichte contactpunt indienen door middel van elektronische middelen die een schriftelijk bewijs kunnen genereren op zodanige wijze dat de aanbieder van hostingdiensten de authenticiteit van het verwijderingsbevel kan vaststellen, inclusief de juistheid van de datum en het tijdstip van de verzending en de ontvangst van het bevel, bijvoorbeeld via beveiligde e-mail of platformen of andere beveiligde kanalen, met inbegrip van die welke door de aanbieder van hostingdiensten beschikbaar worden gesteld, overeenkomstig het Unierecht inzake de bescherming van persoonsgegevens. Het moet mogelijk zijn dat vereiste na te leven onder meer door het gebruik van gekwalificeerde diensten voor elektronisch aangetekende bezorging in de zin van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([10]). Wanneer de hoofdvestiging van de aanbieder van hostingdiensten of de verblijf- of vestigingsplaats van zijn wettelijke vertegenwoordiger zich in een andere lidstaat bevindt dan die van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt, moet tegelijkertijd een kopie van het verwijderingsbevel bij de bevoegde autoriteit van die lidstaat ingediend worden.

(20) Het moet voor de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, mogelijk zijn om het verwijderingsbevel van de bevoegde autoriteiten van een andere lidstaat te toetsen om na te gaan of het geen inbreuk vormt op deze verordening of op de grondrechten uit hoofde van het Handvest. Zowel de aanbieder van inhoud als de aanbieder van hostingdiensten moet het recht hebben om te verzoeken om een dergelijke toetsing door de bevoegde autoriteit in de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft. Indien een dergelijk verzoek wordt gedaan, moet die bevoegde autoriteit een besluit nemen over de vraag of het verwijderingsbevel een dergelijke inbreuk bevat. Indien dat besluit een dergelijke inbreuk vaststelt, mag het verwijderingsbevel geen rechtsgevolgen meer hebben. De toetsing moet snel worden uitgevoerd om ervoor te zorgen dat inhoud die onterecht verwijderd is of waartoe de toegang onterecht geblokkeerd is, zo spoedig mogelijk hersteld wordt of weer toegankelijk gemaakt wordt.

(21) Aanbieders van hostingdiensten die aan terroristische inhoud worden blootgesteld, moeten in hun algemene voorwaarden — als ze die hebben — bepalingen opnemen om het misbruik van hun diensten voor de verspreiding van terroristische inhoud tegen te gaan. Zij moeten die bepalingen op een zorgvuldige, transparante, proportionele en niet-discriminerende wijze toepassen.

(22) Gezien de omvang van het probleem en de snelheid die nodig is om terroristische inhoud effectief te identificeren en te verwijderen, zijn doeltreffende en proportionele specifieke maatregelen een essentieel element om terroristische online-inhoud tegen te gaan. Om terroristische inhoud op hun diensten minder toegankelijk te maken, moeten aanbieders van hostingdiensten die aan terroristische inhoud blootgesteld worden, specifieke maatregelen invoeren, rekening houdend met de risico's en de mate van blootstelling aan terroristische inhoud alsook met de gevolgen voor de rechten van derden en het publieke belang van informatie. Aanbieders van hostingdiensten moeten bepalen welke passende, doeltreffende en proportionele specifieke maatregel ingevoerd moet worden om terroristische inhoud te identificeren en te verwijderen. Specifieke maatregelen kunnen passende technische of operationele maatregelen of capaciteiten omvatten, zoals personele of technische middelen om terroristische inhoud te identificeren en snel te verwijderen of de toegang daartoe snel te blokkeren, mechanismen voor gebruikers om vermeende terroristische inhoud te melden of markeren, of andere maatregelen die de aanbieder van hostingdiensten passend en doeltreffend acht om de beschikbaarheid van terroristische inhoud op zijn diensten tegen te gaan.

(23) Bij het invoeren van specifieke maatregelen moeten aanbieders van hostingdiensten ervoor zorgen dat het recht van gebruikers op vrijheid van meningsuiting en van informatie en de vrijheid en het pluralisme van de media als beschermd uit hoofde van het Handvest behouden blijven. Aanbieders van hostingdiensten moeten niet alleen alle in het recht neergelegde vereisten naleven, waaronder wetgeving inzake de bescherming van persoonsgegevens, maar, waar passend, ook de nodige zorgvuldigheid aan de dag leggen en waarborgen instellen, onder meer toezicht en verificatie door mensen, om onbedoelde of onterechte besluiten te voorkomen die leiden tot de verwijdering van of de blokkering van de toegang tot inhoud die geen terroristische inhoud is.

([10]) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

(24) De aanbieder van hostingdiensten moet bij de bevoegde autoriteit verslag uitbrengen over de specifieke maatregelen zodat die bevoegde autoriteit kan beoordelen of de maatregelen doeltreffend en proportioneel zijn en of, indien automatische middelen worden gebruikt, de aanbieder van hostingdiensten over de nodige capaciteiten beschikt voor toezicht en verificatie door mensen. Bij het beoordelen van de doeltreffendheid en proportionaliteit van de maatregelen moeten de bevoegde autoriteiten rekening houden met relevante parameters, waaronder het aantal tegen de aanbieder van hostingdiensten uitgevaardigde verwijderingsbevelen, de omvang en economische draagkracht van de aanbieder van hostingdiensten en de invloed van zijn diensten op de verspreiding van terroristische inhoud, bijvoorbeeld op basis van het aantal gebruikers in de Unie, alsook met de waarborgen die zijn ingevoerd om misbruik van zijn diensten voor de verspreiding van terroristische online-inhoud tegen te gaan.

(25) Indien de bevoegde autoriteit van oordeel is dat de ingevoerde specifieke maatregelen niet volstaan om de risico's te ondervangen, moet zij kunnen eisen dat bijkomende geschikte, doeltreffende en proportionele specifieke maatregelen worden genomen. Het vereiste om dergelijke bijkomende specifieke maatregelen te nemen, mag niet leiden tot een algemene verplichting tot toezicht of om actief naar feiten te zoeken in de zin van artikel 15, lid 1, van Richtlijn 2000/31/EG, noch tot een verplichting om automatische instrumenten te gebruiken. Het moet evenwel mogelijk zijn voor aanbieders van hostingdiensten om automatische instrumenten te gebruiken indien zij dit geschikt en noodzakelijk achten om misbruik van hun diensten voor de verspreiding van terroristische inhoud doeltreffend tegen te gaan.

(26) De verplichting voor aanbieders van hostingdiensten om verwijderde inhoud en bijbehorende gegevens te bewaren, moet worden opgelegd voor specifieke doeleinden en in de tijd beperkt zijn tot het noodzakelijke. De verplichting tot bewaring moet worden uitgebreid tot de bijbehorende gegevens, als die gegevens bij de verwijdering van de betreffende terroristische inhoud anders verloren zouden gaan. Bijbehorende gegevens kunnen abonneegegevens zijn, waaronder met name gegevens betreffende de identiteit van de aanbieder van inhoud, en toegangsgegevens, waaronder gegevens over de datum en het tijdstip van gebruik door de aanbieder van inhoud en over het in- en uitloggen uit de dienst, samen met het IP-adres dat door de aanbieder van internettoegang aan de aanbieder van inhoud wordt toegekend.

(27) De verplichting tot bewaring van de inhoud met het oog op administratieve of gerechtelijke toetsingsprocedures is noodzakelijk en gerechtvaardigd gelet op de noodzaak om ervoor te zorgen dat de aanbieders van inhoud die verwijderd werd of waartoe de toegang geblokkeerd werd, over doeltreffende voorzieningen in rechte beschikken, en om ervoor te zorgen dat die inhoud hersteld of weer toegankelijk gemaakt wordt, afhankelijk van de uitkomst van die procedures. De verplichting tot bewaring van materiaal met het oog op onderzoek of vervolging is gerechtvaardigd en noodzakelijk gelet op de waarde die het materiaal kan hebben voor het voorkomen of verstoren van terroristische activiteiten. Daarom moet de bewaring van verwijderde terroristische inhoud met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven, ook als gerechtvaardigd worden beschouwd. De terroristische inhoud en de daarmee samenhangende gegevens mogen slechts worden opgeslagen voor de periode die noodzakelijk is om de rechtshandhavingsinstanties in de gelegenheid te stellen die terroristische inhoud te controleren en te beslissen of hij voor die doeleinden nodig is. Voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven moet de vereiste gegevensbewaring beperkt zijn tot gegevens die waarschijnlijk verband houden met terroristische misdrijven, en derhalve kunnen bijdragen tot het vervolgen van terroristische misdrijven of tot het voorkomen van ernstige risico's voor de openbare veiligheid. Wanneer aanbieders van hostingdiensten materiaal verwijderen of de toegang daartoe blokkeren, met name door middel van hun eigen specifieke maatregelen, moeten zij de bevoegde autoriteiten onmiddellijk in kennis stellen van inhoud die informatie bevat die betrekking heeft op een onmiddellijk levensbedreigend gevaar of een vermoedelijk terroristisch misdrijf.

(28) Met het oog op de proportionaliteit moet de bewaringstermijn worden beperkt tot zes maanden om aanbieders van inhoud voldoende tijd te geven om de administratieve of gerechtelijke toetsingsprocedures op te starten, en om de rechtshandhavingsinstanties toegang te bieden tot relevante gegevens voor het onderzoek naar en de vervolging van terroristische misdrijven. Het moet echter mogelijk zijn om die termijn op verzoek van de bevoegde autoriteit of rechterlijke instantie voor zo lang als nodig te verlengen indien die procedures zijn ingeleid maar niet binnen die termijn van zes maanden zijn afgerond. De duur van die bewaringstermijn moet volstaan om de rechtshandhavingsinstanties in staat te stellen het nodige materiaal in verband met onderzoeken en vervolgingen te bewaren, en tegelijk het evenwicht met de grondrechten te garanderen.

(29) Deze verordening heeft geen gevolgen voor de procedurele waarborgen en procedurele onderzoeksmaatregelen in verband met toegang tot inhoud en bijbehorende gegevens die worden bewaard met het oog op het onderzoek naar en de vervolging van terroristische misdrijven, zoals geregeld in het Unierecht of het nationale recht.

(30) Transparantie van het beleid van aanbieders van hostingdiensten met betrekking tot terroristische inhoud is essentieel om hun verantwoordingsplicht tegenover hun gebruikers en het vertrouwen van burgers in de digitale eengemaakte markt te vergroten. Aanbieders van hostingdiensten die op grond van deze verordening maatregelen hebben genomen of verplicht waren maatregelen te nemen in een bepaald kalenderjaar, moeten jaarlijkse transparantierapporten openbaar maken met informatie over de genomen maatregelen in verband met de identificatie en verwijdering van terroristische inhoud.

(31) De bevoegde autoriteiten moeten jaarlijkse transparantierapporten publiceren met informatie over het aantal verwijderingsbevelen, het aantal zaken waarin een verwijderingsbevel niet werd uitgevoerd, het aantal besluiten betreffende specifieke maatregelen, het aantal zaken dat aan administratieve of gerechtelijke toetsingsprocedures werd onderworpen en het aantal besluiten waarbij sancties werden opgelegd.

(32) Het recht op een doeltreffende voorziening in rechte is vastgelegd in artikel 19 van het Verdrag betreffende de Europese Unie (VEU) en artikel 47 van het Handvest. Elke natuurlijke of rechtspersoon heeft recht op een doeltreffende voorziening in rechte voor de bevoegde nationale rechterlijke instantie tegen overeenkomstig deze verordening genomen maatregelen die de rechten van die persoon kunnen aantasten. Dat recht moet met name de mogelijkheid voor aanbieders van hostingdiensten en aanbieders van inhoud omvatten om verwijderingsbevelen of besluiten die voortvloeien uit de toetsing van verwijderingsbevelen uit hoofde van deze verordening daadwerkelijk te betwisten voor een rechterlijke instantie van de lidstaat waarvan de bevoegde autoriteit het verwijderingsbevel heeft uitgevaardigd of het besluit heeft genomen, en voor aanbieders van hostingdiensten om een besluit betreffende specifieke maatregelen of sancties te betwisten voor een rechterlijke instantie van de lidstaat waarvan de bevoegde autoriteit dat besluit heeft genomen.

(33) Klachtenprocedures vormen een noodzakelijke waarborg tegen de onterechte verwijdering van of de onterechte blokkering van de toegang tot online-inhoud indien die online-inhoud onder de vrijheid van meningsuiting en van informatie valt. Aanbieders van hostingdiensten moeten daarom gebruiksvriendelijke klachtenmechanismen instellen en ervoor zorgen dat klachten snel en met volledige transparantie jegens de aanbieder van inhoud worden behandeld. Het vereiste dat de aanbieder van hostingdiensten inhoud moet herstellen of weer toegankelijk maken wanneer die ten onrechte verwijderd werd of wanneer de toegang daartoe onterecht geblokkeerd werd, moet de mogelijkheid onverlet laten dat de aanbieder van hostingdiensten zijn eigen algemene voorwaarden handhaaft.

(34) Een doeltreffende voorziening in rechte in de zin van artikel 19 VEU en artikel 47 van het Handvest vereist dat aanbieders van inhoud kunnen nagaan om welke redenen de door hen verstrekte inhoud verwijderd is of om welke redenen de toegang tot die inhoud geblokkeerd is. Daartoe moet de aanbieder van hostingdiensten aan de aanbieder van inhoud informatie beschikbaar stellen voor het betwisten van de verwijdering van of de blokkering van de toegang tot die informatie. Afhankelijk van de omstandigheden kunnen aanbieders van hostingdiensten inhoud die verwijderd is of waartoe de toegang geblokkeerd is, vervangen door een bericht dat die inhoud overeenkomstig deze verordening verwijderd werd of dat de toegang tot die inhoud overeenkomstig deze verordening geblokkeerd werd. Op verzoek van de aanbieder van inhoud moet nadere informatie worden verstrekt over de verwijdering van of de blokkering van de toegang tot de inhoud en over de voorzieningen in rechte om de verwijdering of de blokkering van de toegang te betwisten. Wanneer de bevoegde autoriteiten besluiten dat het om redenen van openbare veiligheid, onder meer in het kader van een onderzoek, niet wenselijk is of contraproductief is de aanbieder van inhoud rechtstreeks in kennis te stellen van de verwijdering of de blokkering van de toegang, moeten zij de aanbieder van hostingdiensten daarvan in kennis stellen.

(35) Voor de toepassing van deze verordening moeten de lidstaten bevoegde autoriteiten aanwijzen. Dit hoeft echter niet noodzakelijk te betekenen dat er een nieuwe autoriteit moet worden opgericht, en het moet mogelijk zijn om een bestaande instantie met de in deze verordening voorziene functies te belasten. Deze verordening moet de aanwijzing vereisen van autoriteiten die bevoegd zijn voor het uitvaardigen van verwijderingsbevelen, het toetsen van verwijderingsbevelen, het toezicht houden op specifieke maatregelen en het opleggen van sancties, terwijl het voor elke lidstaat mogelijk moet zijn om zelf te beslissen over het aantal aan te wijzen bevoegde autoriteiten en of het administratieve, rechtshandhavings- of gerechtelijke autoriteiten zijn. De lidstaten moeten ervoor zorgen dat de bevoegde autoriteiten hun taken op objectieve en niet-discriminerende wijze uitvoeren en geen instructies van andere instanties vragen of aanvaarden met betrekking tot de uitoefening van de hun uit hoofde van deze verordening opgedragen taken. Dat mag geen beletsel vormen voor toezicht overeenkomstig het nationale constitutionele recht. De lidstaten moeten de Commissie in kennis stellen van de uit hoofde van deze verordening aangewezen bevoegde autoriteiten, en de Commissie moet online een register van de bevoegde autoriteiten publiceren. Dat onlineregister moet gemakkelijk toegankelijk zijn, zodat de authenticiteit van verwijderingsbevelen snel door de aanbieders van hostingdiensten kan worden nagegaan.

(36) Om dubbel werk en mogelijke inmenging in onderzoeken te vermijden en de lasten voor de getroffen aanbieders van hostingdiensten tot een minimum te beperken, moeten de bevoegde autoriteiten informatie uitwisselen en onderling, en waar passend met Europol, coördineren en samenwerken, voordat verwijderingsbevelen worden uitgevaardigd. Wanneer de bevoegde autoriteit overweegt een verwijderingsbevel uit te vaardigen, moet zij terdege rekening houden met alle kennisgevingen van inmenging die in strijd is met het belang van het onderzoek (conflictoplossing). Wanneer een bevoegde autoriteit door een bevoegde autoriteit van een andere lidstaat op de hoogte wordt gebracht van een bestaand verwijderingsbevel, mag zij geen tweede bevel uitvaardigen dat op hetzelfde onderwerp betrekking heeft. Bij de uitvoering van de bepalingen van deze verordening kan Europol steun verlenen in overeenstemming met zijn huidige mandaat en het bestaande juridisch kader.

(37) Om te garanderen dat door aanbieders van hostingdiensten genomen specifieke maatregelen doeltreffend en voldoende coherent worden uitgevoerd, moeten de bevoegde autoriteiten met elkaar coördineren en samenwerken in verband met de uitwisselingen met aanbieders van hostingdiensten over verwijderingsbevelen en de identificatie, uitvoering en beoordeling van specifieke maatregelen. Coördinatie en samenwerking zijn ook nodig met betrekking tot andere maatregelen ter uitvoering van deze verordening, ook ten aanzien van de vaststelling van regels inzake sancties en de handhaving van sancties. De Commissie moet een dergelijke coördinatie en samenwerking faciliteren.

(38) Het is essentieel dat de bevoegde autoriteit van de lidstaat die voor het opleggen van sancties verantwoordelijk is, volledig wordt ingelicht over de uitvaardiging van verwijderingsbevelen en van de daaropvolgende uitwisselingen tussen de aanbieder van hostingdiensten en de bevoegde autoriteiten in andere lidstaten. Daartoe moeten de lidstaten zorgen voor geschikte en veilige communicatiekanalen en -mechanismen om relevante informatie tijdig te kunnen delen.

(39) Om snelle uitwisselingen tussen de bevoegde autoriteiten en met aanbieders van hostingdiensten te faciliteren, en om dubbel werk te voorkomen, moeten de lidstaten aangemoedigd worden om gebruik te maken van de specifieke instrumenten die door Europol zijn ontwikkeld, zoals de huidige toepassing voor het beheer van de melding van internetuitingen of de opvolgers daarvan.

(40) Meldingen door de lidstaten en Europol zijn een doeltreffend en snel middel gebleken om aanbieders van hostingdiensten bewuster te maken van specifieke inhoud die via hun diensten beschikbaar is en hen in staat te stellen snel actie te ondernemen. Dergelijke meldingen, die een mechanisme zijn om aanbieders van hostingdiensten te waarschuwen voor informatie die als terroristische inhoud kan worden beschouwd, opdat de aanbieder vrijwillig nagaat of die inhoud verenigbaar is met zijn eigen algemene voorwaarden, moeten beschikbaar blijven naast de verwijderingsbevelen. Het blijft de aanbieder van hostingdiensten die uiteindelijk besluit of hij informatie verwijdert omdat die onverenigbaar is met zijn algemene voorwaarden. Deze verordening mag geen invloed hebben op het mandaat van Europol overeenkomstig Verordening (EU) 2016/7941 van het Europees Parlement en de Raad ([11]). Derhalve mag niets in deze verordening worden uitgelegd als een beletsel voor de lidstaten en Europol om meldingen te gebruiken als instrument om terroristische online-inhoud tegen te gaan.

(41) Gezien de bijzonder ernstige gevolgen van bepaalde terroristische online-inhoud moeten aanbieders van hostingdiensten de relevante autoriteiten in de betrokken lidstaat of de bevoegde autoriteiten van de lidstaat waar zij gevestigd zijn of waar zij een wettelijke vertegenwoordiger hebben, snel in kennis stellen van terroristische inhoud die informatie bevat die betrekking heeft op een onmiddellijk levensbedreigend gevaar of een vermoedelijk terroristisch misdrijf. Met het oog op de proportionaliteit moet die verplichting beperkt zijn tot terroristische misdrijven als omschreven in artikel 3, lid 1, van Richtlijn (EU) 2017/541. Die informatieverplichting mag niet betekenen dat aanbieders van hostingdiensten verplicht zijn actief te zoeken naar bewijzen van dergelijk onmiddellijk levensbedreigend gevaar of een dergelijk vermoedelijk terroristisch misdrijf. De betrokken lidstaat moet begrepen worden als de lidstaat die rechtsmacht heeft voor het onderzoek naar en de vervolging van die terroristische misdrijven op grond van de nationaliteit van de dader of van het potentiële slachtoffer van het misdrijf of op grond van de beoogde plaats van de terroristische daad. In geval van twijfel moeten aanbieders van hostingdiensten de informatie doorgeven aan Europol, die daaraan het gepaste gevolg moet geven overeenkomstig zijn mandaat, inclusief het doorzenden van die informatie aan de relevante nationale autoriteiten. De bevoegde autoriteiten van de lidstaten moeten die informatie kunnen gebruiken om onderzoeksmaatregelen te nemen waarin het Unierecht of het nationale recht voorziet.

([11]) Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad (PB L 135 van 24.5.2016, blz. 53).

(42) De aanbieders van hostingdiensten moeten contactpunten aanwijzen of oprichten om de snelle behandeling van verwijderingsbevelen te faciliteren. Het contactpunt mag enkel voor operationele doeleinden dienen. Het contactpunt moet bestaan uit ongeacht welke, interne of uitbestede, specifieke middelen waarmee verwijderingsbevelen elektronisch kunnen worden ingediend en uit de technische of personele middelen om die snel te kunnen verwerken. Het contactpunt hoeft niet in de Unie te zijn gevestigd. De aanbieder van hostingdiensten moet vrij zijn om gebruik te maken van een bestaand contactpunt, op voorwaarde dat het contactpunt de in deze verordening vastgestelde functies kan uitoefenen. Om ervoor te zorgen dat terroristische inhoud binnen een uur na ontvangst van een verwijderingsbevel verwijderd wordt of dat de toegang daartoe binnen een uur na ontvangst van een verwijderingsbevel geblokkeerd wordt, moeten de contactpunten van aanbieders van hostingdiensten die aan terroristische inhoud worden blootgesteld, te allen tijde bereikbaar zijn. De informatie over het contactpunt moet onder meer aangeven in welke taal het contactpunt kan worden aangesproken. Om de communicatie tussen de aanbieders van hostingdiensten en de bevoegde autoriteiten te faciliteren, worden aanbieders van hostingdiensten aangemoedigd om communicatie mogelijk te maken in een van de officiële talen van de instellingen van de Unie waarin hun algemene voorwaarden beschikbaar zijn.

(43) Aangezien er geen algemene verplichting geldt voor aanbieders van hostingdiensten om een fysieke aanwezigheid op het grondgebied van de Unie te garanderen, moet duidelijkheid worden verschaft over de vraag welke lidstaat rechtsmacht heeft voor de aanbieder van hostingdiensten die diensten in de Unie verricht. Als algemene regel geldt dat de aanbieder van hostingdiensten onder de rechtsmacht valt van de lidstaat waar hij zijn hoofdvestiging heeft of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft. Dat mag geen afbreuk doen aan de bevoegdheidsregels die zijn vastgesteld met het oog op verwijderingsbevelen en besluiten die voortvloeien uit de toetsing van verwijderingsbevelen uit hoofde van deze verordening. Ten aanzien van een aanbieder van hostingdiensten die geen vestiging in de Unie heeft en geen wettelijke vertegenwoordiger aanwijst, moet elke lidstaat niettemin rechtsmacht hebben en bijgevolg sancties kunnen opleggen, mits het *ne bis in idem*-beginsel wordt geëerbiedigd.

(44) Aanbieders van hostingdiensten die niet in de Unie zijn gevestigd, moeten schriftelijk een wettelijke vertegenwoordiger aanwijzen om de naleving en handhaving van de verplichtingen uit hoofde van deze verordening te garanderen. Het moet voor aanbieders van hostingdiensten mogelijk zijn om voor de toepassing van deze verordening een wettelijke vertegenwoordiger aan te wijzen die al voor andere doeleinden werd aangewezen, op voorwaarde dat die wettelijke vertegenwoordiger in staat is de in deze verordening voorziene taken uit te oefenen. De wettelijke vertegenwoordiger moet wettelijk bevoegd zijn om namens de aanbieder van hostingdiensten te handelen.

(45) Sancties zijn noodzakelijk om de effectieve uitvoering van deze verordening door aanbieders van hostingdiensten te garanderen. De lidstaten moeten regels inzake sancties, die zowel van administratieve als van strafrechtelijke aard kunnen zijn, vaststellen, alsook, waar passend, richtsnoeren voor het opleggen van geldboeten. Niet-naleving in individuele gevallen kan met eerbiediging van het *ne bis in idem*-beginsel en het proportionaliteitsbeginsel worden bestraft, waarbij de sancties rekening houden met systematisch verzuim. Sancties kunnen verschillende vormen aannemen, waaronder formele waarschuwingen in geval van kleine inbreuken of financiële sancties in verband met zwaardere of systematische inbreuken. Bijzonder zware sancties moeten worden opgelegd ingeval de aanbieder van hostingdiensten systematisch of aanhoudend verzuimt terroristische inhoud binnen één uur na ontvangst van een verwijderingsbevel te verwijderen of de toegang daartoe binnen één uur na ontvangst van een verwijderingsbevel te blokkeren. Met het oog op de rechtszekerheid moet in deze verordening worden bepaald welke inbreuken onderhevig zijn aan sancties en welke omstandigheden relevant zijn om het type en de omvang van die sancties in te schatten. Bij het bepalen of er financiële sancties moeten worden opgelegd, moet terdege rekening worden gehouden met de financiële draagkracht van de aanbieder van hostingdiensten. Bovendien moet de bevoegde autoriteit rekening houden met de vraag of de aanbieder van hostingdiensten een startende onderneming of een kleine, middelgrote of micro-onderneming is zoals omschreven in Aanbeveling 2003/361/EG van de Commissie ([12]). Er moet rekening worden gehouden met nog andere omstandigheden, zoals de vraag of het gedrag van de aanbieder van hostingdiensten objectief onvoorzichtig of laakbaar was, en of de inbreuk uit onachtzaamheid of opzettelijk werd gepleegd. De lidstaten moeten ervoor zorgen dat sancties die opgelegd worden voor inbreuken op deze verordening, niet in de hand werken dat materiaal dat geen terroristische inhoud uitmaakt, verwijderd wordt.

(46) Het gebruik van gestandaardiseerde modellen faciliteert samenwerking en de uitwisseling van informatie tussen bevoegde autoriteiten en aanbieders van hostingdiensten, doordat zij sneller en doeltreffender kunnen communiceren. Het is van bijzonder belang dat na de ontvangst van een verwijderingsbevel snel wordt opgetreden. Modellen verminderen de vertaalkosten en dragen bij aan een hogere standaard van het proces. Feedbackmodellen maken een gestandaardiseerde uitwisseling van informatie mogelijk en zijn bijzonder belangrijk als aanbieders van hostingdiensten niet aan een verwijderingsbevel kunnen voldoen. Gecertificeerde indieningskanalen kunnen de authenticiteit van het verwijderingsbevel garanderen, met inbegrip van de datum en het tijdstip van verzending en ontvangst van het bevel.

([12]) Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

(47) Teneinde de inhoud van de modellen die voor de toepassing van deze verordening moeten worden gebruikt, zo nodig snel te kunnen wijzigen, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie handelingen vast te stellen ten aanzien van de wijziging van de bijlagen bij deze verordening. Om rekening te kunnen houden met technologische ontwikkelingen en de ontwikkeling van het juridisch kader ter zake, moet de Commissie ook de bevoegdheid krijgen om gedelegeerde handelingen vast te stellen tot aanvulling van deze verordening met technische voorschriften voor de elektronische middelen die de bevoegde autoriteiten moeten gebruiken voor de verzending van verwijderingsbevelen. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen geschieden in overeenstemming met de beginselen van het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven ([13]). Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(48) De lidstaten moeten informatie verzamelen over de uitvoering van deze verordening. Het moet mogelijk zijn voor de lidstaten om gebruik te maken van de transparantierapporten van aanbieders van hostingdiensten en die zo nodig aanvullen met meer gedetailleerde informatie, zoals hun eigen transparantierapporten op grond van deze verordening. Er moet een gedetailleerd programma voor de monitoring van de outputs, resultaten en effecten van deze verordening worden vastgesteld, zodat die in een evaluatie van de uitvoering van deze verordening kunnen worden meegenomen.

(49) Op basis van de bevindingen en conclusies in het uitvoeringsverslag en de uitkomst van de monitoringexercitie moet de Commissie uiterlijk drie jaar na de datum van inwerkingtreding van deze verordening een evaluatie ervan uitvoeren. De evaluatie moet gebaseerd zijn op de volgende criteria: doelmatigheid, noodzakelijkheid, doeltreffendheid, proportionaliteit, relevantie, samenhang en Unie-meerwaarde. De evaluatie moet een beoordeling maken van de werking van de verschillende operationele en technische maatregelen waarin de verordening voorziet, met inbegrip van de effectiviteit van de maatregelen om de opsporing, identificatie en verwijdering van terroristische online-inhoud te verbeteren, de doeltreffendheid van de waarborgmechanismen alsook de gevolgen voor eventueel geschonden grondrechten, zoals de vrijheid van meningsuiting en van informatie, met inbegrip van de vrijheid en het pluralisme van de media, de vrijheid van ondernemerschap, het recht op privacy en de bescherming van persoonsgegevens. Bovendien moet de Commissie de gevolgen voor mogelijk geschade belangen van derden beoordelen.

(50) Daar de doelstelling van deze verordening, namelijk het garanderen van de goede werking van de digitale eengemaakte markt door de verspreiding van terroristische online-inhoud tegen te gaan, niet voldoende door de lidstaten kan worden verwezenlijkt, maar vanwege de omvang en de gevolgen ervan beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 VEU neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om die doelstelling te verwezenlijken,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

AFDELING I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

1. Deze verordening stelt uniforme regels vast om het misbruik van hostingdiensten voor de verspreiding onder het publiek van terroristische online-inhoud tegen te gaan, met name inzake:

(a) redelijke en evenredige zorgplichten die door aanbieders van hostingdiensten moeten worden nagekomen om de verspreiding onder het publiek van terroristische inhoud via hun diensten tegen te gaan en, zo nodig, de snelle verwijdering van of de snelle blokkering van de toegang tot dergelijke inhoud te garanderen;

([13]) PB L 123 van 12.5.2016, blz. 1.

(b) de maatregelen die de lidstaten moeten invoeren, overeenkomstig het Unierecht en met passende waarborgen ter bescherming van de grondrechten, met name de vrijheid van meningsuiting en van informatie in een open en democratische samenleving, teneinde:

i) terroristische inhoud te identificeren en de snelle verwijdering ervan door aanbieders van hostingdiensten te garanderen, en

ii) de samenwerking tussen de bevoegde autoriteiten van de lidstaten, aanbieders van hostingdiensten en, waar passend, Europol, te faciliteren.

2. Deze verordening is van toepassing op aanbieders van hostingdiensten die, ongeacht de plaats van hun hoofdvestiging, in de Unie diensten aanbieden, voor zover zij informatie onder het publiek verspreiden.

3. Materiaal dat voor educatieve, journalistieke, artistieke of onderzoeksdoeleinden of met het oog op het voorkomen of bestrijden van terrorisme onder het publiek wordt verspreid, met inbegrip van materiaal dat een uiting vormt van polemische of controversiële standpunten in het publieke debat, wordt niet geacht terroristische inhoud te zijn. Met een beoordeling wordt het werkelijke doel van die verspreiding bepaald en wordt nagegaan of het materiaal voor die doeleinden onder het publiek wordt verspreid.

4. Deze verordening heeft niet tot gevolg dat de verplichting tot eerbiediging van de in artikel 6 VEU bedoelde rechten, vrijheden en beginselen wordt gewijzigd en doet geen afbreuk aan de fundamentele beginselen inzake de vrijheid van meningsuiting en van informatie, met inbegrip van de vrijheid en het pluralisme van de media.

5. Deze verordening doet geen afbreuk aan Richtlijnen 2000/31/EG en 2010/13/EU. Voor audiovisuele mediadiensten in de zin van artikel 1, lid 1, punt a) van Richtlijn 2010/13/EU heeft Richtlijn 2010/13/EU voorrang.

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1. "aanbieder van hostingdiensten": een aanbieder van diensten als gedefinieerd in artikel 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad ([14]) die erin bestaan informatie die door een aanbieder van inhoud is verstrekt, op diens verzoek op te slaan;

2. "aanbieder van inhoud": een gebruiker die informatie heeft verstrekt die door een aanbieder van hostingdiensten opgeslagen en onder het publiek verspreid wordt of werd;

3. "verspreiding onder het publiek": het op verzoek van een aanbieder van inhoud beschikbaar stellen van informatie aan een potentieel onbeperkt aantal personen;

4. "in de Unie diensten aanbieden": natuurlijke personen of rechtspersonen in een of meer lidstaten in staat stellen gebruik te maken van de diensten van een aanbieder van hostingdiensten die een wezenlijke band heeft met die lidstaat of lidstaten;

5. "wezenlijke band": de band die een aanbieder van hostingdiensten heeft met een of meer lidstaten die ofwel voortvloeit uit diens vestiging in de Unie, ofwel uit specifieke feitelijke criteria, zoals:

a) het hebben van een aanzienlijk aantal gebruikers van zijn diensten in een of meer lidstaten, of

b) het richten van zijn activiteiten op een of meer lidstaten;

6. "terroristische misdrijven": misdrijven als gedefinieerd in artikel 3 van Richtlijn (EU) 2017/541;

([14]) Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB L 241 van 17.9.2015, blz.1).

7. "terroristische inhoud": een of meer van de volgende soorten materiaal, namelijk materiaal dat:

a) aanzet tot het plegen van een van de in artikel 3, lid 1, punten a) tot en met i), van Richtlijn (EU) 2017/541 genoemde misdrijven, indien dat materiaal direct of indirect, bijvoorbeeld door terroristische daden te verheerlijken, het plegen van terroristische misdrijven bepleit, waardoor een gevaar ontstaat dat een of meer van die misdrijven mogelijk worden gepleegd;

b) een persoon of een groep personen aanspoort om een van de in artikel 3, lid 1, punten a) tot en met i), van Richtlijn (EU) 2017/541 genoemde misdrijven te plegen of daaraan een bijdrage te leveren;

c) een persoon of een groep personen aanspoort om deel te nemen aan de activiteiten van een terroristische groepering, in de zin van artikel 4, punt b), van Richtlijn (EU) 2017/541;

d) instructies biedt voor het vervaardigen of gebruiken van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, of voor andere specifieke methoden of technieken, met als doel een van de in artikel 3, lid 1, punten a) tot en met i), van Richtlijn (EU) 2017/541 bedoelde terroristische misdrijven te plegen of daaraan een bijdrage te leveren;

e) een dreiging vormt om een van de in artikel 3, lid 1, punten a) tot en met i), van Richtlijn (EU) 2017/541 bedoelde misdrijven te plegen;

8. "algemene voorwaarden": alle algemene voorwaarden en clausules, ongeacht hun naam of vorm, waarin de contractuele betrekking tussen een aanbieder van hostingdiensten en zijn gebruikers wordt geregeld;

9. "hoofdvestiging": het hoofdkantoor of de statutaire zetel van de aanbieder van hostingdiensten waar de voornaamste financiële functies en de operationele zeggenschap worden uitgeoefend.

AFDELING II

MAATREGELEN OM DE VERSPREIDING VAN TERRORISTISCHE ONLINE-INHOUD TEGEN TE GAAN

Artikel 3

Verwijderingsbevelen

1. De bevoegde autoriteit van elke lidstaat heeft de bevoegdheid om een verwijderingsbevel uit te vaardigen op grond waarvan aanbieders van hostingdiensten terroristische inhoud moeten verwijderen of de toegang daartoe in alle lidstaten moeten blokkeren.

2. Indien een bevoegde autoriteit nog niet eerder een verwijderingsbevel heeft uitgevaardigd aan een aanbieder van hostingdiensten, verstrekt zij ten minste twaalf uur voor de uitvaardiging van het verwijderingsbevel informatie aan die aanbieder van hostingdiensten over de toepasselijke procedures en termijnen.

De eerste alinea is niet van toepassing op terdege gemotiveerde noodgevallen.

3. Aanbieders van hostingdiensten verwijderen terroristische inhoud zo spoedig mogelijk en in elk geval binnen één uur na ontvangst van het verwijderingsbevel, of ze blokkeren zo spoedig mogelijk en in elk geval binnen één uur na ontvangst van het verwijderingsbevel de toegang daartoe in alle lidstaten.

4. De bevoegde autoriteiten vaardigen verwijderingsbevelen uit aan de hand van het model in bijlage I. Verwijderingsbevelen bevatten de volgende elementen:

a) de identificatiegegevens van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt en de authenticatie van het verwijderingsbevel door die bevoegde autoriteit;

b) een voldoende gedetailleerde motivering waarom de inhoud als terroristische inhoud wordt beschouwd en een verwijzing naar het relevante soort materiaal als bedoeld in artikel 2, punt 7);

c) een exacte uniform resource locator (URL-adres) en, zo nodig, aanvullende informatie om de terroristische inhoud te kunnen identificeren;

d) een verwijzing naar deze verordening als de rechtsgrondslag voor het verwijderingsbevel;

e) datum, tijdstempel en elektronische handtekening van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt;

f) eenvoudig te begrijpen informatie over de rechtsmiddelen waarover de aanbieder van hostingdiensten en de aanbieder van inhoud beschikken, met inbegrip van informatie over rechtsmiddelen bij de bevoegde autoriteit en over beroep bij een rechterlijke instantie, alsook over de termijnen voor het instellen van een hoger beroep;

g) indien noodzakelijk en evenredig, het besluit om geen informatie openbaar te maken over de verwijdering van of de blokkering van de toegang tot terroristische inhoud overeenkomstig artikel 11, lid 3.

5. De bevoegde autoriteit verstuurt het verwijderingsbevel naar de hoofdvestiging van de aanbieder van hostingdiensten of naar zijn overeenkomstig artikel 17 aangewezen wettelijke vertegenwoordiger.

Die bevoegde autoriteit stuurt het verwijderingsbevel aan het in artikel 15, lid 1, bedoelde contactpunt door met gebruikmaking, van elektronische middelen die een schriftelijk bewijs kunnen genereren op zodanige wijze dat authenticatie van de afzender mogelijk wordt, met inbegrip van de juistheid van de datum en het tijdstip van verzending en ontvangst van het bevel.

6. De aanbieder van hostingdiensten stelt de bevoegde autoriteit aan de hand van het model in bijlage II zonder onnodige vertraging in kennis van de verwijdering van de terroristische inhoud of van de blokkering in alle lidstaten van de toegang tot de terroristische inhoud, met vermelding van met name het tijdstip van die verwijdering of blokkering.

7. Als de aanbieder van hostingdiensten het verwijderingsbevel niet kan naleven vanwege overmacht of feitelijke onmogelijkheid die hem niet kan worden toegerekend, waaronder objectief te rechtvaardigen technische of operationele redenen, stelt hij de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd daar zonder onnodige vertraging van in kennis aan de hand van het model in bijlage III.

De in lid 3 vastgestelde termijn vangt aan zodra de in de eerste alinea van dit lid aangevoerde redenen niet langer bestaan.

8. Indien de aanbieder van hostingdiensten het verwijderingsbevel niet kan naleven omdat het kennelijke fouten bevat of niet voldoende informatie bevat om het uit te voeren, stelt hij de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd daar zonder onnodige vertraging van in kennis en vraagt hij de nodige verduidelijking aan de hand van het model in bijlage III.

De in lid 3 vastgestelde termijn vangt aan zodra de aanbieder van hostingdiensten de nodige verduidelijking heeft ontvangen.

9. Een verwijderingsbevel wordt definitief bij het verstrijken van de termijn voor het instellen van een hoger beroep indien geen hoger beroep is ingesteld overeenkomstig het nationaal recht, of wanneer het na een hoger beroep is bevestigd.

Wanneer het verwijderingsbevel definitief wordt, stelt de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd, de in artikel 12, lid 1, punt c), bedoelde bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, daarvan in kennis.

Artikel 4

Procedure voor grensoverschrijdende verwijderingsbevelen

1. Met inachtneming van artikel 3 dient de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd, indien de aanbieder van hostingdiensten geen hoofdvestiging of wettelijke vertegenwoordiger heeft in de lidstaat van die bevoegde autoriteit, tegelijkertijd een afschrift van het verwijderingsbevel in bij de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft.

2. Indien een aanbieder van hostingdiensten een in dit artikel bedoeld verwijderingsbevel ontvangt, neemt hij de in artikel 3 vastgestelde maatregelen en neemt hij overeenkomstig lid 7 van dit artikel de nodige maatregelen om de inhoud te kunnen herstellen of weer toegankelijk te kunnen maken.

3. De bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, kan op eigen initiatief binnen 72 uur na ontvangst van het verwijderingsbevel overeenkomstig lid 1, het verwijderingsbevel toetsen om te bepalen of het een ernstige of kennelijke inbreuk op deze verordening of op de grondrechten en vrijheden zoals verankerd in het Handvest inhoudt.

Indien zij vaststelt dat er sprake is van een inbreuk, neemt zij daartoe binnen diezelfde periode een met redenen omkleed besluit.

4. Aanbieders van hostingdiensten en aanbieders van inhoud hebben het recht om binnen 48 uur na ontvangst van respectievelijk een verwijderingsbevel of informatie op grond van artikel 11, lid 2, een met redenen omkleed verzoek in te dienen bij de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, om het verwijderingsbevel te toetsen zoals bedoeld in de eerste alinea van lid 3 van dit artikel.

Binnen 72 uur na ontvangst van het verzoek neemt de bevoegde autoriteit, nadat zij het verwijderingsbevel heeft getoetst, een met redenen omkleed besluit waarin zij uiteenzet of er al dan niet sprake is van een inbreuk.

5. Alvorens een besluit te nemen op grond van lid 3, tweede alinea, of een besluit waarbij een inbreuk wordt vastgesteld te nemen op grond van lid 4, tweede alinea, stelt de bevoegde autoriteit de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd in kennis van haar voornemen om het besluit te nemen en van de redenen daartoe.

6. Indien de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, overeenkomstig lid 3 of lid 4 van dit artikel een met redenen omkleed besluit neemt, deelt zij dat besluit onverwijld mee aan de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd, aan de aanbieder van hostingdiensten, aan de aanbieder van inhoud die om de in lid 4 van dit artikel bedoelde toetsing heeft verzocht, en, overeenkomstig artikel 14, aan Europol. Indien bij het besluit een inbreuk op grond van lid 3 of lid 4 van dit artikel wordt vastgesteld, heeft het verwijderingsbevel geen rechtsgevolgen meer.

7. Zodra hij een besluit ontvangt waarbij een inbreuk werd vastgesteld en dat overeenkomstig lid 6 aan hem werd meegedeeld, herstelt de betrokken aanbieder van hostingdiensten de inhoud of maakt hij die weer toegankelijk, onverminderd de mogelijkheid om zijn algemene voorwaarden te handhaven overeenkomstig het Unierecht en het nationale recht.

Artikel 5

Specifieke maatregelen

1. Een aanbieder van hostingdiensten die aan terroristische inhoud als bedoeld in lid 4 is blootgesteld, neemt, voor zover van toepassing, in zijn algemene voorwaarden bepalingen op om het misbruik van zijn diensten voor de verspreiding van terroristische inhoud onder het publiek tegen te gaan, en hij past die bepalingen toe.

Dit doet hij op zorgvuldige, evenredige en niet-discriminerende wijze, met inachtneming onder alle omstandigheden van de grondrechten van de gebruikers, en met name rekening houdend met het fundamentele belang van de vrijheid van meningsuiting en van informatie in een open en democratische samenleving, teneinde te voorkomen dat materiaal dat geen terroristische inhoud uitmaakt, wordt verwijderd.

2. Een aanbieder van hostingdiensten die aan terroristische inhoud is blootgesteld als bedoeld in lid 4, neemt specifieke maatregelen om zijn diensten te beschermen tegen de verspreiding van terroristische inhoud onder het publiek.

Het besluit over de keuze van de specifieke maatregelen blijft bij de aanbieder van hostingdiensten berusten. Die specifieke maatregelen kunnen een of meer van de volgende maatregelen omvatten:

a) passende technische en operationele maatregelen of capaciteiten, zoals passende personele of technische middelen voor het identificeren en snel verwijderen van of snel blokkeren van de toegang tot terroristische inhoud;

b) gemakkelijk toegankelijke en gebruiksvriendelijke mechanismen waarmee gebruikers vermoedelijke terroristische inhoud bij de aanbieder van hostingdiensten kunnen melden of markeren;

c) andere mechanismen om het bewustzijn rond terroristische inhoud op zijn diensten te vergroten, zoals mechanismen voor gebruikersmoderatie;

d) alle andere maatregelen die de aanbieder van hostingdiensten passend acht om de beschikbaarheid van terroristische inhoud op zijn diensten tegen te gaan.

3. Specifieke maatregelen voldoen aan alle volgende vereisten:

a) zij zijn doeltreffend om de mate van blootstelling van de diensten van de aanbieder van hostingdiensten aan terroristische inhoud te beperken;

b) zij zijn doelgericht en evenredig, waarbij met name rekening wordt gehouden met de ernst van de blootstelling van de diensten van de aanbieder van hostingdiensten aan terroristische inhoud, de technische en operationele capaciteiten, de financiële draagkracht, het aantal gebruikers van de diensten van de aanbieder van hostingdiensten en de hoeveelheid inhoud die zij leveren;

c) zij worden toegepast op een manier die de rechten en rechtmatige belangen van de gebruikers ten volle in acht neemt, met name de grondrechten van de gebruikers inzake de vrijheid van meningsuiting en van informatie, de eerbiediging van het privéleven en de bescherming van persoonsgegevens;

d) zij worden op zorgvuldige en niet-discriminerende wijze toegepast.

Indien er bij de specifieke maatregelen technische maatregelen aan te pas komen, worden passende en doeltreffende waarborgen geboden, met name door te voorzien in toezicht en verificatie door mensen, om nauwkeurigheid te waarborgen en te voorkomen dat materiaal dat geen terroristische inhoud uitmaakt, wordt verwijderd.

4. Een aanbieder van hostingdiensten is aan terroristische inhoud blootgesteld, indien de bevoegde autoriteit van de lidstaat waar hij zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft:

a) op basis van objectieve factoren zoals het feit dat de aanbieder van hostingdiensten in de voorafgaande twaalf maanden twee of meer definitieve verwijderingsbevelen heeft ontvangen, een besluit heeft genomen waarbij is vastgesteld dat de aanbieder van hostingdiensten aan terroristische inhoud is blootgesteld, en

b) het in punt a) bedoelde besluit aan de aanbieder van hostingdiensten heeft meegedeeld.

5. Na een in lid 4 of, in voorkomend geval, in lid 6 bedoeld besluit ontvangen te hebben, brengt een aanbieder van hostingdiensten aan de bevoegde autoriteit verslag uit over de specifieke maatregelen die hij heeft genomen en voornemens is te nemen om aan de leden 2 en 3 te voldoen. Hij doet dit binnen drie maanden na ontvangst van het besluit en vervolgens op jaarbasis. Die verplichting vervalt zodra de bevoegde autoriteit, na een verzoek op grond van lid 7, heeft besloten dat de aanbieder van hostingdiensten niet langer aan terroristische inhoud is blootgesteld.

6. Indien de bevoegde autoriteit op basis van de in lid 5 bedoelde verslagen en, in voorkomend geval, andere objectieve factoren van oordeel is dat de genomen specifieke maatregelen niet voldoen aan de leden 2 en 3, richt die bevoegde autoriteit een besluit tot de aanbieder van hostingdiensten dat hem ertoe verplicht de nodige maatregelen te nemen om ervoor te zorgen dat aan de leden 2 en 3 wordt voldaan.

De aanbieder van hostingdiensten mag het type te nemen specifieke maatregelen kiezen.

7. Een aanbieder van hostingdiensten kan de bevoegde autoriteit te allen tijde verzoeken om herziening en, waar passend, wijziging of intrekking van een in lid 4 of lid 6 bedoeld besluit.

Binnen drie maanden na ontvangst van het verzoek neemt de bevoegde autoriteit op basis van objectieve factoren een met redenen omkleed besluit over het verzoek en stelt zij de aanbieder van hostingdiensten daarvan in kennis.

8. De verplichting tot het nemen van specifieke maatregelen doet geen afbreuk aan artikel 15, lid 1, van Richtlijn 2000/31/EG en houdt voor aanbieders van hostingdiensten noch een algemene verplichting in om toezicht te houden op de informatie die zij doorsturen of opslaan, noch een algemene verplichting om actief te zoeken naar feiten of omstandigheden die op illegale activiteiten duiden.

De verplichting tot het nemen van specifieke maatregelen omvat geen verplichting voor de aanbieder van hostingdiensten om automatische instrumenten te gebruiken.

Artikel 6

Bewaring van inhoud en bijbehorende gegevens

1. Aanbieders van hostingdiensten bewaren terroristische inhoud die is verwijderd of waartoe de toegang is geblokkeerd ten gevolge van een verwijderingsbevel of van specifieke maatregelen op grond van artikel 3 of 5, alsmede de bijbehorende gegevens die ten gevolge van de verwijdering van dergelijke terroristische inhoud zijn verwijderd, welke nodig zijn voor:

a) administratieve of gerechtelijke toetsingsprocedures of klachtenbehandeling uit hoofde van artikel 10 tegen een besluit om terroristische inhoud en gerelateerde gegevens te verwijderen of de toegang daartoe te blokkeren, of

b) het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven.

2. De in lid 1 bedoelde terroristische inhoud en de bijbehorende gegevens worden gedurende zes maanden na de verwijdering of de blokkering van de toegang bewaard. De terroristische inhoud wordt, op verzoek van de bevoegde autoriteit of rechterlijke instantie, gedurende een nader bepaalde periode bewaard indien en zolang zulks nodig is voor lopende administratieve of gerechtelijke toetsingsprocedures als bedoeld in lid 1, punt a).

3. Aanbieders van hostingdiensten zorgen ervoor dat voor op grond van lid 1 bewaarde terroristische inhoud en de bijbehorende gegevens passende technische en organisatorische waarborgen gelden.

Die technische en organisatorische waarborgen zorgen ervoor dat de bewaarde terroristische inhoud en de bijbehorende gegevens uitsluitend voor de in lid 1 genoemde doeleinden worden gebruikt en verwerkt, en voorzien in een hoog niveau van beveiliging van de betrokken persoonsgegevens. Aanbieders van hostingdiensten evalueren die waarborgen en actualiseren deze indien nodig.

AFDELING III

WAARBORGEN EN VERANTWOORDINGSPLICHT

Artikel 7

Transparantieverplichtingen voor aanbieders van hostingdiensten

1. Aanbieders van hostingdiensten stellen in hun algemene voorwaarden duidelijk hun beleid voor het tegengaan van de verspreiding van terroristische inhoud vast, met inbegrip van, waar passend, een omstandige toelichting van de werking van specifieke maatregelen, waaronder, indien van toepassing, het gebruik van automatische instrumenten.

2. Een aanbieder van hostingdiensten die op grond van deze verordening in een bepaald kalenderjaar maatregelen heeft genomen of heeft moeten nemen om de verspreiding van terroristische inhoud tegen te gaan, maakt een transparantieverslag openbaar over de maatregelen die in die periode zijn genomen. Hij publiceert dat verslag vóór 1 maart van het volgende jaar.

3. Transparantieverslagen bevatten ten minste de volgende informatie:

a) informatie over de maatregelen die de aanbieder van hostingdiensten heeft genomen met betrekking tot de identificatie en verwijdering van of blokkering van de toegang tot terroristische inhoud;

b) informatie over de maatregelen die de aanbieder van hostingdiensten heeft genomen om te voorkomen dat materiaal dat eerder is verwijderd of waartoe de toegang eerder werd geblokkeerd omdat het als terroristische inhoud werd beschouwd, opnieuw online verschijnt, met name in gevallen waarin automatische instrumenten zijn gebruikt;

c) het aantal items met terroristische inhoud die verwijderd zijn of waartoe de toegang geblokkeerd is naar aanleiding van verwijderingsbevelen of specifieke maatregelen, en het aantal verwijderingsbevelen waarbij de inhoud op grond van artikel 3, lid 7, eerste alinea, en artikel 3, lid 8, eerste alinea, niet verwijderd is of waartoe de toegang niet geblokkeerd is, alsook de redenen daarvoor;

d) het aantal en het resultaat van de klachten die de aanbieder van hostingdiensten overeenkomstig artikel 10 heeft behandeld;

e) het aantal en het resultaat van de administratieve of gerechtelijke toetsingsprocedures die de aanbieder van hostingdiensten heeft ingesteld;

f) het aantal gevallen waarin de aanbieder van hostingdiensten inhoud moest herstellen of weer toegankelijk moest maken als gevolg van een administratieve of gerechtelijke toetsing;

g) het aantal gevallen waarin de aanbieder van hostingdiensten inhoud hersteld of weer toegankelijk gemaakt heeft na een klacht van de aanbieder van inhoud.

Artikel 8

Transparantieverslagen van bevoegde autoriteiten

1. De bevoegde autoriteiten publiceren jaarlijkse transparantieverslagen over hun activiteiten in het kader van deze verordening. Die verslagen bevatten ten minste de volgende informatie over het betrokken kalenderjaar:

a) het aantal verwijderingsbevelen dat uit hoofde van artikel 3 is uitgevaardigd, waarbij het aantal verwijderingsbevelen die onderworpen zijn aan artikel 4, lid 1, wordt gespecificeerd, het aantal verwijderingsbevelen dat uit hoofde van artikel 4 is getoetst, en informatie over de uitvoering die de betrokken aanbieders van hostingdiensten aan die verwijderingsbevelen hebben gegeven, met inbegrip van het aantal gevallen waarin terroristische inhoud verwijderd werd of de toegang daartoe geblokkeerd werd en het aantal gevallen waarin terroristische inhoud niet verwijderd werd of de toegang daartoe niet geblokkeerd werd;

b) het aantal besluiten die overeenkomstig artikel 5, lid 4, lid 6 of lid 7, zijn genomen en informatie over de uitvoering die aanbieders van hostingdiensten aan die besluiten hebben gegeven, met inbegrip van een beschrijving van de specifieke maatregelen;

c) het aantal gevallen waarin overeenkomstig artikel 5, leden 4 en 6, genomen verwijderingsbevelen en besluiten onderworpen waren aan administratieve of gerechtelijke toetsingsprocedures, en informatie over de uitkomst van de betrokken procedures;

d) het aantal besluiten waarbij op grond van artikel 18 sancties zijn opgelegd, en een beschrijving van het soort opgelegde sanctie.

2. De in lid 1 bedoelde jaarlijkse transparantieverslagen bevatten geen informatie die lopende activiteiten met het oog op de voorkoming, opsporing, onderzoek of vervolging van terroristische misdrijven of nationale veiligheidsbelangen kunnen schaden.

Artikel 9

Voorzieningen in rechte

1. Aanbieders van hostingdiensten die een op grond van artikel 3, lid 1, uitgevaardigd verwijderingsbevel, een besluit op grond van artikel 4, lid 4, of een besluit op grond van artikel 5, lid 4, lid 6 of lid 7, hebben ontvangen, hebben recht op een doeltreffende voorziening in rechte. Dat recht omvat het recht om een dergelijk verwijderingsbevel te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd en het recht om een dergelijk besluit op grond van artikel 4, lid 4 of artikel 5, lid 4, lid 6 of lid 7, te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het besluit heeft genomen.

2. Aanbieders van inhoud die na een verwijderingsbevel verwijderd is of waartoe de toegang na een verwijderingsbevel geblokkeerd is, hebben recht op een doeltreffende voorziening in rechte. Dat recht omvat het recht om een op grond van artikel 3, lid 1, uitgevaardigd verwijderingsbevel te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd en het recht om een besluit op grond van artikel 4, lid 4, te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het besluit heeft genomen.

3. De lidstaten voorzien in doeltreffende procedures voor de uitoefening van de in dit artikel bedoelde rechten.

Artikel 10

Klachtenmechanismen

1. Elke aanbieder van hostingdiensten stelt een doeltreffend en toegankelijk mechanisme in waarmee aanbieders van inhoud die verwijderd is of waartoe de toegang geblokkeerd is ten gevolge van specifieke maatregelen op grond van artikel 5,een klacht betreffende die verwijdering of die blokkering van de toegang kunnen indienen waarbij om het herstel of het weer toegankelijk maken van de inhoud wordt verzocht.

2. Elke aanbieder van hostingdiensten onderzoekt snel alle door hem via het in lid 1 bedoelde mechanisme ontvangen klachten en herstelt de inhoud, of maakt die weer toegankelijk, zonder onnodige vertraging indien de verwijdering daarvan of de blokkering van de toegang daartoe onterecht was. Hij stelt de klager binnen twee weken na ontvangst van de klacht in kennis van het resultaat van de klacht.

Indien de klacht wordt afgewezen, verstrekt de aanbieder van hostingdiensten de redenen daarvoor aan de klager.

Een herstel of weer toegankelijk maken van inhoud sluit niet uit dat er een administratieve of gerechtelijke toetsingsprocedure tot betwisting van het besluit van de aanbieder van hostingdiensten of van de bevoegde autoriteit plaatsvindt.

Artikel 11

Informatie voor aanbieders van inhoud

1. Wanneer een aanbieder van hostingdiensten terroristische inhoud verwijdert of de toegang daartoe blokkeert, stelt hij aan de aanbieder van inhoud informatie beschikbaar over die verwijdering of die blokkering van de toegang.

2. De aanbieder van hostingdiensten stelt de aanbieder van inhoud op diens verzoek ofwel in kennis van de redenen voor de verwijdering of de blokkering van de toegang en van zijn rechten om het verwijderingsbevel te betwisten, ofwel verstrekt hij de aanbieder van inhoud een afschrift van het verwijderingsbevel.

3. De verplichting op grond van de leden 1 en 2 is niet van toepassing indien de bevoegde autoriteit die het verwijderingsbevel uitvaardigt, besluit dat het noodzakelijk en evenredig is om niet in openbaarmaking te voorzien om redenen van openbare veiligheid, zoals het voorkomen, onderzoeken, opsporen en vervolgen van terroristische misdrijven, zolang het nodig is, maar niet langer dan zes weken te rekenen vanaf dat besluit. In dat geval maakt de aanbieder van hostingdiensten geen informatie openbaar over de verwijdering van of de blokkering van de toegang tot terroristische inhoud.

Die bevoegde autoriteit kan die termijn met zes weken verlengen, indien die niet-openbaarmaking nog steeds gerechtvaardigd is.

AFDELING IV

BEVOEGDE AUTORITEITEN EN SAMENWERKING

Artikel 12

Aanwijzing van bevoegde autoriteiten

1. Elke lidstaat wijst de bevoegde autoriteit of autoriteiten aan voor:

a) het uitvaardigen van verwijderingsbevelen op grond van artikel 3;

b) het toetsen van verwijderingsbevelen op grond van artikel 4;

c) het toezien op de uitvoering van specifieke maatregelen op grond van artikel 5;

d) het opleggen van sancties op grond van artikel 18.

2. Elke lidstaat zorgt ervoor dat binnen de in lid 1, punt a), bedoelde bevoegde autoriteit een contactpunt wordt aangewezen of opgericht voor de behandeling van verzoeken om verduidelijking en feedback met betrekking tot de door die bevoegde autoriteit uitgevaardigde verwijderingsbevelen.

De lidstaten zorgen ervoor dat de informatie over het contactpunt openbaar wordt gemaakt.

3. Uiterlijk op 7 juni 2022 stellen de lidstaten de Commissie in kennis van de in lid 1 bedoelde bevoegde autoriteit of autoriteiten, en van alle wijzigingen daarvan. De Commissie maakt de kennisgeving en alle wijzigingen daarvan bekend in het *Publicatieblad van de Europese Unie*.

4. Uiterlijk op 7 juni 2022 zet de Commissie een onlineregister op met de in lid 1 bedoelde bevoegde autoriteiten en voor elke bevoegde autoriteit het op grond van lid 2 aangewezen of opgerichte contactpunt. De Commissie publiceert op regelmatige basis alle wijzigingen daarvan.

Artikel 13

Bevoegde autoriteiten

1. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten over de nodige bevoegdheden en voldoende middelen beschikken om de doelstellingen uit hoofde van deze verordening te verwezenlijken en hun verplichtingen uit hoofde van deze verordening na te komen.

2. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten hun taken uit hoofde van deze verordening op objectieve en niet-discriminerende wijze uitoefenen met volledige eerbiediging van de grondrechten. De bevoegde autoriteiten vragen noch aanvaarden instructies van andere instanties met betrekking tot de uitoefening van hun taken uit hoofde van artikel 12, lid 1.

De eerste alinea vormt geen beletsel voor toezicht overeenkomstig het nationale constitutionele recht.

Artikel 14

Samenwerking tussen aanbieders van hostingdiensten, bevoegde autoriteiten en Europol

1. De bevoegde autoriteiten wisselen informatie uit, coördineren en werken samen met elkaar en, waar passend, met Europol, met betrekking tot verwijderingsbevelen, met name teneinde dubbel werk te voorkomen, de coördinatie te verbeteren en inmenging in onderzoeken in verschillende lidstaten te voorkomen.

2. De bevoegde autoriteiten van de lidstaten wisselen informatie uit, coördineren en werken samen met de in artikel 12, lid 1, punten c) en d), bedoelde bevoegde autoriteiten met betrekking tot op grond van artikel 5 genomen specifieke maatregelen en op grond van artikel 18 opgelegde sancties. De lidstaten zorgen ervoor dat de in artikel 12, lid 1, punten c) en d), bedoelde bevoegde autoriteiten in het bezit zijn van alle relevante informatie.

3. Voor de toepassing van lid 1 voorzien de lidstaten in passende en veilige communicatiekanalen of -mechanismen om ervoor te zorgen dat de relevante informatie tijdig wordt uitgewisseld.

4. Met het oog op de effectieve uitvoering van deze verordening en de voorkoming van dubbel werk kunnen de lidstaten en de aanbieders van hostingdiensten gebruikmaken van speciale instrumenten, met inbegrip van instrumenten die zijn ingesteld door Europol, om met name het volgende te faciliteren:

a) de verwerking van en de feedback over verwijderingsbevelen op grond van artikel 3, en

b) de samenwerking met het oog op het bepalen en uitvoeren van specifieke maatregelen op grond van artikel 5.

5. Indien aanbieders van hostingdiensten kennis krijgen van terroristische inhoud die een onmiddellijk levensbedreigend gevaar inhoudt, lichten zij snel de autoriteiten in die in de betrokken lidstaten bevoegd zijn voor het onderzoek en de vervolging van strafbare feiten. Indien het onmogelijk is de betrokken lidstaten te bepalen, stellen de aanbieders van hostingdiensten het contactpunt op grond van artikel 12, lid 2, in de lidstaat waar zij hun hoofdvestiging hebben of waar hun wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, daarvan in kennis en geven zij de informatie over die terroristische inhoud door aan Europol met het oog op passende follow-up.

6. De bevoegde autoriteiten worden aangemoedigd afschriften van de verwijderingsbevelen toe te zenden aan Europol, opdat Europol een jaarverslag kan opstellen met een analyse van de soorten terroristische inhoud waarvoor verwijderingsbevelen op grond van deze verordening zijn uitgevaardigd.

Artikel 15

Contactpunten van aanbieders van hostingdiensten

1. Elke aanbieder van hostingdiensten wijst een contactpunt aan of richt een contactpunt op voor de ontvangst van verwijderingsbevelen met elektronische middelen en de snelle behandeling ervan op grond van de artikelen 3 en 4. De aanbieder van hostingdiensten zorgt ervoor dat de informatie over het contactpunt openbaar wordt gemaakt.

2. De in lid 1 van dit artikel bedoelde informatie specificeert de in Verordening (EG) nr. 1/58 ([15]) bedoelde officiële talen van de instellingen van de Unie waarin het contactpunt kan worden benaderd en waarin verdere uitwisselingen met betrekking tot verwijderingsbevelen op grond van artikel 3 moeten plaatsvinden. Van die talen is er ten minste één van de officiële talen van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging heeft of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft.

AFDELING V

UITVOERING EN HANDHAVING

Artikel 16

Rechtsmacht

1. De lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging heeft, heeft rechtsmacht voor de toepassing van de artikelen 5, 18 en 21. Een aanbieder van hostingdiensten die zijn hoofdvestiging niet in de Unie heeft, wordt geacht onder de rechtsmacht te vallen van de lidstaat waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft.

2. Indien een aanbieder van hostingdiensten die zijn hoofdvestiging niet in de Unie heeft, verzuimt een wettelijke vertegenwoordiger aan te wijzen, hebben alle lidstaten rechtsmacht.

3. Indien een bevoegde autoriteit van een lidstaat zijn rechtsmacht op grond van lid 2 uitoefent, stelt hij daar de bevoegde autoriteiten van alle andere lidstaten van in kennis.

Artikel 17

Wettelijke vertegenwoordiger

1. Een aanbieder van hostingdiensten die zijn hoofdvestiging niet in de Unie heeft, wijst schriftelijk een natuurlijke persoon of rechtspersoon aan als zijn wettelijke vertegenwoordiger in de Unie voor de ontvangst, naleving en handhaving van verwijderingsbevelen en besluiten van de bevoegde autoriteiten.

2. De aanbieder van hostingdiensten verleent zijn wettelijke vertegenwoordiger de nodige bevoegdheden en middelen om die verwijderingsbevelen en besluiten na te leven en om met de bevoegde autoriteiten samen te werken.

De wettelijke vertegenwoordiger heeft zijn verblijf- of vestigingsplaats in een van de lidstaten waar de aanbieder van hostingdiensten zijn diensten aanbiedt.

3. De wettelijke vertegenwoordiger kan aansprakelijk worden gesteld voor inbreuken op deze verordening, onverminderd de aansprakelijkheid of vorderingen in rechte tegen de aanbieder van hostingdiensten.

4. De aanbieder van hostingdiensten stelt de in artikel 12, lid 1, punt d), bedoelde bevoegde autoriteit van de lidstaat waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, in kennis van de aanwijzing.

De aanbieder van hostingdiensten maakt de informatie over de wettelijke vertegenwoordiger openbaar.

AFDELING VI

SLOTBEPALINGEN

Artikel 18

Sancties

1. De lidstaten stellen voorschriften vast ten aanzien van de sancties die van toepassing zijn op inbreuken op deze verordening door aanbieders van hostingdiensten, en nemen alle nodige maatregelen om ervoor te zorgen dat die sancties worden uitgevoerd. Die sancties worden beperkt tot het aanpakken van inbreuken op artikel 3, leden 3 en 6, artikel 4, leden 2 en 7, artikel 5, leden 1, 2, 3, 5 en 6, artikelen 6, 7, 10 en 11, artikel 14, lid 5, artikel 15, lid 1, en artikel 17.

([15]) Verordening nr. 1 tot regeling van het taalgebruik in de Europese Economische Gemeenschap (PB 17 van 6.10.1958, blz. 385).

De in de eerste alinea bedoelde sancties zijn doeltreffend, evenredig en afschrikkend. De lidstaten stellen de Commissie uiterlijk op … [*twaalf maanden na de datum van inwerkingtreding van deze verordening*] van die voorschriften en maatregelen in kennis en delen haar onverwijld alle latere wijzigingen daarvan mee.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten, wanneer zij besluiten al dan niet een sanctie op te leggen en wanneer zij het type en de omvang van de sanctie bepalen, rekening houden met alle relevante omstandigheden, waaronder:

a) de aard, de ernst en de duur van de inbreuk;

b) de opzettelijke dan wel nalatige aard van de inbreuk;

c) eerdere inbreuken door de aanbieder van hostingdiensten;

d) de financiële draagkracht van de aanbieder van hostingdiensten;

e) de mate waarin de aansprakelijk geachte aanbieder van hostingdiensten met de bevoegde autoriteiten samenwerkt;

f) de aard en omvang van de aanbieder van hostingdiensten, met name of het gaat om een micro-, kleine of middelgrote onderneming;

g) de schuldgraad van de aanbieder van hostingdiensten, rekening houdend met de technische en organisatorische maatregelen die de aanbieder van hostingdiensten heeft genomen om te voldoen aan deze verordening.

3. De lidstaten zorgen ervoor dat bij een systematisch of aanhoudend verzuim de verplichtingen op grond van artikel 3, lid 3, na te leven, financiële sancties worden opgelegd van ten hoogste 4 % van de mondiale omzet van de aanbieder van hostingdiensten in het voorafgaande boekjaar.

Artikel 19

Technische vereisten en wijzigingen van de bijlagen

1. De Commissie is bevoegd overeenkomstig artikel 20 gedelegeerde handelingen vast te stellen om deze verordening aan te vullen met de nodige technische voorschriften voor de elektronische middelen die de bevoegde autoriteiten moeten gebruiken voor de verzending van verwijderingsbevelen.

2. De Commissie is bevoegd overeenkomstig artikel 20 gedelegeerde handelingen vast te stellen tot wijziging van de bijlagen om doeltreffend te reageren als verbeteringen moeten worden aangebracht aan de inhoud van de modellen voor verwijderingsbevelen en om informatie te verstrekken over de onmogelijkheid om verwijderingsbevelen uit te voeren.

Artikel 20

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De in artikel 19 bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor onbepaalde tijd met ingang van 7 juni 2022.

3. Het Europees Parlement of de Raad kan de in artikel 19 bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een op grond van artikel 19 vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 21

Monitoring

1. De lidstaten verzamelen bij hun bevoegde autoriteiten en de onder hun rechtsmacht vallende aanbieders van hostingdiensten informatie over de maatregelen die zij overeenkomstig deze verordening in het vorige kalenderjaar hebben genomen, en zenden die informatie elk jaar uiterlijk op 31 maart aan de Commissie. Die informatie omvat:

a) het aantal uitgevaardigde verwijderingsbevelen en het aantal items met terroristische inhoud die verwijderd zijn of waartoe de toegang geblokkeerd is, en de snelheid waarmee die items verwijderd zijn of waarmee de toegang tot die items geblokkeerd is;

b) de op grond van artikel 5 genomen specifieke maatregelen, met inbegrip van het aantal items met terroristische inhoud die verwijderd zijn of waartoe de toegang geblokkeerd is, en de snelheid waarmee die items verwijderd zijn of waarmee de toegang tot die items geblokkeerd is;

c) het aantal door bevoegde autoriteiten verzonden verzoeken om toegang tot inhoud die aanbieders van hostingdiensten op grond van artikel 6 hebben bewaard;

d) het aantal ingestelde klachtenprocedures en door de aanbieders van hostingdiensten genomen maatregelen op grond van artikel 10;

e) het aantal ingestelde administratieve of gerechtelijke toetsingsprocedures en door de bevoegde autoriteit overeenkomstig het nationale recht genomen besluiten.

2. Uiterlijk op 7 juni 2023 stelt de Commissie een gedetailleerd programma vast voor de monitoring van de outputs, resultaten en effecten van deze verordening. Het monitoringprogramma vermeldt de indicatoren en middelen waarmee en de tijdstippen waarop de gegevens en ander nodig bewijsmateriaal moeten worden verzameld. Het specificeert de maatregelen die de Commissie en de lidstaten bij het verzamelen en analyseren van de gegevens en ander bewijsmateriaal moeten nemen om de voortgang te monitoren en deze verordening op grond van artikel 23 te evalueren.

Artikel 22

Uitvoeringsverslag

Uiterlijk op 7 juni 2023 dient de Commissie bij het Europees Parlement en bij de Raad een verslag in over de toepassing van deze verordening. Dat verslag bevat informatie over monitoring uit hoofde van artikel 21 en informatie die voortkomt uit de transparantieverplichtingen uit hoofde van artikel 8. De lidstaten verstrekken de Commissie de informatie die nodig is om het verslag op te stellen.

Artikel 23

Evaluatie

Uiterlijk op 7 juni 2024 verricht de Commissie een evaluatie van deze verordening en dient zij bij het Europees Parlement en bij de Raad een verslag in over de toepassing ervan, met inbegrip van:

a) de werking en de doeltreffendheid van de waarborgmechanismen, met name de waarborgmechanismen die in artikel 4, lid 4, artikel 6, lid 3, en in de artikelen 7 tot en met 11 voorzien zijn;

b) de impact van de toepassing van deze verordening op de grondrechten, met name de vrijheid van meningsuiting en van informatie, de eerbiediging van het privéleven en de bescherming van persoonsgegevens, en

c) de bijdrage van deze verordening tot de bescherming van de openbare veiligheid.

Waar passend gaat het verslag vergezeld van wetgevingsvoorstellen.

De lidstaten verstrekken de Commissie de informatie die nodig is om het verslag op te stellen.

De Commissie gaat tevens na of het nodig en haalbaar is een Europees platform inzake terroristische online-inhoud op te zetten om de communicatie en samenwerking in het kader van deze verordening te faciliteren.

Artikel 24

Inwerkingtreding en toepassing

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Zij is van toepassing met ingang van 7 juni 2022.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 29 april 2021.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
D.M. SASSOLI	A.P. ZACARIAS

BIJLAGE I

VERWIJDERINGSBEVEL

(artikel 3 van Verordening (EU) 2021/784 van het Europees Parlement en de Raad)

Op grond van artikel 3 van Verordening (EU) 2021/784 (de "verordening") verwijdert de geadresseerde van dit verwijderingsbevel terroristische inhoud zo spoedig mogelijk en in elk geval binnen één uur na ontvangst van het verwijderingsbevel, of blokkeert hij zo spoedig mogelijk en in elk geval binnen één uur na ontvangst van het verwijderingsbevel de toegang tot terroristische inhoud in alle lidstaten.

Op grond van artikel 6 van de verordening bewaart de geadresseerde de inhoud en bijbehorende gegevens die verwijderd zijn of waartoe de toegang geblokkeerd is, gedurende zes maanden, of langer op verzoek van de bevoegde autoriteiten of rechterlijke instanties.

Op grond van artikel 15, lid 2, van de verordening wordt dit verwijderingsbevel verzonden in een van de talen die door de geadresseerde zijn aangewezen.

DEEL A:

Lidstaat van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt:

.....

NB: de gegevens van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt, moeten in delen E en F worden vermeld

Geadresseerde en, indien toepasselijk, wettelijke vertegenwoordiger:

.....

Contactpunt:

.....

Lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft:

.....

Tijdstip en datum van uitvaardiging van het verwijderingsbevel:

.....

Referentienummer van het verwijderingsbevel:

.....

DEEL B: Terroristische inhoud die zo spoedig mogelijk en in elk geval binnen één uur na ontvangst van het verwijderingsbevel verwijderd moet worden of waartoe de toegang in alle lidstaten zo spoedig mogelijk en in elk geval binnen één uur na ontvangst van het verwijderingsbevel geblokkeerd moet worden

URL-adres en aanvullende informatie om de terroristische inhoud en de precieze locatie daarvan te kunnen identificeren:

.....

Redenen waarom het materiaal als terroristische inhoud wordt beschouwd, overeenkomstig artikel 2, punt 7), van de verordening.

Het materiaal (gelieve aan te kruisen wat van toepassing is):

☐ zet anderen aan tot het plegen van terroristische misdrijven, bijvoorbeeld door terroristische daden te verheerlijken, door het plegen van terroristische misdrijven te bepleiten (artikel 2, punt 7), onder a), van de verordening)

☐ spoort anderen aan tot het plegen van terroristische misdrijven of tot het leveren van een bijdrage aan het plegen van terroristische misdrijven (artikel 2, punt 7), onder b), van de verordening)

☐ spoort anderen aan om deel te nemen aan de activiteiten van een terroristische groepering (artikel 2, punt 7), onder c), van de verordening)

☐ biedt instructies voor het vervaardigen of gebruiken van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, of voor andere specifieke methoden of technieken, met als doel terroristische misdrijven te plegen of daaraan een bijdrage te leveren (artikel 2, punt 7), onder d), van de verordening)

☐ vormt een dreiging voor het plegen van een van de terroristische misdrijven (artikel 2, punt 7), onder e), van de verordening).

Aanvullende informatie om het materiaal als terroristische inhoud te beschouwen:

.....

.....

.....

DEEL C: Informatie voor de aanbieder van inhoud

Gelieve op te merken dat (gelieve aan te kruisen, indien van toepassing):

☐ de geadresseerde, om redenen van openbare veiligheid, zich **moet onthouden van het inlichten van de aanbieder van inhoud** over de verwijdering van of de blokkering van de toegang tot de terroristische inhoud.

Indien het bovenstaande niet toepasselijk is, zie deel G voor nadere gegevens over de mogelijkheden om het verwijderingsbevel uit hoofde van het nationale recht te betwisten in de lidstaat van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt (een kopie van het verwijderingsbevel moet naar de aanbieder van inhoud gestuurd worden, indien hij daar om vraagt).

DEEL D: Informatie voor de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft.

Gelieve aan te kruisen wat van toepassing is:

☐ De lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, is een andere dan de lidstaat van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt.

☐ Een kopie van het verwijderingsbevel wordt gezonden aan de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft.

DEEL E: Nadere gegevens over de bevoegde autoriteit die het verwijderingsbevel uitvaardigt

Type (gelieve aan te kruisen wat van toepassing is):

☐ rechter, rechterlijke instantie of onderzoeksrechter

☐ rechtshandhavingsinstantie

☐ andere bevoegde autoriteit → gelieve ook deel F in te vullen

Nadere gegevens over de bevoegde autoriteit die het verwijderingsbevel uitvaardigt of haar vertegenwoordiger die certificeert dat het verwijderingsbevel nauwkeurig en correct is:

Naam van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt:

.....

Naam en functie (titel en rang) van haar vertegenwoordiger:

.....

Dossiernummer:

.....

Adres:

.....

Telefoonnummer (landcode) (districts-/stadscode):

.....

Faxnummer (landcode) (districts-/stadscode):

.....

E-mailadres .....

Datum .....

Officieel stempel (indien beschikbaar) en handtekening ([1]):

.....

([1]) Een handtekening is niet nodig indien het verwijderingsbevel wordt gezonden via gecertificeerde indieningskanalen die de authenticiteit van de verwijderingsbevelen kunnen garanderen.

DEEL F: Contactgegevens voor follow-up

Contactgegevens van de bevoegde autoriteit die het verwijderingsbevel uitvaardigt, om feedback te ontvangen over het tijdstip van de verwijdering of de blokkering van de toegang, of om verdere verduidelijking te verstrekken:

.....

Contactgegevens van de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft:

.....

DEEL G: Informatie over de mogelijke rechtsmiddelen

Informatie over het bevoegde orgaan of de bevoegde rechterlijke instantie, termijnen en procedures voor het betwisten van het verwijderingsbevel:

Bevoegd orgaan of bevoegde rechterlijke instantie waarbij het verwijderingsbevel betwist kan worden:

.....

Termijn voor het betwisten van het verwijderingsbevel (dagen/maanden te beginnen vanaf)

.....

Links naar bepalingen in de nationale wetgeving:

.....

BIJLAGE II

FEEDBACK NA VERWIJDERING VAN OF BLOKKERING VAN DE TOEGANG TOT TERRORISTISCHE INHOUD

(artikel 3, lid 6, van Verordening (EU) 2021/784 van het Europees Parlement en de Raad)

DEEL A:

Geadresseerde van het verwijderingsbevel:

.....

Bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd:

.....

Dossiernummer van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd:

.....

Dossiernummer van de geadresseerde:

.....

Tijdstip en datum van ontvangst van het verwijderingsbevel:

.....

DEEL B: Genomen maatregelen om het verwijderingsbevel na te leven

(gelieve aan te kruisen wat van toepassing is):

☐ de terroristische inhoud werd verwijderd

☐ de toegang tot de terroristische inhoud werd in alle lidstaten geblokkeerd

Tijdstip en datum van de genomen maatregel:

.....

DEEL C: Nadere gegevens van de geadresseerde

Naam van de aanbieder van hostingdiensten:

.....

OF

Naam van de wettelijke vertegenwoordiger van de aanbieder van hostingdiensten:

.....

Lidstaat van de hoofdvestiging van de aanbieder van hostingdiensten

.....

OF

Lidstaat van de verblijf- of vestigingsplaats van de wettelijke vertegenwoordiger van de aanbieder van hostingdiensten:

.....

Naam van de gemachtigde:

.....

E-mailadres van het contactpunt:

.....

Datum:

.....

BIJLAGE III

INFORMATIE OVER DE ONMOGELIJKHEID OM HET VERWIJDERINGSBEVEL UIT TE VOEREN

(artikel 3, leden 7 en 8, van Verordening (EU) 2021/784 van het Europees Parlement en de Raad)

DEEL A:

Geadresseerde van het verwijderingsbevel:

.....

Bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd:

.....

Dossiernummer van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd:

.....

Dossiernummer van de geadresseerde:

.....

Tijdstip en datum van ontvangst van het verwijderingsbevel:

.....

DEEL B: Niet-uitvoering

1) Het verwijderingsbevel kan niet binnen de termijn worden uitgevoerd om de volgende redenen (gelieve aan te kruisen wat van toepassing is):

☐ overmacht of feitelijke onmogelijkheid die, onder meer om objectief te rechtvaardigen technische of operationele redenen, niet aan de aanbieder van hostingdiensten kan worden toegerekend

☐ het verwijderingsbevel bevat kennelijke fouten

☐ het verwijderingsbevel bevat onvoldoende informatie

2) Gelieve nadere informatie te verstrekken over de redenen voor niet-uitvoering:

.....

3) Als het verwijderingsbevel kennelijke fouten en/of onvoldoende informatie bevat, gelieve de fouten en de nodige nadere informatie of verduidelijking te specificeren:

.....

DEEL C: Nadere gegevens over de aanbieder van hostingdiensten of zijn wettelijke vertegenwoordiger

Naam van de aanbieder van hostingdiensten:

.....

OF

Naam van de wettelijke vertegenwoordiger van de aanbieder van hostingdiensten

.....

Naam van de gemachtigde:

.....

Contactgegevens (e-mailadres):

.....

Handtekening:

.....

Tijdstip en datum:

.....