EUROPESE
COMMISSIE

Brussel, 12.9.2018
COM(2018) 640 final

2018/0331 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

ter voorkoming van de verspreiding van terroristische online-inhoud

Een bijdrage van de Europese Commissie aan de bijeenkomst van de EU-leiders in Salzburg op 19-20 september 2018

{SEC(2018) 397 final} - {SWD(2018) 408 final} - {SWD(2018) 409 final}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

1.1. Motivering en doel van het voorstel

Door de alomtegenwoordigheid van het internet kunnen de gebruikers communiceren, werken, socialiseren en informatie en inhoud creëren, verkrijgen en delen met honderden miljoenen mensen over de hele wereld. Internetplatforms genereren aanzienlijke voordelen voor het economische en sociale welzijn van de gebruikers, zowel in de Unie als daarbuiten. De mogelijkheid zoveel mensen tegen minimale kosten te bereiken trekt echter ook criminelen aan die het internet willen misbruiken voor illegale doeleinden. De recente terroristische aanslagen op Europese bodem hebben laten zien dat terroristen het internet misbruiken om aanhangers te indoctrineren en te werven, terroristische activiteiten voor te bereiden en te faciliteren, hun wreedheden te verheerlijken, anderen ertoe aan te zetten in hun sporen te treden en het grote publiek angst in te boezemen.

Terroristische inhoud die met die bedoeling online wordt gedeeld, wordt verspreid via aanbieders van hostingdiensten waarop inhoud van derden kan worden geüpload. Bij verschillende recente terroristische aanslagen in Europa is gebleken dat terroristische online-inhoud radicalisering mede in de hand heeft gewerkt en zogeheten lone wolves tot aanslagen heeft geïnspireerd. Dergelijke inhoud heeft niet alleen aanzienlijk negatieve effecten op mensen en de samenleving in het algemeen, maar vermindert ook het vertrouwen van de gebruikers in het internet en tast de bedrijfsmodellen en de reputatie van de getroffen ondernemingen aan. Terroristen misbruiken niet alleen grote socialemediaplatforms, maar steeds vaker kleinere aanbieders die wereldwijd verschillende soorten hostingdiensten aanbieden. Dit misbruik van het internet laat zien dat internetplatforms een bijzondere maatschappelijke verantwoordelijkheid hebben om hun gebruikers te beschermen tegen blootstelling aan terroristische inhoud, en dat deze inhoud ernstige veiligheidsrisico's met zich meebrengt voor de samenleving als geheel.

Naar aanleiding van verzoeken van overheidsinstanties hebben aanbieders van hostingdiensten bepaalde maatregelen genomen om terroristische inhoud op hun diensten te bestrijden. Er is vooruitgang geboekt via vrijwillige kaders en partnerschappen, zoals het EU-internetforum dat in december 2015 van start ging in het kader van de Europese veiligheidsagenda. Het EU-internetforum heeft vrijwillige samenwerking tussen de lidstaten en de aanbieders van hostingdiensten bevorderd en maatregelen ondersteund om terroristische online-inhoud minder toegankelijk te maken en het maatschappelijk middenveld de middelen aan te reiken een doeltreffend alternatief discours op grotere schaal online te verspreiden. Deze inspanningen hebben bijgedragen aan meer samenwerking, betere reacties van bedrijven op doorverwijzingen van nationale autoriteiten en de eenheid voor de doorverwijzing van internetuitingen van Europol, de invoering van vrijwillige proactieve maatregelen om de automatische opsporing van terroristische inhoud te verbeteren, meer samenwerking tussen de bedrijven uit de sector, onder meer bij de ontwikkeling van de "databank van hashcodes" om te voorkomen dat bekende terroristische inhoud wordt geüpload op aangesloten platforms, en grotere transparantie van de inspanningen. Hoewel de samenwerking in het kader van het EU-internetforum in de toekomst moet worden voortgezet, is ook gebleken dat de vrijwillige regelingen hun beperkingen hebben. Ten eerste zijn niet alle getroffen aanbieders van hostingdiensten bij het forum betrokken en ten tweede volstaan de schaal en het tempo van de vooruitgang bij de aanbieders van hostingdiensten in hun geheel niet om dit probleem adequaat aan te pakken.

Dit maakt duidelijk dat de Europese Unie meer actie moet ondernemen tegen terroristische online-inhoud. Op 1 maart 2018 heeft de Commissie een aanbeveling aangenomen over maatregelen om illegale online-inhoud effectief te bestrijden, die voortbouwt op de mededeling van de Commissie van september[1] en de inspanningen in het kader van het EU-internetforum. In de aanbeveling is een hoofdstuk specifiek gewijd aan een aantal maatregelen om het uploaden en delen van terroristische onlinepropaganda effectief te stoppen, zoals verbeteringen van het doorverwijzingsproces, een termijn van één uur om te reageren op doorverwijzingen, proactievere opsporing, doeltreffende verwijdering en voldoende waarborgen om terroristische inhoud correct te beoordelen[2].

Dat er meer actie moet worden ondernomen tegen terroristische online-inhoud, komt ook terug in oproepen van de lidstaten van de EU. Sommige lidstaten hebben reeds wetgeving aangenomen of hebben laten weten dat zij dat van plan zijn. Na een reeks terroristische aanslagen in de EU en gelet op het feit dat terroristische online-inhoud gemakkelijk toegankelijk blijft, heeft de Europese Raad van 22-23 juni 2017 de sector opgeroepen nieuwe technologie en instrumenten te ontwikkelen "waarmee inhoud die aanzet tot terroristische daden, beter automatisch kan worden opgespoord om vervolgens te worden verwijderd. Dit moet zo nodig worden aangevuld met ter zake doende wetgevingsmaatregelen op EU-niveau". De Europese Raad van 28 juni 2018 heeft zich ingenomen getoond met "het voornemen van de Commissie om een wetgevingsvoorstel in te dienen ter verbetering van het opsporen en verwijderen van inhoud die tot haat en terreurdaden aanzet". Voorts heeft het Europees Parlement er in zijn resolutie over onlineplatforms en de digitale eengemaakte markt van 15 juni 2017 bij de platforms op aangedrongen "krachtigere maatregelen te nemen om illegale en schadelijke inhoud online aan te pakken" en heeft het de Commissie verzocht voorstellen in te dienen om deze problemen aan te pakken.

Om deze uitdagingen aan te pakken en gevolg te geven aan de oproepen van de lidstaten en het Europees Parlement, beoogt dit Commissievoorstel een duidelijk en geharmoniseerd rechtskader tot stand te brengen om misbruik van hostingdiensten voor de verspreiding van terroristische online-inhoud te voorkomen, teneinde de goede werking van de digitale eengemaakte markt te waarborgen en tegelijkertijd het vertrouwen en de veiligheid te garanderen. Deze verordening beoogt duidelijkheid te verschaffen over de verantwoordelijkheid van aanbieders van hostingdiensten voor het nemen van alle passende, redelijke en evenredige maatregelen die noodzakelijk zijn om de veiligheid van hun diensten te garanderen en om terroristische online-inhoud snel en doeltreffend op te sporen en te verwijderen, rekening houdend met het fundamentele belang van de vrijheid van meningsuiting en van informatie in een open en democratische samenleving. Zij voert ook een aantal waarborgen in die noodzakelijk zijn om te garanderen dat grondrechten zoals de vrijheid van meningsuiting en van informatie in een democratische samenleving ten volle worden geëerbiedigd, en voorziet tevens in de mogelijkheid rechtsmiddelen in te stellen, die wordt gegarandeerd door het recht op een doeltreffende voorziening in rechte dat in artikel 19 VEU en artikel 47 van het Handvest van de grondrechten van de EU is neergelegd.

Door de vaststelling van een minimale reeks zorgplichten voor aanbieders van hostingdiensten, waaronder enkele specifieke regels en verplichtingen, alsook verplichtingen voor de lidstaten, beoogt het voorstel de huidige maatregelen voor het opsporen, identificeren en verwijderen van terroristische online-inhoud doeltreffender te maken, zonder dat

[1] Mededeling (COM(2017) 555 final) over de bestrijding van illegale online-inhoud.

[2] Aanbeveling (C(2018) 1177 final) van 1 maart 2018 over maatregelen om illegale online-inhoud effectief te bestrijden.

grondrechten, zoals de vrijheid van meningsuiting en van informatie, in het gedrang komen. Dit geharmoniseerde rechtskader zal de verlening van onlinediensten in de hele digitale eengemaakte markt faciliteren, een gelijk speelveld garanderen voor alle aanbieders van hostingdiensten die hun diensten op de Europese Unie richten, en een solide rechtskader bieden voor de opsporing en verwijdering van terroristische inhoud dat ook voorziet in passende waarborgen ter bescherming van de grondrechten. Met name de verplichtingen inzake transparantie zullen het vertrouwen bij de burgers, en in het bijzonder de internetgebruikers, versterken en zullen de verantwoordingsplicht voor en de transparantie van de maatregelen van de ondernemingen vergroten, onder meer tegenover overheidsinstanties. Het voorstel bevat ook de verplichting rechtsmiddelen en klachtenmechanismen in te voeren om ervoor te zorgen dat gebruikers de verwijdering van hun inhoud kunnen aanvechten. De verplichtingen voor de lidstaten zullen aan deze doelstellingen bijdragen en de betrokken autoriteiten beter in staat stellen passende actie te ondernemen tegen terroristische online-inhoud en criminaliteit te bestrijden. Als aanbieders van hostingdiensten de verordening niet naleven, kunnen de lidstaten sancties opleggen.

1.2. Verenigbaarheid met het bestaande EU-rechtskader op het beleidsgebied

Dit voorstel is in overeenstemming met het acquis dat verband houdt met de digitale eengemaakte markt en met name met de richtlijn inzake elektronische handel. De door de aanbieder van hostingdiensten in naleving van deze verordening genomen maatregelen, waaronder proactieve maatregelen, mogen op zich niet ertoe leiden dat die dienstverlener de vrijstelling van aansprakelijkheid verliest waarin artikel 14 van de richtlijn inzake elektronische handel onder bepaalde voorwaarden voorziet. Een besluit van de nationale autoriteiten om evenredige en specifieke proactieve maatregelen op te leggen, mag er in beginsel niet toe leiden dat de lidstaten een algemene toezichtverplichting in de zin van artikel 15, lid 1, van Richtlijn 2000/31/EG wordt opgelegd. Gezien de bijzonder ernstige risico's die met de verspreiding van terroristische inhoud gepaard gaan, kunnen de besluiten op grond van deze verordening echter in uitzonderingsgevallen afwijken van dit in het EU-recht vastgelegde beginsel. Alvorens een dergelijk besluit te nemen, moet de bevoegde autoriteit een billijke afweging maken tussen de behoeften op het gebied van openbare veiligheid en de betrokken belangen en grondrechten, waaronder met name de vrijheid van meningsuiting en van informatie, de vrijheid van ondernemerschap en de bescherming van persoonsgegevens en de persoonlijke levenssfeer. De zorgplichten van aanbieders van hostingdiensten moeten dit in de richtlijn inzake elektronische handel vastgelegde evenwicht weerspiegelen en eerbiedigen.

Het voorstel is ook in overeenstemming met en sluit nauw aan bij Richtlijn (EU) 2017/541 inzake terrorismebestrijding, die een harmonisatie van de wetgevingen van de lidstaten waarbij terroristische misdrijven strafbaar worden gesteld, tot doel heeft. Artikel 21 van de richtlijn inzake terrorismebestrijding verplicht de lidstaten alleen maatregelen te nemen om te zorgen voor de snelle verwijdering van online-inhoud die het publiekelijk uitlokken betreft, en laat de lidstaten de keuze van de maatregelen. Omdat deze verordening preventief van aard is, betreft zij niet alleen materiaal dat tot terrorisme aanzet, maar ook materiaal voor wervings- of opleidingsdoeleinden, waardoor zij rekening houdt met andere misdrijven in verband met terroristische activiteiten, die ook onder Richtlijn (EU) 2017/541 vallen. Deze verordening legt de aanbieders van hostingdiensten rechtstreeks een zorgplicht op om terroristische inhoud te verwijderen en harmoniseert de procedures voor verwijderingsbevelen, met als doel terroristische online-inhoud minder toegankelijk te maken.

De verordening vult de in de toekomstige richtlijn audiovisuele mediadiensten vastgestelde regels aan, in die zin dat haar personele en materiële toepassingsgebied ruimer is. De

verordening heeft niet alleen betrekking op platforms voor het delen van video's, maar op alle verschillende soorten aanbieders van hostingdiensten. Bovendien heeft zij niet alleen betrekking op video's, maar ook op beelden en tekst. Voorts gaat deze verordening in materieel opzicht verder dan de richtlijn, doordat de regels voor verzoeken tot verwijdering van terroristische inhoud en de proactieve maatregelen worden geharmoniseerd.

De voorgestelde verordening bouwt voort op de aanbeveling van de Commissie van maart 2018 over illegale inhoud[3]. De aanbeveling blijft van kracht en allen die een rol kunnen spelen om illegale inhoud - waaronder terroristische inhoud - minder toegankelijk te maken, moeten hun inspanningen blijven afstemmen op de in de aanbeveling genoemde maatregelen.

1.3. Samenvatting van de voorgestelde verordening

De personele werkingssfeer van het voorstel omvat aanbieders van hostingdiensten die hun diensten aanbieden in de Unie, ongeacht hun plaats van vestiging of hun omvang. De voorgestelde wetgeving voorziet in een aantal maatregelen om te voorkomen dat hostingdiensten worden misbruikt voor de verspreiding van terroristische online-inhoud, teneinde de goede werking van de digitale eengemaakte markt te waarborgen en tegelijkertijd vertrouwen en veiligheid te garanderen. De definitie van illegale terroristische inhoud is in overeenstemming met de definitie van terroristische misdrijven in Richtlijn (EU) 2017/541: het gaat om informatie die wordt gebruikt om aan te zetten tot het plegen van terroristische misdrijven of het plegen van terroristische misdrijven te verheerlijken, en waarin het bijdragen aan het plegen van terroristische misdrijven wordt aangemoedigd en daarvoor instructies worden gegeven alsook het deelnemen aan terroristische groeperingen wordt bevorderd.

Om de verwijdering van illegale terroristische inhoud te garanderen, voert de verordening een verwijderingsbevel in, dat kan worden uitgevaardigd als een administratief besluit of rechterlijke beslissing van een bevoegde autoriteit in een lidstaat. In die gevallen is de aanbieder van hostingdiensten verplicht de inhoud te verwijderen of de toegang daartoe onmogelijk te maken binnen één uur. Daarenboven harmoniseert de verordening de minimumvereisten voor doorverwijzingen die door bevoegde autoriteiten van de lidstaten en organen van de Unie (zoals Europol) worden gezonden aan aanbieders van hostingdiensten, die de betrokken inhoud moeten toetsen aan hun eigen voorwaarden. Ten slotte schrijft de verordening voor dat aanbieders van hostingdiensten, waar passend, proactieve maatregelen moeten nemen die in verhouding staan tot de omvang van het risico, en terroristisch materiaal van hun diensten moeten verwijderen, onder meer met behulp van automatische opsporingsinstrumenten.

De maatregelen ter vermindering van terroristische online-inhoud gaan vergezeld van een aantal belangrijke waarborgen om de volledige bescherming van grondrechten te garanderen. Als onderdeel van de maatregelen om inhoud die geen terroristische inhoud is tegen onterechte verwijdering te beschermen, bevat het voorstel de verplichting rechtsmiddelen en klachtenmechanismen in te voeren waarmee gebruikers de verwijdering van hun inhoud kunnen aanvechten. Daarnaast bevat de verordening verplichtingen inzake transparantie voor de maatregelen die door aanbieders van hostingdiensten ten aanzien van terroristische inhoud worden genomen, wat zorgt voor verantwoordingsplicht tegenover gebruikers, burgers en overheidsinstanties.

[3] Aanbeveling (C(2018) 1177 final) van 1 maart 2018 over maatregelen om illegale online-inhoud effectief te bestrijden.

De verordening verplicht de lidstaten ook ervoor te zorgen dat hun bevoegde autoriteiten over de nodige capaciteit beschikken om tegen terroristische online-inhoud op te treden. Daarnaast zijn de lidstaten verplicht elkaar op de hoogte te houden en met elkaar samen te werken: om te zorgen voor coördinatie met betrekking tot verwijderingsbevelen en doorverwijzingen kunnen zij gebruikmaken van de door Europol opgezette kanalen. De verordening voorziet ook in verplichtingen voor aanbieders van hostingdiensten om meer in detail verslag uit te brengen over de genomen maatregelen en de rechtshandhaving in te lichten wanneer zij inhoud detecteren die mensenlevens of de veiligheid in gevaar brengt. Ten slotte zijn aanbieders van hostingdiensten verplicht de door hen verwijderde inhoud te bewaren, wat een waarborg vormt tegen onterechte verwijdering en ervoor zorgt dat potentieel bewijsmateriaal niet verloren gaat voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

2.1. Rechtsgrondslag

De rechtsgrondslag is artikel 114 van het Verdrag betreffende de werking van de Europese Unie, dat voorziet in de vaststelling van maatregelen om de werking van de interne markt te garanderen.

Artikel 114 VWEU is de passende rechtsgrondslag om de voorwaarden te harmoniseren waaronder aanbieders van hostingdiensten diensten kunnen verlenen over grenzen heen in de digitale eengemaakte markt, en de verschillen tussen de bepalingen van de lidstaten aan te pakken die anders de werking van de interne markt zouden kunnen belemmeren. Het voorkomt ook het ontstaan van toekomstige belemmeringen voor de economische bedrijvigheid als gevolg van verschillen in de wijze waarop de nationale wetgevingen zich kunnen ontwikkelen.

Artikel 114 VWEU kan ook worden gebruikt om verplichtingen op te leggen aan dienstverleners die buiten het grondgebied van de EU zijn gevestigd, wanneer hun dienstverlening van invloed is op de interne markt, aangezien dit noodzakelijk is voor het nagestreefde doel van de interne markt.

2.2. Keuze van het instrument

Artikel 114 VWEU geeft de wetgever van de Unie de mogelijkheid verordeningen en richtlijnen vast te stellen.

Aangezien het voorstel betrekking heeft op verplichtingen van dienstverleners die gewoonlijk in meer dan één lidstaat diensten aanbieden, zouden verschillen in de toepassing van deze regels een belemmering vormen voor de verlening van diensten door dienstverleners die in meerdere lidstaten actief zijn. Een verordening maakt het mogelijk dezelfde verplichting op uniforme wijze in de hele Unie op te leggen, is rechtstreeks van toepassing, zorgt voor duidelijkheid en meer rechtszekerheid en voorkomt dat de omzetting in de lidstaten uiteenloopt. Daarom wordt een verordening geacht de meest geschikte vorm voor dit instrument te zijn.

2.3. Subsidiariteit

Gezien de grensoverschrijdende dimensie van de problemen die dit voorstel aanpakt, moeten de erin opgenomen maatregelen op het niveau van de Unie worden vastgesteld teneinde de doelstellingen te bereiken. Het internet is van nature grensoverschrijdend en inhoud die in één lidstaat wordt gehost, is normaal gesproken toegankelijk vanuit alle andere lidstaten.

Er is een onsamenhangend kader van nationale regels ter bestrijding van terroristische online-inhoud aan het ontstaan, waardoor de omvang van de risico's alleen maar zal toenemen. Dit zou leiden tot een last voor het bedrijfsleven dat uiteenlopende regels zou moeten naleven, tot ongelijke voorwaarden voor ondernemingen en tot lacunes in de beveiliging.

Een optreden van de EU zorgt dus voor meer rechtszekerheid en maakt de maatregelen van aanbieders van hostingdiensten tegen terroristische online-inhoud doeltreffender. Daardoor zullen meer bedrijven, ook van buiten de EU, actie kunnen ondernemen, waardoor de integriteit van de digitale eengemaakte markt wordt versterkt.

Een optreden van de EU is dus gerechtvaardigd, zoals ook blijkt uit de conclusies van de Europese Raad van juni 2018, waarin de Commissie wordt verzocht een wetgevingsvoorstel op dit gebied in te dienen.

2.4. Evenredigheid

Het voorstel bevat regels voor aanbieders van hostingdiensten, die maatregelen moeten nemen om terroristische inhoud snel van hun diensten te verwijderen. Essentiële onderdelen ervan beperken het voorstel tot wat nodig is om de beleidsdoelstellingen te verwezenlijken.

Het voorstel houdt rekening met de last voor de aanbieders van hostingdiensten en bevat waarborgen, onder meer ter bescherming van de vrijheid van meningsuiting en van informatie en van andere grondrechten. Het tijdsbestek van één uur voor verwijdering geldt alleen voor verwijderingsbevelen voor inhoud waarvan de bevoegde autoriteiten in een aan rechterlijke toetsing onderworpen besluit hebben vastgesteld dat die illegaal is. Voor doorverwijzingen is er een verplichting maatregelen te nemen om de snelle toetsing van terroristische inhoud te faciliteren, echter zonder dat daarvoor verplichtingen tot verwijdering of absolute termijnen worden opgelegd. Het uiteindelijke besluit blijft een vrijwillig besluit van de aanbieder van hostingdiensten. De last voor ondernemingen ten gevolge van de toetsing van de inhoud wordt verlicht door het feit dat de bevoegde autoriteiten van de lidstaten en de organen van de Unie moeten uitleggen waarom de inhoud als terroristische inhoud kan worden beschouwd. Aanbieders van hostingdiensten nemen, waar passend, proactieve maatregelen om hun diensten te beschermen tegen de verspreiding van terroristische inhoud. De specifieke verplichtingen in verband met proactieve maatregelen blijven beperkt tot die aanbieders van hostingdiensten die aan terroristische inhoud worden blootgesteld, wat blijkt uit de ontvangst van een definitief geworden verwijderingsbevel, en moeten in verhouding staan tot de omvang van het risico en de middelen van het bedrijf. De bewaring van de verwijderde inhoud en bijbehorende gegevens wordt beperkt tot een termijn die in verhouding staat tot het doel dat procedures voor administratieve of rechterlijke toetsing en het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven mogelijk moeten zijn.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

3.1. Raadpleging van belanghebbenden

Bij de voorbereiding van dit wetgevingsvoorstel heeft de Commissie alle belanghebbenden geraadpleegd om hun standpunten te begrijpen en een mogelijke koers voor te stellen. De Commissie heeft een openbare raadpleging gehouden over maatregelen om de strijd tegen illegale inhoud doeltreffender te maken, waarop 8 961 antwoorden werden ontvangen, waarvan 8 749 van particulieren, 172 van organisaties, 10 van overheidsdiensten en 30 van andere categorieën respondenten. Parallel hiermee is een Eurobarometer-enquête over illegale online-inhoud gehouden met een willekeurige steekproef van 33 500 inwoners van de EU. De Commissie heeft in mei en juni 2018 ook de autoriteiten van de lidstaten en aanbieders van

hostingdiensten geraadpleegd over specifieke maatregelen om terroristische online-inhoud aan te pakken.

De meeste belanghebbenden zijn van mening dat terroristische online-inhoud een ernstig maatschappelijk probleem vormt voor de internetgebruikers en de bedrijfsmodellen van aanbieders van hostingdiensten. Meer in het algemeen is 65 % van de respondenten van de Eurobarometer-enquête[4] van mening dat het internet niet veilig is voor zijn gebruikers en vindt 90 % van de respondenten het belangrijk om de verspreiding van illegale online-inhoud tegen te gaan. Uit overleg met de lidstaten is gebleken dat vrijwillige regelingen weliswaar resultaten opleveren, maar dat velen vinden dat er bindende verplichtingen inzake terroristische inhoud moeten komen, wat in de conclusies van de Europese Raad van juni 2018 is herhaald. Hoewel de aanbieders van hostingdiensten doorgaans voorstander waren van de voortzetting van vrijwillige maatregelen, hebben zij gewezen op de potentiële negatieve effecten van de toenemende versnippering van de wetgeving in de Unie.

Veel belanghebbenden hebben ook erop gewezen dat alle regelgevende maatregelen voor de verwijdering van inhoud, in het bijzonder proactieve maatregelen en strikte termijnen, moeten worden afgewogen tegen de waarborgen voor de grondrechten, meer bepaald de vrijheid van meningsuiting. De belanghebbenden hebben gewezen op een aantal noodzakelijke maatregelen op het gebied van transparantie en verantwoordingsplicht en op het feit dat het gebruik van automatische instrumenten menselijke controle vereist.

3.2. Effectbeoordeling

De Raad voor regelgevingstoetsing heeft een positief advies met voorbehoud uitgebracht over de effectbeoordeling en heeft een aantal voorstellen voor verbetering gedaan[5]. Naar aanleiding van dit advies is het effectbeoordelingsverslag gewijzigd om met de belangrijkste opmerkingen van de Raad rekening te houden, door de focus specifiek op terroristische inhoud te leggen terwijl de gevolgen voor de werking van de digitale eengemaakte markt verder worden benadrukt en het effect op de grondrechten en de werking van de in de opties voorgestelde waarborgen diepgaander worden geanalyseerd.

Als er geen aanvullende maatregelen worden genomen, wordt verwacht dat de vrijwillige maatregelen in het kader van het basisscenario worden voortgezet en tot enige vermindering van terroristische online-inhoud leiden. Waarschijnlijk zullen echter niet alle aanbieders van hostingdiensten die aan dergelijke inhoud worden blootgesteld, vrijwillige maatregelen nemen en de verdere versnippering van de wetgeving zal naar verwachting extra belemmeringen voor grensoverschrijdende dienstverlening doen ontstaan. Naast het basisscenario zijn drie belangrijke beleidsopties in overweging genomen, die in toenemende mate doeltreffend zijn voor de verwezenlijking van de in de effectbeoordeling beschreven doelstellingen en de algemene beleidsdoelstelling terroristische online-inhoud te verminderen.

In de drie opties is het toepassingsgebied van de verplichtingen gefocust op alle aanbieders van hostingdiensten (personeel toepassingsgebied) die in de EU en in derde landen zijn gevestigd, in zoverre zij hun diensten in de Unie aanbieden (geografisch toepassingsgebied). Gezien de aard van het probleem en het feit dat misbruik van kleinere platforms moet worden voorkomen, is in geen van de opties voorzien in uitzonderingen voor kmo's. Alle opties vereisen dat aanbieders van hostingdiensten, ook die van buiten de EU, een wettelijke

[4] Eurobarometer 469, Illegale content online, juni 2018.

[5] Link naar het advies van de Raad voor regelgevingstoetsing op RegDoc.

vertegenwoordiger in de EU aanwijzen, zodat de EU-regels kunnen worden gehandhaafd. In alle opties moeten de lidstaten sanctiemechanismen ontwikkelen.

Alle opties voorzien in de oprichting van een nieuw, geharmoniseerd systeem van wettelijke verwijderingsbevelen met betrekking tot terroristische online-inhoud die door de nationale autoriteiten worden uitgevaardigd tegen aanbieders van hostingdiensten, en in de verplichting om die inhoud binnen één uur te verwijderen. Deze bevelen vereisen niet noodzakelijkerwijs een beoordeling door de aanbieder van hostingdiensten en er kan een rechtsmiddel tegen worden ingesteld.

De drie opties hebben als gemeenschappelijk kenmerk dat wordt voorzien in waarborgen, meer bepaald klachtenprocedures en doeltreffende voorzieningen in rechte, met inbegrip van rechtsmiddelen en andere bepalingen ter voorkoming van de onterechte verwijdering van inhoud die geen terroristische inhoud is, om te garanderen dat de grondrechten worden geëerbiedigd. Voorts omvatten alle opties verslagleggingsverplichtingen in de vorm van openbare transparantie en verslaglegging aan de lidstaten en de Commissie, alsook aan de autoriteiten in geval van vermeende misdrijven. Daarnaast wordt voorzien in verplichtingen tot samenwerking tussen nationale autoriteiten, aanbieders van hostingdiensten en, in voorkomend geval, Europol.

De belangrijkste verschillen tussen de drie opties betreffen de reikwijdte van de definitie van terroristische inhoud, de mate van harmonisatie van de doorverwijzingen, de omvang van de proactieve maatregelen, de coördinatieverplichtingen van de lidstaten en de vereisten inzake bewaring van gegevens. Bij optie 1 zou het materiële toepassingsgebied worden beperkt tot inhoud die wordt verspreid om rechtstreeks aan te zetten tot het plegen van een terroristische handeling, volgens een enge definitie, terwijl de opties 2 en 3 voorzien in een ruimere aanpak, die ook materiaal betreffende werving en opleiding omvat. Wat de proactieve maatregelen betreft, zouden aanbieders van hostingdiensten die aan terroristische inhoud worden blootgesteld, bij optie 1 een risicobeoordeling moeten uitvoeren, maar proactieve maatregelen om het risico aan te pakken, zouden vrijwillig blijven. Bij optie 2 zouden aanbieders van hostingdiensten een actieplan moeten opstellen, dat kan voorzien in het gebruik van automatische instrumenten om te voorkomen dat reeds verwijderde inhoud opnieuw wordt geüpload. Optie 3 omvat uitgebreidere proactieve maatregelen waarbij aanbieders van hostingdiensten die aan terroristische inhoud worden blootgesteld, ook nieuw materiaal moeten identificeren. Bij alle opties zouden de vereisten met betrekking tot proactieve maatregelen in verhouding staan tot de mate van blootstelling aan terroristisch materiaal en de economische draagkracht van de dienstverlener. Wat de doorverwijzingen betreft, zou optie 1 de aanpak van doorverwijzingen niet harmoniseren, terwijl optie 2 dit wel zou doen voor Europol en optie 3 tevens doorverwijzingen door de lidstaten zou harmoniseren. Bij de opties 2 en 3 zouden de lidstaten verplicht zijn elkaar in te lichten en met elkaar te coördineren en samen te werken, en in optie 3 zouden zij er ook voor moeten zorgen dat hun bevoegde autoriteiten de capaciteit hebben om terroristische inhoud op te sporen en te melden. Tot slot omvat optie 3 ook een verplichting tot bewaring van gegevens als een waarborg in gevallen van onterechte verwijdering, en om strafrechtelijke onderzoeken te faciliteren.

Naast de wettelijke bepalingen zouden alle wetgevingsopties vergezeld gaan van een reeks ondersteunende maatregelen, met name om de samenwerking tussen de nationale autoriteiten en Europol alsook de samenwerking met aanbieders van hostingdiensten te faciliteren, en van steun voor onderzoek, ontwikkeling en innovatie met het oog op de ontwikkeling en invoering van technologische oplossingen. Na de goedkeuring van het rechtsinstrument zouden ook

aanvullende bewustmakings- en ondersteuningsinstrumenten voor kmo's kunnen worden ingezet.

De effectbeoordeling concludeerde dat een reeks maatregelen nodig is om de beleidsdoelstelling te verwezenlijken. De uitgebreide definitie van terroristische inhoud, die op het schadelijkste materiaal zou slaan, zou de voorkeur genieten boven een enge definitie van inhoud (optie 1). Proactieve verplichtingen die ertoe beperkt blijven te voorkomen dat terroristische inhoud opnieuw wordt geüpload (optie 2), zouden minder effect hebben dan verplichtingen inzake de opsporing van nieuwe terroristische inhoud (optie 3). De bepalingen inzake doorverwijzingen zouden zowel doorverwijzingen door Europol als door de lidstaten moeten omvatten (optie 3) en niet enkel beperkt mogen blijven tot doorverwijzingen door Europol (optie 2), aangezien doorverwijzingen door de lidstaten een belangrijke bijdrage vormen in het kader van de algemene inspanning om terroristische online-inhoud minder toegankelijk te maken. Deze maatregelen zouden moeten worden uitgevoerd bovenop de maatregelen die alle opties gemeenschappelijk hebben, waartoe ook solide waarborgen tegen onterechte verwijdering van inhoud behoren.

3.3. Grondrechten

Onlinepropaganda van terroristen is bedoeld om individuen ertoe aan te zetten terroristische aanslagen te plegen, onder meer door het geven van gedetailleerde instructies om maximale schade toe te brengen. Verdere propaganda wordt meestal verspreid nadat dergelijke wreedheden hebben plaatsgevonden, en bestaat eruit die handelingen te verheerlijken en anderen aan te moedigen het voorbeeld te volgen. Deze verordening draagt bij aan de bescherming van de openbare veiligheid door terroristische inhoud die de schending van grondrechten bevordert en aanmoedigt, minder toegankelijk te maken.

Het voorstel kan effect hebben op een aantal grondrechten:

(a) rechten van de aanbieder van inhoud: het recht op vrijheid van meningsuiting, het recht op bescherming van persoonsgegevens, het recht op eerbiediging van het privéleven en van het familie- en gezinsleven, het non-discriminatiebeginsel en het recht op een doeltreffende voorziening in rechte;

(b) rechten van de dienstverlener: het recht op vrijheid van ondernemerschap, het recht op een doeltreffende voorziening in rechte;

(c) rechten van alle burgers: het recht op vrijheid van meningsuiting en van informatie.

Rekening houdend met het desbetreffende acquis zijn in de voorgestelde verordening passende en solide waarborgen opgenomen om ervoor te zorgen dat de rechten van deze personen worden beschermd.

Een eerste element in dit verband is dat de verordening een definitie van terroristische online-inhoud vaststelt die in overeenstemming is met de definitie van terroristische misdrijven in Richtlijn (EU) 2017/541. Deze definitie is van toepassing op verwijderingsbevelen en doorverwijzingen, alsook op proactieve maatregelen. Deze definitie garandeert dat alleen illegale inhoud die aan een voor de hele Unie geldende definitie van daarmee verband houdende strafbare feiten beantwoordt, moet worden verwijderd. Daarnaast omvat de verordening algemene zorgplichten voor aanbieders van hostingdiensten: zij moeten op zorgvuldige, evenredige en niet-discriminerende wijze handelen ten aanzien van inhoud die zij opslaan, met name wanneer zij hun eigen voorwaarden toepassen, teneinde te voorkomen dat inhoud wordt verwijderd die geen terroristische inhoud is.

Meer in het bijzonder is de verordening zodanig vormgegeven dat wordt gegarandeerd dat de maatregelen die met betrekking tot de grondrechten worden genomen, evenredig zijn. Met betrekking tot verwijderingsbevelen rechtvaardigt de beoordeling van de inhoud (met inbegrip van juridische controles, zo nodig) door een bevoegde autoriteit dat voor deze maatregel een tijdsbestek van één uur voor verwijdering geldt. Voorts gelden de bepalingen in deze verordening die betrekking hebben op doorverwijzingen, alleen voor de doorverwijzingen die door de bevoegde autoriteiten en de organen van de Unie zijn gezonden en waarin wordt uitgelegd waarom de inhoud als terroristische inhoud kan worden beschouwd. Voor het verwijderen van in een doorverwijzing geïdentificeerde inhoud blijft weliswaar de aanbieder van hostingdiensten verantwoordelijk, maar zijn besluit wordt gefaciliteerd door bovenvermelde beoordeling.

Bij proactieve maatregelen blijft de verantwoordelijkheid voor het identificeren, beoordelen en verwijderen van inhoud bij de aanbieders van hostingdiensten en zijn zij verplicht te voorzien in waarborgen om te garanderen dat inhoud niet ten onrechte wordt verwijderd, onder meer door menselijke evaluatie, in het bijzonder wanneer met een grotere context rekening moet worden gehouden. Bovendien zou, anders dan in het basisscenario waarin de meest getroffen bedrijven automatische instrumenten zonder publiek toezicht invoeren, aan de bevoegde instanties in de lidstaten verslag moeten worden uitgebracht over de vormgeving van de maatregelen en de uitvoering daarvan. Deze verplichting vermindert het risico op onterechte verwijderingen, zowel voor bedrijven die nieuwe instrumenten ontwikkelen als voor bedrijven die er al gebruik van maken. Daarnaast zijn aanbieders van hostingdiensten verplicht gebruiksvriendelijke klachtenmechanismen in te voeren waarmee aanbieders van inhoud het besluit tot verwijdering van hun inhoud kunnen betwisten, en moeten zij transparantieverslagen voor het grote publiek publiceren.

Tot slot moeten aanbieders van hostingdiensten, mochten inhoud en bijbehorende gegevens ondanks deze waarborgen ten onrechte worden verwijderd, die inhoud en gegevens gedurende zes maanden bewaren om die inhoud opnieuw te kunnen plaatsen en zo de doeltreffendheid te garanderen van de klachten- en toetsingsprocedures ter bescherming van de vrijheid van meningsuiting en van informatie. Tegelijkertijd dient de bewaring ook rechtshandhavingsdoeleinden. Aanbieders van hostingdiensten moeten zorgen voor technische en organisatorische waarborgen om te voorkomen dat de gegevens voor andere doeleinden worden gebruikt.

De voorgestelde maatregelen, meer bepaald die welke betrekking hebben op verwijderingsbevelen, doorverwijzingen, proactieve maatregelen en de bewaring van gegevens, moeten niet alleen de internetgebruikers beschermen tegen terroristische inhoud, maar ook bijdragen aan de bescherming van het recht op leven van de burgers doordat terroristische online-inhoud minder toegankelijk wordt gemaakt.

4. GEVOLGEN VOOR DE BEGROTING

Het voorstel voor een verordening heeft geen gevolgen voor de begroting van de Unie.

5. OVERIGE ELEMENTEN

5.1. Uitvoeringsplanning en regelingen betreffende monitoring, evaluatie en rapportage

De Commissie zal binnen [één jaar na de datum waarop deze verordening van toepassing wordt] een gedetailleerd programma vaststellen voor de monitoring van de outputs, resultaten

en effecten van deze verordening. Het monitoringprogramma stelt de indicatoren vast en de middelen waarmee en de tijdstippen waarop gegevens en ander noodzakelijk bewijsmateriaal zullen 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 te evalueren.

Op basis van het vastgestelde monitoringprogramma zal de Commissie binnen twee jaar na de inwerkingtreding van deze verordening verslag uitbrengen over de uitvoering van deze verordening op basis van de door de bedrijven gepubliceerde transparantieverslagen en de door de lidstaten verstrekte informatie. De Commissie zal ten vroegste vier jaar na de inwerkingtreding van de verordening een evaluatie verrichten.

Op basis van de bevindingen van de evaluatie, onder meer of bepaalde lacunes of kwetsbaarheden blijven bestaan, en rekening houdend met de technologische ontwikkelingen, zal de Commissie nagaan of het toepassingsgebied van de verordening moet worden uitgebreid. Zo nodig zal de Commissie voorstellen indienen om deze verordening aan te passen.

De Commissie zal de uitvoering, monitoring en evaluatie van de verordening ondersteunen via een deskundigengroep van de Commissie. De groep zal ook de samenwerking tussen aanbieders van hostingdiensten, rechtshandhavingsautoriteiten en Europol faciliteren, uitwisselingen en praktijken bevorderen om terroristische inhoud op te sporen en te verwijderen, zijn deskundigheid inzake de ontwikkeling van de modus operandi van terroristen op het internet ter beschikking stellen en, waar passend, advies en richtsnoeren verstrekken met het oog op de uitvoering van de bepalingen.

De uitvoering van de voorgestelde verordening kan worden gefaciliteerd door middel van een aantal ondersteunende maatregelen. Daarbij gaat het onder meer om de mogelijke ontwikkeling van een platform binnen Europol om bijstand te verlenen in de coördinatie van doorverwijzingen en verwijderingsbevelen. Door de EU gefinancierd onderzoek over de ontwikkeling van de modus operandi van terroristen vergroot het inzicht en de kennis van alle belanghebbenden. Daarnaast ondersteunt Horizon 2020 onderzoek met het oog op de ontwikkeling van nieuwe technologieën, bijvoorbeeld om het uploaden van terroristische inhoud automatisch te voorkomen. Voorts zal de Commissie blijven analyseren hoe bevoegde autoriteiten en aanbieders van hostingdiensten bij de uitvoering van deze verordening kunnen worden ondersteund met financieringsinstrumenten van de EU.

5.2. Artikelsgewijze toelichting

Artikel 1 beschrijft het onderwerp en geeft aan dat de verordening regels vaststelt om te voorkomen dat hostingdiensten worden misbruikt voor de verspreiding van terroristische online-inhoud, met inbegrip van zorgplichten voor aanbieders van hostingdiensten en door de lidstaten te nemen maatregelen. Het vermeldt ook het geografische toepassingsgebied, namelijk aanbieders van hostingdiensten die diensten aanbieden in de Unie, ongeacht hun plaats van vestiging.

Artikel 2 bevat definities van in het voorstel gebruikte termen. Het voorziet ook in een definitie van terroristische inhoud met het oog op preventie, die gebaseerd is op de richtlijn inzake terrorismebestrijding zodat zij slaat op materiaal en informatie die aanzetten tot het plegen van terroristische misdrijven of het bijdragen aan terroristische misdrijven, of dit

aanmoedigen of verdedigen, die instructies geven voor het plegen van dergelijke misdrijven of het deelnemen aan de activiteiten van een terroristische groepering bevorderen.

Artikel 3 voorziet in zorgplichten die aanbieders van hostingdiensten moeten nakomen wanneer zij overeenkomstig deze verordening maatregelen nemen, en met name om de betrokken grondrechten naar behoren te eerbiedigen. Het voorziet in passende bepalingen die in de voorwaarden van aanbieders van hostingdiensten moeten worden opgenomen en die vervolgens moeten worden toegepast.

Artikel 4 bepaalt dat de lidstaten de bevoegde autoriteiten de bevoegdheid moeten verlenen om verwijderingsbevelen uit te vaardigen, en vereist dat dienstverleners binnen één uur na ontvangst van een verwijderingsbevel inhoud verwijderen. Het bepaalt ook de elementen die verwijderingsbevelen ten minste moeten bevatten, en stelt de procedures vast die aanbieders van hostingdiensten moeten volgen om feedback te geven aan de uitvaardigende autoriteit, of om die autoriteit ervan in kennis te stellen dat het niet mogelijk is aan het bevel te voldoen of als verdere verduidelijking nodig is. Het vereist ook dat de autoriteit die toeziet op proactieve maatregelen van de lidstaat die rechtsmacht heeft ten aanzien van de aanbieder van hostingdiensten, door de uitvaardigende autoriteit in kennis wordt gesteld.

Artikel 5 bepaalt dat aanbieders van hostingdiensten maatregelen moeten nemen om inhoud die door een bevoegde autoriteit in een lidstaat of een orgaan van de Unie is doorverwezen, zo snel mogelijk te beoordelen, echter zonder de verplichting op te leggen de betrokken inhoud te verwijderen en zonder specifieke termijnen voor actie vast te stellen. Dit artikel bepaalt ook de elementen die doorverwijzingen ten minste moeten bevatten, en stelt de procedures vast die aanbieders van hostingdiensten moeten volgen om feedback te geven aan de uitvaardigende autoriteit, of om de autoriteit die de inhoud heeft doorverwezen om verduidelijking te verzoeken.

Artikel 6 verplicht aanbieders van hostingdiensten, waar passend, doeltreffende en evenredige proactieve maatregelen te nemen. Het voorziet in een procedure die garandeert dat bepaalde aanbieders van hostingdiensten (d.w.z. die welke een definitief geworden verwijderingsbevel hebben ontvangen) zo nodig aanvullende proactieve maatregelen nemen om de risico's te beperken naargelang de blootstelling aan terroristische inhoud op hun diensten. De aanbieder van hostingdiensten moet met de bevoegde autoriteit samenwerken met betrekking tot de noodzakelijke maatregelen die moeten worden genomen; indien geen overeenstemming kan worden bereikt, kan de autoriteit de aanbieder van hostingdiensten maatregelen opleggen. Het artikel voorziet ook in een toetsingsprocedure met betrekking tot het besluit van de autoriteit.

Krachtens artikel 7 moeten aanbieders van hostingdiensten gedurende zes maanden verwijderde inhoud en bijbehorende gegevens bewaren met het oog op toetsingsprocedures en voor onderzoeksdoeleinden. Deze termijn kan worden verlengd als de toetsing nog niet is afgerond. Dit artikel verplicht aanbieders van hostingdiensten ook om waarborgen in te voeren om te garanderen dat bewaarde inhoud en bijbehorende houdende gegevens niet om andere doeleinden worden geraadpleegd of verwerkt.

Artikel 8 voorziet in een verplichting voor aanbieders van hostingdiensten om hun beleid ter bestrijding van terroristische inhoud toe te lichten en jaarlijkse transparantieverslagen over de in dit verband genomen maatregelen te publiceren.

Artikel 9 voorziet in specifieke waarborgen voor het gebruik en de uitvoering van proactieve maatregelen wanneer automatische instrumenten worden gebruikt om ervoor te zorgen dat besluiten correct en goed onderbouwd zijn.

Artikel 10 verplicht aanbieders van hostingdiensten om klachtenmechanismen voor verwijderingen, doorverwijzingen en proactieve maatregelen in te voeren en elke klacht snel te onderzoeken.

Artikel 11 verplicht aanbieders van hostingdiensten om aan de aanbieder van inhoud informatie over de verwijdering beschikbaar te stellen, tenzij de bevoegde autoriteit om redenen van openbare veiligheid voorschrijft dat die informatie niet openbaar mag worden gemaakt.

Artikel 12 verplicht de lidstaten ervoor te zorgen dat de bevoegde autoriteiten over voldoende capaciteit en middelen beschikken om hun verantwoordelijkheden uit hoofde van deze verordening te kunnen nakomen.

Artikel 13 verplicht de lidstaten onderling en, in voorkomend geval, met Europol samen te werken om dubbel werk en inmenging in onderzoeken te voorkomen. Het artikel voorziet ook in de mogelijkheid voor lidstaten en aanbieders van hostingdiensten om gebruik te maken van speciale instrumenten, waaronder die van Europol, voor de verwerking van en de feedback over verwijderingsbevelen en doorverwijzingen, en voor de samenwerking in verband met proactieve maatregelen. Het artikel legt de lidstaten ook op over passende communicatiekanalen te beschikken om ervoor te zorgen dat informatie tijdig wordt uitgewisseld in het kader van de toepassing en handhaving van de bepalingen van deze verordening. Het artikel verplicht ook de aanbieders van hostingdiensten om de betrokken autoriteiten in te lichten wanneer zij kennis hebben van bewijs van terroristische misdrijven in de zin van artikel 3 van Richtlijn (EU) 2017/541 inzake terrorismebestrijding.

Artikel 14 voorziet in de aanwijzing van contactpunten, zowel door de aanbieders van hostingdiensten als door de lidstaten, om hun onderlinge communicatie te vergemakkelijken, met name met betrekking tot doorverwijzingen en verwijderingsbevelen.

Artikel 15 stelt de rechtsmacht van de lidstaten vast met het oog op het toezicht op proactieve maatregelen, het opleggen van sancties en het monitoren van de inspanningen.

Artikel 16 vereist dat aanbieders van hostingdiensten die geen vestiging hebben in een lidstaat maar wel diensten aanbieden in de Unie, een wettelijke vertegenwoordiger in de Unie aanwijzen.

Op grond van artikel 17 moeten de lidstaten autoriteiten aanwijzen voor het uitvaardigen van verwijderingsbevelen, voor het doorverwijzen van terroristische inhoud, voor het toezicht op de uitvoering van proactieve maatregelen en voor de handhaving van de verordening.

Artikel 18 bepaalt dat de lidstaten regels inzake sancties bij niet-naleving moeten vaststellen, en voorziet in criteria waarmee de lidstaten rekening moeten houden bij het bepalen van het soort en de hoogte van de sancties. Gezien het bijzondere belang van snelle verwijdering van terroristische inhoud die in een verwijderingsbevel geïdentificeerd is, moeten specifieke regels worden vastgesteld inzake financiële sancties bij systematische inbreuken op dit vereiste.

Artikel 19 voorziet in een snellere en flexibelere procedure voor de wijziging van de modellen die voor verwijderingsbevelen en geauthenticeerde indieningskanalen worden verstrekt, door middel van gedelegeerde handelingen.

Artikel 20 stelt de voorwaarden vast waaronder de Commissie gedelegeerde handelingen kan vaststellen om te voorzien in de nodige wijzigingen van de modellen en technische vereisten voor verwijderingsbevelen.

Artikel 21 vereist dat de lidstaten specifieke informatie verzamelen en rapporteren met betrekking tot de toepassing van de verordening, teneinde de Commissie bij te staan in de uitoefening van haar taken uit hoofde van artikel 23. De Commissie stelt een gedetailleerd programma vast voor de monitoring van de outputs, resultaten en effecten van deze verordening.

In artikel 22 wordt bepaald dat de Commissie twee jaar na de inwerkingtreding van deze verordening verslag uitbrengt over de uitvoering ervan.

In artikel 23 wordt bepaald dat de Commissie ten vroegste drie jaar na de inwerkingtreding van deze verordening verslag uitbrengt over de evaluatie ervan.

Artikel 24 bepaalt dat de voorgestelde verordening in werking zal treden op de twintigste dag na de bekendmaking ervan in het Publicatieblad en van toepassing zal zijn zes maanden na de datum van haar inwerkingtreding. Deze termijn wordt voorgesteld rekening houdend met het feit dat uitvoeringsmaatregelen nodig zijn, terwijl tegelijkertijd wordt erkend dat de volledige toepassing van de regels van de voorgestelde verordening dringend is. De termijn van zes maanden is vastgesteld op basis van de aanname dat de onderhandelingen snel zullen verlopen.

2018/0331 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

ter voorkoming van de verspreiding van terroristische online-inhoud

Een bijdrage van de Europese Commissie aan de bijeenkomst van de EU-leiders in Salzburg op 19-20 september 2018

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[6],

Handelend volgens de gewone wetgevingsprocedure,

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 te voorkomen. 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 onlineomgeving te vergroten en de waarborgen voor de vrijheid van meningsuiting en van informatie solider te maken.

(2) 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, hetgeen een aanzienlijke bijdrage levert aan innovatie, economische groei en het scheppen van banen in de Unie. Hun diensten worden echter in bepaalde gevallen door derden misbruikt om illegale activiteiten online uit te voeren. Bijzonder zorgwekkend is het misbruik van aanbieders van hostingdiensten door terroristische groeperingen en hun aanhangers om terroristische online-inhoud te verspreiden en hun boodschap uit te dragen, te radicaliseren en te werven en terroristische activiteiten te faciliteren en aan te sturen.

(3) De aanwezigheid van terroristische online-inhoud heeft ernstige negatieve gevolgen voor de gebruikers, de burgers en de samenleving in het algemeen alsook voor de aanbieders van onlinediensten die dergelijke inhoud hosten, omdat hierdoor het

[6] PB C […] van […], blz. […].

vertrouwen van hun gebruikers wordt ondermijnd en hun bedrijfsmodellen worden geschaad. Aanbieders van onlinediensten 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 de bestrijding van terroristische inhoud die via hun diensten wordt verspreid.

(4) De inspanningen op het niveau van de Unie om terroristische online-inhoud te bestrijden, die in 2015 begonnen met een kader voor vrijwillige samenwerking tussen lidstaten en aanbieders van hostingdiensten, moeten worden aangevuld met een duidelijk wetgevingskader teneinde terroristische online-inhoud nog minder toegankelijk te maken en een snel om zich heen grijpend probleem adequaat aan te pakken. Dit wetgevingskader wil voortbouwen op de vrijwillige inspanningen, die zijn versterkt door Aanbeveling (EU) 2018/334 van de Commissie[7], en is een reactie op de oproep van het Europees Parlement om de maatregelen tegen illegale en schadelijke inhoud aan te scherpen, en de oproep van de Europese Raad om de automatische detectie en verwijdering van inhoud die tot terroristische daden aanzet, te verbeteren.

(5) De toepassing van deze verordening mag geen afbreuk doen aan de toepassing van artikel 14 van Richtlijn 2000/31/EG[8]. Met name mogen door de aanbieder van hostingdiensten in overeenstemming met deze verordening genomen maatregelen, waaronder alle proactieve maatregelen, op zich niet ertoe leiden dat die dienstverlener de vrijstelling van aansprakelijkheid verliest waarin die bepaling voorziet. Deze verordening laat de bevoegdheden van nationale autoriteiten en rechterlijke instanties onverlet om aanbieders van hostingdiensten aansprakelijk te stellen in specifieke gevallen waarin niet is voldaan aan de in artikel 14 van Richtlijn 2000/31/EG vastgestelde voorwaarden voor vrijstelling van aansprakelijkheid.

(6) De regels ter voorkoming van het misbruik van hostingdiensten voor de verspreiding van terroristische online-inhoud teneinde de goede werking van de interne markt te waarborgen, worden in deze verordening vastgesteld met volledige eerbiediging van de grondrechten die zijn beschermd in de rechtsorde van de Unie, en meer bepaald die welke zijn verankerd in het Handvest van de grondrechten van de Europese Unie.

(7) Deze verordening draagt bij aan de bescherming van de openbare veiligheid en creëert passende en solide waarborgen om de bescherming van de grondrechten in kwestie te garanderen. Dit omvat het recht op eerbiediging van het privéleven en de bescherming van persoonsgegevens, het recht op doeltreffende rechtsbescherming, het recht op vrijheid van meningsuiting, waaronder de vrijheid kennis te nemen en te geven van informatie, de vrijheid van ondernemerschap en het beginsel van non-discriminatie. De bevoegde autoriteiten en de aanbieders van hostingdiensten mogen alleen maatregelen vaststellen die noodzakelijk, passend en evenredig zijn in een democratische samenleving, waarbij zij rekening houden met het bijzondere belang dat wordt gehecht aan de vrijheid van meningsuiting en van informatie, die één van de essentiële fundamenten van een pluralistische, democratische samenleving is en één van de waarden waarop de Unie is gegrondvest. Maatregelen die een inmenging vormen in de vrijheid van meningsuiting en van informatie moeten strikt afgebakend

[7] 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).

[8] 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).

zijn, in die zin dat ze moeten dienen om de verspreiding van terroristische inhoud te voorkomen, maar zonder dat dit afbreuk doet aan het recht op rechtmatige wijze kennis te nemen en te geven van informatie, rekening houdend met de centrale rol van aanbieders van hostingdiensten bij het faciliteren van het publieke debat en de verspreiding en ontvangst van feiten, meningen en ideeën overeenkomstig de wet.

(8) Het recht op een doeltreffende voorziening in rechte is vastgelegd in artikel 19 VEU en artikel 47 van het Handvest van de grondrechten van de Europese Unie. 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 een negatief effect kunnen hebben op de rechten van die persoon. Het recht omvat met name de mogelijkheid voor aanbieders van hostingdiensten en aanbieders van inhoud om verwijderingsbevelen daadwerkelijk te betwisten voor de rechterlijke instantie van de lidstaat waarvan de autoriteiten het verwijderingsbevel hebben uitgevaardigd.

(9) Om duidelijkheid te verschaffen over de maatregelen die zowel aanbieders van hostingdiensten als bevoegde autoriteiten moeten nemen om de verspreiding van terroristische online-inhoud te voorkomen, moet deze verordening een definitie van terroristische inhoud vaststellen met het oog op preventieve doeleinden, op basis van de definitie van terroristische misdrijven van Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad[9]. Omdat de schadelijkste terroristische onlinepropaganda moet worden aangepakt, moet de definitie slaan op materiaal en informatie die aanzetten tot het plegen van terroristische misdrijven of het bijdragen aan terroristische misdrijven, of dit aanmoedigen of verdedigen, die instructies geven voor het plegen van dergelijke misdrijven of het deelnemen aan activiteiten van een terroristische groepering bevorderen. Dergelijke informatie omvat met name tekst, beelden, geluidsopnamen en videobestanden. Bij de beoordeling of inhoud terroristische inhoud is in de zin van deze verordening, moeten bevoegde autoriteiten en aanbieders van hostingdiensten rekening houden met factoren zoals de aard en de formulering van de verklaringen, de context waarin de verklaringen zijn afgelegd en hun potentieel om schadelijke gevolgen teweeg te brengen, waardoor de veiligheid van personen in gevaar komt. Het feit dat het materiaal geproduceerd is door, toe te rekenen is aan of verspreid is namens een terroristische organisatie of persoon die op de EU-terroristenlijst is geplaatst, is een belangrijke factor in de beoordeling. Inhoud die voor educatieve, journalistieke of onderzoeksdoeleinden wordt verspreid, moet adequaat worden beschermd. Voorts mag de uiting van radicale, polemische of controversiële standpunten in het publieke debat over gevoelige politieke vraagstukken niet als terroristische inhoud worden beschouwd.

(10) Om van toepassing te zijn op onlinehostingdiensten waarop terroristische inhoud wordt verspreid, moet deze verordening van toepassing zijn op diensten van de informatiemaatschappij die op verzoek van een afnemer van de dienst door hem verstrekte informatie opslaan en de opgeslagen informatie aan derden beschikbaar stellen, ongeacht of deze activiteit louter technisch, automatisch en passief is. Dergelijke aanbieders van diensten van de informatiemaatschappij omvatten bijvoorbeeld socialemediaplatforms, videostreamingdiensten, diensten voor het delen van video- en audiobestanden en beelden, bestandsdeling en andere clouddiensten in

[9] 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).

zoverre daarmee de informatie aan derden beschikbaar wordt gesteld, en websites waarop gebruikers opmerkingen of beoordelingen kunnen posten. De verordening moet ook van toepassing zijn op aanbieders van hostingdiensten die buiten de Unie zijn gevestigd maar diensten aanbieden in de Unie, aangezien een aanzienlijk deel van de aanbieders van hostingdiensten die aan terroristische inhoud op hun diensten zijn blootgesteld, in derde landen gevestigd zijn. Dit moet ervoor zorgen dat alle ondernemingen die in de digitale eengemaakte markt actief zijn, dezelfde vereisten moeten naleven, ongeacht het land van vestiging. Om te bepalen of een dienstverlener diensten aanbiedt in de Unie, moet worden nagegaan of de dienstverlener rechtspersonen of natuurlijke personen in een of meer lidstaten in staat stelt om zijn diensten te gebruiken. De loutere toegankelijkheid van de website van een dienstverlener of van een e-mailadres en van andere contactgegevens in een of meer lidstaten mag op zich echter niet volstaan als voorwaarde voor de toepassing van deze verordening.

(11) Een wezenlijke band met de Unie moet relevant zijn om het toepassingsgebied van deze verordening te bepalen. Deze wezenlijke band met de Unie moet worden geacht te bestaan wanneer de dienstverlener een vestiging in de Unie heeft of, als dat niet het geval is, op basis van het bestaan van een aanzienlijk aantal gebruikers in een of meer lidstaten, of het richten van activiteiten op een of meer lidstaten. Of de activiteiten op een of meer lidstaten zijn gericht, kan worden bepaald aan de hand van alle relevante omstandigheden, waaronder factoren zoals het gebruik van een taal of een munteenheid die in die lidstaat algemeen gangbaar is, of de mogelijkheid goederen of diensten te bestellen. Dat de activiteiten op een lidstaat zijn gericht, kan ook blijken uit de beschikbaarheid van een applicatie in de desbetreffende nationale applicationstore, het maken van lokale reclame of reclame in de taal die in die lidstaat gangbaar is, of het beheren van klantenrelaties, bijvoorbeeld door het aanbieden van een klantenservice in de taal die in die lidstaat algemeen gangbaar is. Een wezenlijke band moet ook worden aangenomen wanneer een dienstverlener zijn activiteiten op een of meer lidstaten richt zoals bepaald in artikel 17, lid 1, onder c), van Verordening (EG) nr. 1215/2012 van het Europees Parlement en de Raad[10]. Anderzijds kan het verlenen van de dienst met het oog op de loutere naleving van het discriminatieverbod dat in Verordening (EU) nr. 2018/302 van het Europees Parlement en de Raad[11] is neergelegd, op die grond alleen niet worden beschouwd als het richten van activiteiten op een bepaald grondgebied in de Unie.

(12) Aanbieders van hostingdiensten moeten bepaalde zorgplichten nakomen om de verspreiding van terroristische inhoud op hun diensten te voorkomen. Deze zorgplichten mogen niet neerkomen op een algemene toezichtverplichting. Zorgplichten moeten inhouden dat aanbieders van hostingdiensten bij de toepassing van deze verordening op zorgvuldige, evenredige en niet-discriminerende wijze moeten handelen ten aanzien van inhoud die zij opslaan, met name wanneer zij hun eigen voorwaarden toepassen, teneinde te voorkomen dat inhoud wordt verwijderd die

[10] 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).

[11] 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 601 van 2.3.2018, blz. 1).

geen terroristische inhoud is. De verwijdering of het onmogelijk maken van de toegang moet plaatsvinden met eerbiediging van de vrijheid van meningsuiting en van informatie.

(13) De procedure en verplichtingen die voortvloeien uit wettelijke bevelen waarin aanbieders van hostingdiensten na een beoordeling door de bevoegde autoriteiten wordt gevraagd terroristische inhoud te verwijderen of de toegang daartoe onmogelijk te maken, moeten worden geharmoniseerd. De lidstaten moeten vrij blijven in de keuze van de bevoegde autoriteiten en kunnen administratieve instanties, rechtshandhavingsautoriteiten of rechterlijke instanties met deze taak belasten. Gezien de snelheid waarmee terroristische inhoud via onlinediensten wordt verspreid, legt deze bepaling aanbieders van hostingdiensten de verplichting op te garanderen dat in het verwijderingsbevel geïdentificeerde terroristische inhoud binnen één uur na ontvangst van het verwijderingsbevel wordt verwijderd of dat de toegang daartoe onmogelijk wordt gemaakt. Het zijn de aanbieders van hostingdiensten die besluiten of zij de inhoud in kwestie verwijderen of de toegang daartoe onmogelijk maken voor gebruikers in de Unie.

(14) De bevoegde autoriteit moet het verwijderingsbevel rechtstreeks aan de geadresseerde en het contactpunt zenden met elektronische middelen die een schriftelijk bewijs kunnen genereren op zodanige wijze dat de dienstverlener de authenticiteit kan vaststellen, met vermelding van de datum en het tijdstip van verzending en ontvangst van het bevel, bijvoorbeeld via beveiligde e-mail en platformen of andere beveiligde kanalen, met inbegrip van die welke door de dienstverlener beschikbaar worden gesteld, overeenkomstig de regels inzake de bescherming van persoonsgegevens. Dit vereiste kan met name worden nageleefd 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[12].

(15) Doorverwijzingen door de bevoegde autoriteiten of Europol vormen een doeltreffende en snelle manier om aanbieders van hostingdiensten bewust te maken van specifieke inhoud op hun diensten. Dit mechanisme 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 voorwaarden, moet beschikbaar blijven naast de verwijderingsbevelen. Het is van belang dat aanbieders van hostingdiensten dergelijke doorverwijzingen bij voorrang beoordelen en snel feedback geven over de genomen maatregelen. Het blijft de aanbieder van hostingdiensten die uiteindelijk besluit of hij inhoud al dan niet verwijdert omdat die niet verenigbaar is met zijn voorwaarden. Bij de uitvoering van deze verordening met betrekking tot doorverwijzingen blijft het mandaat van Europol overeenkomstig Verordening (EU) 2016/794[13] onverlet.

(16) Gezien de omvang en snelheid die nodig zijn om terroristische inhoud doeltreffend te identificeren en te verwijderen, zijn evenredige proactieve maatregelen, onder meer met gebruikmaking van automatische middelen in bepaalde gevallen, een essentieel

---

12 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).

13 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).

onderdeel in de strijd tegen terroristische online-inhoud. Om terroristische inhoud op hun diensten minder toegankelijk te maken, moeten aanbieders van hostingdiensten beoordelen of het passend is proactieve maatregelen te nemen, afhankelijk van de risico's en de mate van blootstelling aan terroristische inhoud alsook van de gevolgen voor de rechten van derden en het publieke belang van informatie. Bijgevolg moeten aanbieders van hostingdiensten bepalen welke passende, doeltreffende en evenredige proactieve maatregelen moeten worden genomen. Dit vereiste mag niet neerkomen op een algemene toezichtverplichting. In het kader van deze beoordeling wijzen de afwezigheid van aan een aanbieder van hostingdiensten gerichte verwijderingsbevelen en doorverwijzingen op een lage mate van blootstelling aan terroristische inhoud.

(17) Bij het invoeren van proactieve maatregelen moeten aanbieders van hostingdiensten ervoor zorgen dat het recht van gebruikers op vrijheid van meningsuiting en van informatie - waaronder het vrij kennis nemen en geven van informatie - behouden blijft. Aanbieders van hostingdiensten moeten niet alleen alle in de wet neergelegde vereisten naleven, waaronder de wetgeving inzake de bescherming van persoonsgegevens, maar ook de nodige zorgvuldigheid aan de dag leggen en waarborgen instellen, onder meer met name menselijk toezicht en menselijke verificatie, waar passend, om onbedoelde en onterechte besluiten te voorkomen die leiden tot de verwijdering van inhoud die geen terroristische inhoud is. Dit is bijzonder relevant wanneer aanbieders van hostingdiensten automatische middelen gebruiken om terroristische inhoud op te sporen. Elk besluit om automatische middelen te gebruiken, ongeacht of dit wordt genomen door de aanbieder van hostingdiensten zelf of op verzoek van de bevoegde autoriteit, moet worden beoordeeld rekening houdend met de betrouwbaarheid van de onderliggende technologie en het daaruit voortvloeiende effect op de grondrechten.

(18) Om ervoor te zorgen dat aanbieders van hostingdiensten die aan terroristische inhoud worden blootgesteld, passende maatregelen nemen om misbruik van hun diensten te voorkomen, moeten de bevoegde autoriteiten aanbieders van hostingdiensten die een verwijderingsbevel hebben ontvangen dat definitief is geworden, verzoeken verslag uit te brengen over de genomen proactieve maatregelen. Deze kunnen bestaan uit maatregelen om te voorkomen dat terroristische inhoud die is verwijderd of waartoe de toegang onmogelijk is gemaakt als gevolg van een verwijderingsbevel dat of een doorverwijzing die de aanbieder van hostingdiensten heeft ontvangen, opnieuw wordt geüpload, door gebruik te maken van publieke of particuliere instrumenten waarmee die inhoud kan worden vergeleken met bekende terroristische inhoud. Zij kunnen ook gebruikmaken van betrouwbare technische instrumenten om nieuwe terroristische inhoud te identificeren, hetzij op de markt beschikbare instrumenten hetzij instrumenten die de aanbieder van hostingdiensten zelf heeft ontwikkeld. De dienstverlener moet verslag uitbrengen over de specifieke proactieve maatregelen zodat de bevoegde autoriteit kan beoordelen of de maatregelen doeltreffend en evenredig zijn en of, indien automatische middelen worden gebruikt, de aanbieder van hostingdiensten over de nodige capaciteiten beschikt voor menselijk toezicht en menselijke verificatie. Bij het beoordelen van de doeltreffendheid en evenredigheid van de maatregelen moeten de bevoegde autoriteiten rekening houden met relevante parameters, waaronder het aantal aan de aanbieder gerichte verwijderingsbevelen en doorverwijzingen, zijn economische draagkracht en het effect van zijn dienst in de verspreiding van terroristische inhoud (bijvoorbeeld rekening houdend met het aantal gebruikers in de Unie).

(19) Na het verzoek moet de bevoegde autoriteit een dialoog aangaan met de aanbieder van hostingdiensten over de nodige proactieve maatregelen die moeten worden genomen. Zo nodig moet de bevoegde autoriteit het nemen van passende, doeltreffende en evenredige proactieve maatregelen opleggen wanneer zij van oordeel is dat de genomen maatregelen niet volstaan om de risico's aan te pakken. Een besluit om dergelijke specifieke proactieve maatregelen op te leggen mag in beginsel niet leiden tot het opleggen van een algemene toezichtverplichting, zoals bepaald in artikel 15, lid 1, van Richtlijn 2000/31/EG. Gezien de bijzonder ernstige risico's die met de verspreiding van terroristische inhoud gepaard gaan, kunnen de door de bevoegde autoriteiten op grond van deze verordening genomen besluiten afwijken van de aanpak die in artikel 15, lid 1, van Richtlijn 2000/31/EG is vastgesteld, wat betreft bepaalde specifieke, gerichte maatregelen die moeten worden genomen om dwingende redenen van openbare veiligheid. Alvorens dergelijke besluiten te nemen, moet de bevoegde autoriteit een billijke afweging maken tussen de doelstellingen van openbaar belang en de betrokken grondrechten, waaronder met name de vrijheid van meningsuiting en van informatie en de vrijheid van ondernemerschap, en een passende motivering verstrekken.

(20) De verplichting voor aanbieders van hostingdiensten om verwijderde inhoud en bijbehorende gegevens te bewaren, moet worden vastgesteld voor specifieke doeleinden en beperkt zijn in de tijd tot wat nodig is. Het vereiste van bewaring moet worden uitgebreid tot de bijbehorende gegevens, in zoverre dat die gegevens anders verloren zouden gaan als gevolg van de verwijdering van de betrokken inhoud. Bijbehorende gegevens kunnen "gegevens betreffende de abonnee" zijn, waaronder met name gegevens betreffende de identiteit van de aanbieder van inhoud, alsook "gegevens betreffende toegang", waaronder bijvoorbeeld gegevens over de datum en het tijdstip van gebruik door de aanbieder van inhoud of het aanmelden bij en uitloggen uit de dienst, samen met het IP-adres dat door de aanbieder van internettoegang aan de aanbieder van inhoud wordt toegekend.

(21) De verplichting tot bewaring van de inhoud met het oog op procedures van administratieve of rechterlijke toetsing is noodzakelijk en gerechtvaardigd om te garanderen dat de aanbieder van inhoud wiens inhoud is verwijderd of tot wiens inhoud de toegang onmogelijk is gemaakt, over doeltreffende rechtsmiddelen beschikt, en dat die inhoud wordt hersteld in de staat van vóór de verwijdering afhankelijk van de uitkomst van de toetsingsprocedure. De verplichting tot bewaring van inhoud met het oog op onderzoek en vervolging is gerechtvaardigd en noodzakelijk in het licht van de waarde die dit materiaal kan hebben voor het verstoren of voorkomen van terroristische activiteiten. Wanneer ondernemingen materiaal verwijderen of de toegang daartoe onmogelijk maken, met name door middel van hun eigen proactieve maatregelen, en de bevoegde autoriteit niet inlichten omdat zij van mening zijn dat dit niet onder artikel 13, lid 4, van deze verordening valt, kan de rechtshandhaving geen kennis hebben van het bestaan van de inhoud. Daarom is de bewaring van inhoud ook gerechtvaardigd met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven. Voor deze doeleinden is de vereiste bewaring van gegevens beperkt tot gegevens die waarschijnlijk verband houden met terroristische misdrijven, en kan zij derhalve bijdragen tot het vervolgen van terroristische misdrijven of tot het voorkomen van ernstige risico's voor de openbare veiligheid.

(22) Met het oog op de evenredigheid moet de bewaringstermijn worden beperkt tot zes maanden om de aanbieders van inhoud voldoende tijd te geven om het toetsingsproces in te leiden, en de rechtshandhaving toegang te bieden tot relevante gegevens voor het

onderzoek naar en de vervolging van terroristische misdrijven. Deze termijn kan echter worden verlengd met de termijn die nodig is ingeval de toetsingsprocedure is ingeleid doch niet binnen de termijn van zes maanden is afgerond, en dit op verzoek van de autoriteit die de toetsing verricht. Die duur moet volstaan om de rechtshandhavingsautoriteiten in staat te stellen het nodige bewijsmateriaal in verband met het onderzoek te bewaren, terwijl het evenwicht met de betrokken grondrechten wordt gegarandeerd.

(23) Deze verordening heeft geen gevolgen voor de procedurele waarborgen en procedurele onderzoeksmaatregelen in verband met de 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 nationale recht van de lidstaten en in de wetgeving van de Unie.

(24) 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 moeten jaarlijkse transparantieverslagen publiceren met nuttige informatie over de maatregelen die zijn genomen met betrekking tot de opsporing, identificatie en verwijdering van terroristische inhoud.

(25) Klachtenprocedures zijn een noodzakelijke waarborg tegen onterechte verwijdering van inhoud die op grond van de vrijheid van meningsuiting en van informatie beschermd is. Aanbieders van hostingdiensten moeten dan ook gebruiksvriendelijke klachtenmechanismen instellen en ervoor zorgen dat klachten onmiddellijk en met volledige transparantie voor de aanbieder van inhoud worden behandeld. Het vereiste dat de aanbieder van hostingdiensten de inhoud moet herstellen wanneer die ten onrechte is verwijderd, laat de mogelijkheid onverlet dat aanbieders van hostingdiensten hun eigen voorwaarden op andere gronden handhaven.

(26) Doeltreffende rechtsbescherming in de zin van artikel 19 VEU en artikel 47 van het Handvest van de grondrechten van de Europese Unie vereist dat personen kunnen nagaan om welke redenen de door hen geüploade inhoud is verwijderd of de toegang daartoe onmogelijk is gemaakt. Daartoe moet de aanbieder van hostingdiensten aan de aanbieder van inhoud relevante informatie beschikbaar stellen die hem in staat stelt het besluit te betwisten. Dit hoeft echter niet noodzakelijkerwijs te bestaan in een kennisgeving aan de aanbieder van inhoud. Afhankelijk van de omstandigheden kunnen aanbieders van hostingdiensten inhoud die als terroristische inhoud wordt beschouwd, vervangen door een bericht dat die inhoud overeenkomstig deze verordening is verwijderd of dat de toegang daartoe onmogelijk is gemaakt. Op verzoek moet nadere informatie worden verstrekt over de redenen en over de mogelijkheden voor de aanbieder van inhoud om het besluit te betwisten. Wanneer de bevoegde autoriteiten besluiten dat het om redenen van openbare veiligheid, waaronder in het kader van een onderzoek, niet passend of contraproductief wordt geacht om de aanbieder van inhoud rechtstreeks in kennis te stellen van de verwijdering van inhoud of van het onmogelijk maken van de toegang daartoe, moeten zij de aanbieder van hostingdiensten daarvan in kennis stellen.

(27) Om dubbel werk en mogelijke inmenging in onderzoeken te vermijden, moeten de bevoegde autoriteiten elkaar inlichten en met elkaar, en zo nodig met Europol, coördineren en samenwerken bij het uitvaardigen van verwijderingsbevelen of het zenden van doorverwijzingen aan aanbieders van hostingdiensten. Bij de uitvoering

van de bepalingen van deze verordening kan Europol steun verlenen in overeenstemming met zijn huidige mandaat en het bestaande rechtskader.

(28) Om te garanderen dat proactieve maatregelen doeltreffend en voldoende coherent worden uitgevoerd, moeten de bevoegde autoriteiten in de lidstaten met elkaar contact houden in verband met de besprekingen die zij met aanbieders van hostingdiensten voeren over de identificatie, uitvoering en beoordeling van specifieke proactieve maatregelen. Deze samenwerking is ook nodig met betrekking tot de vaststelling van regels inzake sancties, alsook de uitvoering en de handhaving van sancties.

(29) Het is essentieel dat de bevoegde autoriteit binnen de lidstaat die voor het opleggen van sancties verantwoordelijk is, volledig wordt ingelicht over de uitvaardiging van verwijderingsbevelen en de zending van doorverwijzingen en de daaropvolgende uitwisselingen tussen de aanbieder van hostingdiensten en de betrokken bevoegde autoriteit. Daartoe moeten de lidstaten voorzien in passende communicatiekanalen en -mechanismen om relevante informatie tijdig te kunnen delen.

(30) Om snelle uitwisselingen tussen de bevoegde autoriteiten alsook met aanbieders van hostingdiensten te faciliteren, en om dubbel werk te voorkomen, kunnen de lidstaten gebruikmaken van instrumenten die door Europol zijn ontwikkeld, zoals de huidige Internet Referral Management application (IRMa) of vervolginstrumenten.

(31) Gezien de bijzonder ernstige gevolgen van bepaalde terroristische inhoud moeten aanbieders van hostingdiensten onverwijld de autoriteiten in de betrokken lidstaat of de bevoegde autoriteiten waar zij gevestigd zijn of een wettelijke vertegenwoordiger hebben, inlichten over het bestaan van bewijs van terroristische misdrijven waarvan zij kennis hebben gekregen. Met het oog op de evenredigheid is deze verplichting beperkt tot terroristische misdrijven als omschreven in artikel 3, lid 1, van Richtlijn (EU) 2017/541. De informatieverplichting komt niet neer op een verplichting voor aanbieders van hostingdiensten om dergelijk bewijsmateriaal actief te zoeken. De betrokken lidstaat is de lidstaat die rechtsmacht heeft voor het onderzoek naar en de vervolging van terroristische misdrijven overeenkomstig Richtlijn (EU) 2017/541 op grond van de nationaliteit van de dader, van het potentiële slachtoffer van het misdrijf of de doellocatie van de terroristische daad. In geval van twijfel kunnen aanbieders van hostingdiensten de informatie doorgeven aan Europol die daaraan gevolg moet geven overeenkomstig zijn mandaat, inclusief het doorzenden aan de betrokken nationale autoriteiten.

(32) De bevoegde autoriteiten in de lidstaten moeten die informatie kunnen gebruiken om onderzoeksmaatregelen te nemen waarin het recht van de lidstaten of het recht van de Unie voorziet, onder meer de uitvaardiging van een Europees bevel tot verstrekking op grond van de verordening betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken[14].

(33) Zowel de aanbieders van hostingdiensten als de lidstaten moeten contactpunten aanwijzen om de snelle behandeling van verwijderingsbevelen en doorverwijzingen te faciliteren. Anders dan de wettelijke vertegenwoordiger dient het contactpunt operationele doeleinden. Het contactpunt van de aanbieder van hostingdiensten moet bestaan uit alle speciale middelen waarmee verwijderingsbevelen en doorverwijzingen elektronisch kunnen worden ingediend en uit de technische en persoonlijke middelen om die snel te kunnen verwerken. Het contactpunt voor de aanbieder van

[14] COM(2018) 225 final.

hostingdiensten hoeft niet in de Unie te zijn gevestigd en de aanbieder van hostingdiensten is vrij om een bestaand contactpunt aan te wijzen, op voorwaarde dat dit contactpunt de functies uit hoofde van deze verordening kan uitoefenen. Om te garanderen dat terroristische inhoud wordt verwijderd of de toegang daartoe onmogelijk wordt gemaakt binnen één uur na ontvangst van een verwijderingsbevel, moeten aanbieders van hostingdiensten garanderen dat het contactpunt 24 uur per dag en zeven dagen per week bereikbaar is. 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 Unie waarin hun voorwaarden beschikbaar zijn.

(34) Aangezien er geen algemene verplichting geldt voor dienstverleners 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 zijn hoofdvestiging zich bevindt of waar hij een wettelijke vertegenwoordiger heeft aangewezen. Wanneer een andere lidstaat een verwijderingsbevel uitvaardigt, moeten zijn autoriteiten niettemin hun bevelen kunnen handhaven door middel van dwangmaatregelen van niet-bestraffende aard, zoals dwangsommen. Ten aanzien van een aanbieder van hostingdiensten die geen vestiging in de Unie heeft en geen wettelijke vertegenwoordiger aanwijst, moet elke lidstaat niettemin sancties kunnen opleggen, mits het ne bis in idem-beginsel wordt geëerbiedigd.

(35) 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.

(36) De wettelijke vertegenwoordiger moet juridisch bevoegd zijn om namens de aanbieder van hostingdiensten te handelen.

(37) Voor de toepassing van deze verordening moeten de lidstaten bevoegde autoriteiten aanwijzen. De aanwijzing van bevoegde autoriteiten vereist niet noodzakelijkerwijs de oprichting van nieuwe autoriteiten: bestaande instanties kunnen met de in deze verordening vastgestelde functies worden belast. Deze verordening verplicht tot aanwijzing van autoriteiten die bevoegd zijn voor het uitvaardigen van verwijderingsbevelen, het zenden van doorverwijzingen, het toezicht houden op proactieve maatregelen en het opleggen van sancties. Het is aan de lidstaten om te bepalen hoeveel autoriteiten zij voor deze taken wensen aan te wijzen.

(38) Sancties zijn noodzakelijk om te garanderen dat aanbieders van hostingdiensten de verplichtingen uit hoofde van deze verordening daadwerkelijk uitvoeren. De lidstaten moeten regels inzake sancties vaststellen, waar passend met inbegrip van richtsnoeren voor het opleggen van geldboeten. Met name moeten ernstige sancties worden vastgesteld ingeval de aanbieder van hostingdiensten systematisch verzuimt terroristische inhoud te verwijderen of de toegang daartoe onmogelijk te maken binnen één uur na ontvangst van een verwijderingsbevel. Een dergelijke niet-naleving in individuele gevallen kan worden bestraft met eerbiediging van het ne bis in idem-beginsel en het evenredigheidsbeginsel, waarbij in de sancties rekening wordt gehouden met systematisch verzuim. Met het oog op de rechtszekerheid moet in de verordening worden bepaald in hoeverre aan de betrokken verplichtingen sancties

kunnen worden verbonden. Sancties in geval van niet-naleving van artikel 6 mogen alleen worden toegepast met betrekking tot verplichtingen die voortvloeien uit een verzoek verslag uit te brengen krachtens artikel 6, lid 2, of een besluit tot het opleggen van aanvullende proactieve maatregelen krachtens artikel 6, lid 4. Bij het bepalen of er al dan niet financiële sancties moeten worden opgelegd, moet naar behoren rekening worden gehouden met de financiële draagkracht van de aanbieder. De lidstaten zorgen ervoor dat sancties niet aanmoedigen dat inhoud wordt verwijderd die geen terroristische inhoud is.

(39) Het gebruik van gestandaardiseerde modellen faciliteert samenwerking en de uitwisseling van informatie tussen bevoegde autoriteiten en dienstverleners, doordat zij sneller en doeltreffender kunnen communiceren. Het is van bijzonder belang dat na de ontvangst van een verwijderingsbevel snelle actie gegarandeerd is. Modellen verminderen de vertaalkosten en dragen bij aan een hoge kwaliteitsnorm. Ook de antwoordformulieren moeten een gestandaardiseerde uitwisseling van informatie mogelijk maken, wat bijzonder belangrijk is als dienstverleners niet aan een bevel kunnen voldoen. Geauthenticeerde kanalen voor indiening kunnen de authenticiteit van het verwijderingsbevel garanderen, met inbegrip van de datum en het tijdstip van verzending en ontvangst van het bevel.

(40) 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 gedelegeerd om overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie handelingen vast te stellen tot wijziging van de bijlagen I, II en III bij deze verordening. Om rekening te kunnen houden met technologische ontwikkelingen en de ontwikkeling van het rechtskader terzake, 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[15]. 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 gedelegeerde handelingen.

(41) De lidstaten moeten informatie verzamelen over de uitvoering van de wetgeving. 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 wetgeving kunnen worden meegenomen.

(42) Op basis van de bevindingen en conclusies in het uitvoeringsverslag en de uitkomst van de monitoringexercitie moet de Commissie ten vroegste drie jaar na de inwerkingtreding van deze verordening een evaluatie ervan uitvoeren. De evaluatie moet gebaseerd zijn op de volgende vijf criteria: doelmatigheid, doeltreffendheid, relevantie, samenhang en meerwaarde van de EU. De werking van de verschillende

[15] PB L 123 van 12.5.2016, blz. 1.

operationele en technische maatregelen waarin de verordening voorziet, waaronder de doeltreffendheid van de maatregelen om de opsporing, identificatie en verwijdering van terroristische inhoud te verbeteren, de doeltreffendheid van de waarborgmechanismen alsook de gevolgen voor mogelijk getroffen rechten en belangen van derden, moet worden beoordeeld, waarbij ook een evaluatie moet plaatsvinden van de verplichting de aanbieders van inhoud te informeren.

(43) Daar de doelstelling van deze verordening, namelijk het garanderen van de goede werking van de digitale eengemaakte markt door te voorkomen dat terroristische online-inhoud wordt verspreid, niet voldoende door de lidstaten kan worden verwezenlijkt, maar vanwege de omvang en de gevolgen van de beperking beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze 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 te voorkomen dat hostingdiensten worden misbruikt voor de verspreiding van terroristische online-inhoud. Zij stelt met name het volgende vast:

   (a) regels inzake zorgplichten die door aanbieders van hostingdiensten moeten worden nagekomen om de verspreiding van terroristische inhoud via hun diensten te voorkomen en, zo nodig, de snelle verwijdering van dergelijke inhoud te garanderen;

   (b) een reeks maatregelen die de lidstaten moeten invoeren om terroristische inhoud te identificeren, de snelle verwijdering ervan door aanbieders van hostingdiensten mogelijk te maken en de samenwerking met de bevoegde autoriteiten in andere lidstaten, aanbieders van hostingdiensten en, in voorkomend geval, betrokken organen van de Unie te faciliteren.

2. Deze verordening is van toepassing op aanbieders van hostingdiensten die diensten aanbieden in de Unie, ongeacht de plaats van hun hoofdvestiging.

Artikel 2
Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "aanbieder van hostingdiensten": een aanbieder van diensten van de informatiemaatschappij die eruit bestaan door een aanbieder van inhoud verstrekte informatie op verzoek van die aanbieder van inhoud op te slaan en de opgeslagen informatie aan derden beschikbaar te stellen;

(2) "aanbieder van inhoud": een gebruiker die informatie heeft verstrekt die in zijn opdracht wordt of was opgeslagen door een aanbieder van hostingdiensten;

(3) "in de Unie diensten aanbieden": rechtspersonen of natuurlijke personen in een of meer lidstaten in staat stellen gebruik te maken van de diensten van de aanbieder van hostingdiensten die een wezenlijke band heeft met die lidstaat of lidstaten, zoals:

(a) een vestiging van de aanbieder van hostingdiensten in de Unie;

(b) een aanzienlijk aantal gebruikers in een of meer lidstaten;

(c) een toespitsing van activiteiten op een of meer lidstaten;

(4) "terroristische misdrijven": strafbare feiten als omschreven in artikel 3, lid 1, van Richtlijn (EU) 2017/541;

(5) "terroristische inhoud": informatie die aan een of meer van de volgende voorwaarden voldoet:

(a) het aanzetten tot of het verdedigen van het plegen van terroristische misdrijven, onder meer door ze te verheerlijken, waardoor het gevaar ontstaat dat dergelijke daden worden gepleegd;

(b) het aanmoedigen van het bijdragen aan terroristische misdrijven;

(c) het bevorderen van de activiteiten van een terroristische groepering, met name door aanmoediging van het deelnemen aan of het ondersteunen van een terroristische groepering in de zin van artikel 2, lid 3, van Richtlijn (EU) 2017/541;

(d) het instrueren over methoden of technieken voor het plegen van terroristische misdrijven;

(6) "verspreiding van terroristische inhoud": het aan derden beschikbaar stellen van terroristische inhoud op de diensten van aanbieders van hostingdiensten;

(7) "voorwaarden": alle voorwaarden en clausules, ongeacht hun naam of vorm, waarin de contractuele betrekking tussen de aanbieder van hostingdiensten en zijn gebruikers wordt geregeld;

(8) "doorverwijzing": een melding door een bevoegde autoriteit of, in voorkomend geval, een bevoegd orgaan van de Unie aan een aanbieder van hostingdiensten van informatie die als terroristische inhoud kan worden beschouwd, opdat de aanbieder vrijwillig nagaat of die informatie verenigbaar is met zijn eigen voorwaarden ter voorkoming van de verspreiding van terroristische inhoud;

(9) "hoofdvestiging": het hoofdkantoor of de maatschappelijke zetel waar de voornaamste financiële functies en de operationele zeggenschap worden uitgeoefend.

AFDELING II
Maatregelen ter voorkoming van de verspreiding van terroristische online-inhoud

Artikel 3
Zorgplichten

1. Aanbieders van hostingdiensten treffen passende, redelijke en evenredige maatregelen in overeenstemming met deze verordening, tegen de verspreiding van terroristische inhoud en ter bescherming van gebruikers tegen terroristische inhoud. Daarbij handelen zij op zorgvuldige, evenredige en niet-discriminerende wijze en met inachtneming van de grondrechten van de gebruikers, en houden zij rekening

met het fundamentele belang van de vrijheid van meningsuiting en van informatie in een open en democratische samenleving.

2. Aanbieders van hostingdiensten nemen in hun voorwaarden bepalingen op ter voorkoming van de verspreiding van terroristische inhoud en passen die bepalingen toe.

Artikel 4
Verwijderingsbevelen

1. De bevoegde autoriteit heeft de bevoegdheid om een besluit uit te vaardigen op grond waarvan de aanbieder van hostingdiensten terroristische inhoud moet verwijderen of de toegang daartoe onmogelijk moet maken.

2. Aanbieders van hostingdiensten verwijderen terroristische inhoud of maken de toegang daartoe onmogelijk binnen één uur na ontvangst van het verwijderingsbevel.

3. Verwijderingsbevelen bevatten de volgende elementen overeenkomstig het model in bijlage I:

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

   (b) een motivering waarom de inhoud als terroristische inhoud wordt beschouwd, ten minste met verwijzing naar de in artikel 2, lid 5, vermelde categorieën van terroristische inhoud;

   (c) een Uniform Resource Locator (URL-adres) en, zo nodig, aanvullende informatie om de bedoelde inhoud te kunnen identificeren;

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

   (e) datum en tijdstip van uitvaardiging;

   (f) informatie over de rechtsmiddelen waarover de aanbieder van hostingdiensten en de aanbieder van inhoud beschikken;

   (g) in voorkomend geval, het besluit om geen informatie openbaar te maken over de verwijdering van terroristische inhoud of het onmogelijk maken van de toegang daartoe, als bedoeld in artikel 11.

4. Op verzoek van de aanbieder van hostingdiensten of de aanbieder van inhoud verstrekt de bevoegde autoriteit een gedetailleerde motivering, onverminderd de verplichting van de aanbieder van hostingdiensten om het verwijderingsbevel binnen de in lid 2 vastgestelde termijn na te leven.

5. De bevoegde autoriteiten zenden verwijderingsbevelen aan de hoofdvestiging van de aanbieder van hostingdiensten of aan de wettelijke vertegenwoordiger die door de aanbieder van hostingdiensten krachtens artikel 16 is aangewezen, en geven ze door aan het in artikel 14, lid 1, bedoelde contactpunt. Deze bevelen worden gezonden met 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. Aanbieders van hostingdiensten bevestigen de ontvangst en stellen de bevoegde autoriteit zonder onnodige vertraging in kennis van de verwijdering van de

terroristische inhoud of het onmogelijk maken van de toegang daartoe, met vermelding van met name het tijdstip van actie, aan de hand van het model in bijlage II.

7. Als de aanbieder van hostingdiensten het verwijderingsbevel niet kan naleven vanwege overmacht of feitelijke onmogelijkheid die hem niet kan worden toegerekend, stelt hij de bevoegde instantie zonder onnodige vertraging daarvan in kennis, met opgave van de redenen, aan de hand van het model in bijlage III. De in lid 2 vastgestelde termijn is van toepassing zodra de aangevoerde redenen niet langer bestaan.

8. Als 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 zonder onnodige vertraging daarvan in kennis en vraagt hij de nodige verduidelijking aan de hand van het model in bijlage III. De in lid 2 vastgestelde termijn is van toepassing zodra de verduidelijking is verstrekt.

9. De bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd, stelt de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit die toeziet op de uitvoering van proactieve maatregelen, in kennis wanneer het verwijderingsbevel definitief wordt. Een verwijderingsbevel wordt definitief wanneer niet binnen de overeenkomstig het toepasselijke nationale recht vastgestelde termijn een hogere voorziening is ingesteld of wanneer het na een hogere voorziening is bevestigd.

Artikel 5
Doorverwijzingen

1. De bevoegde autoriteit of het betrokken orgaan van de Unie kan een doorverwijzing zenden aan een aanbieder van hostingdiensten.

2. Aanbieders van hostingdiensten voorzien in operationele en technische maatregelen ter facilitering van de snelle beoordeling van inhoud die door bevoegde autoriteiten en, in voorkomend geval, betrokken organen van de Unie is gezonden met het oog op vrijwillige toetsing.

3. De doorverwijzing wordt gezonden aan de hoofdvestiging van de aanbieder van hostingdiensten of aan de wettelijke vertegenwoordiger die door de aanbieder van hostingdiensten krachtens artikel 16 is aangewezen, en doorgegeven aan het in artikel 14, lid 1, bedoelde contactpunt. Deze doorverwijzingen worden gezonden met elektronische middelen.

4. De doorverwijzing bevat voldoende gedetailleerde informatie, met inbegrip van de redenen waarom de inhoud als terroristische inhoud wordt beschouwd, een URL-adres en, zo nodig, aanvullende informatie om de bedoelde terroristische inhoud te kunnen identificeren.

5. De aanbieder van hostingdiensten toetst bij voorrang de in de doorverwijzing geïdentificeerde inhoud aan zijn eigen voorwaarden en besluit of hij die inhoud verwijdert dan wel de toegang daartoe onmogelijk maakt.

6. De aanbieder van hostingdiensten stelt de bevoegde autoriteit of het betrokken orgaan van de Unie snel in kennis van de uitkomst van de toetsing en van het tijdschema van de maatregelen die naar aanleiding van de doorverwijzing zijn genomen.

7. Wanneer de aanbieder van hostingdiensten van oordeel is dat de doorverwijzing onvoldoende informatie bevat om de bedoelde inhoud te toetsen, stelt hij de bevoegde autoriteiten of het betrokken orgaan van de Unie onverwijld daarvan in kennis, met vermelding van de nadere informatie of verduidelijking die hij nodig heeft.

Artikel 6
Proactieve maatregelen

1. Aanbieders van hostingdiensten nemen, waar passend, proactieve maatregelen om hun diensten te beschermen tegen de verspreiding van terroristische inhoud. De maatregelen zijn doeltreffend en evenredig, rekening houdend met het risico en de mate van blootstelling aan terroristische inhoud, de grondrechten van de gebruikers en het fundamentele belang van de vrijheid van meningsuiting en van informatie in een open en democratische samenleving.

2. In geval van een kennisgeving overeenkomstig artikel 4, lid 9, verzoekt de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit de aanbieder van hostingdiensten om binnen drie maanden na ontvangst van het verzoek en vervolgens ten minste eenmaal per jaar een verslag in te dienen over de specifieke proactieve maatregelen die hij heeft genomen, onder meer met behulp van automatische instrumenten, teneinde:

   (a) te voorkomen dat inhoud die eerder is verwijderd of waartoe de toegang onmogelijk is gemaakt omdat hij als terroristische inhoud wordt beschouwd, opnieuw wordt geüpload;

   (b) terroristische inhoud op te sporen, te identificeren en snel te verwijderen of de toegang daartoe onmogelijk te maken.

   Een dergelijk verzoek wordt gezonden aan de hoofdvestiging van de aanbieder van hostingdiensten of aan de door hem aangewezen wettelijke vertegenwoordiger.

   De verslagen bevatten alle relevante informatie aan de hand waarvan de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit kan beoordelen of de proactieve maatregelen doeltreffend en evenredig zijn, met inbegrip van een evaluatie van de werking van alle gebruikte automatische instrumenten en van de ingezette mechanismen voor menselijk toezicht en menselijke verificatie.

3. Wanneer de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit van oordeel is dat de genomen proactieve maatregelen waarover overeenkomstig lid 2 verslag is uitgebracht, niet volstaan om het risico en de mate van blootstelling te beperken en te beheersen, kan zij de aanbieder van hostingdiensten verzoeken specifieke aanvullende proactieve maatregelen te nemen. Daartoe werkt de aanbieder van hostingdiensten met de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit samen om de door hem te nemen specifieke maatregelen te bepalen en de belangrijkste doelstellingen en benchmarks alsook de termijnen voor de uitvoering daarvan vast te stellen.

4. Indien binnen drie maanden na de indiening van het verzoek krachtens lid 3 geen overeenstemming kan worden bereikt, kan de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit een besluit uitvaardigen waarbij specifieke aanvullende nodige en evenredige proactieve maatregelen worden opgelegd. In het besluit wordt met name rekening gehouden met de economische draagkracht van de aanbieder van hostingdiensten en met het effect van die maatregelen op de grondrechten van de

gebruikers en het fundamentele belang van de vrijheid van meningsuiting en van informatie. Dit besluit wordt gezonden aan de hoofdvestiging van de aanbieder van hostingdiensten of aan de door hem aangewezen wettelijke vertegenwoordiger. De aanbieder van hostingdiensten brengt regelmatig verslag uit over de uitvoering van de maatregelen zoals gespecificeerd door de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit.

5. Een aanbieder van hostingdiensten kan te allen tijde de in artikel 17, lid 1, onder c), bedoelde bevoegde autoriteit om herziening verzoeken en, waar passend, om intrekking van een verzoek of een besluit krachtens de leden 2, 3 respectievelijk 4. De bevoegde autoriteit neemt een met redenen omkleed besluit binnen een redelijke termijn na ontvangst van het verzoek van de aanbieder van hostingdiensten.

Artikel 7
Bewaring van inhoud en bijbehorende gegevens

1. Aanbieders van hostingdiensten bewaren terroristische inhoud die is verwijderd of waartoe de toegang onmogelijk is gemaakt ten gevolge van een verwijderingsbevel, een doorverwijzing of proactieve maatregelen krachtens de artikelen 4, 5 en 6, en de bijbehorende gegevens die ten gevolge van de verwijdering van de terroristische inhoud zijn verwijderd, en die nodig zijn voor:

   (a) procedures van administratieve of rechterlijke toetsing,

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

2. De in lid 1 bedoelde terroristische inhoud en bijbehorende gegevens worden gedurende zes maanden bewaard. De terroristische inhoud wordt, op verzoek van de bevoegde autoriteit of rechterlijke instantie, gedurende een langere periode bewaard wanneer en zolang het nodig is voor lopende procedures van administratieve of rechterlijke toetsing als bedoeld in lid 1, onder a).

3. Aanbieders van hostingdiensten zorgen ervoor dat voor krachtens de leden 1 en 2 bewaarde terroristische inhoud en bijbehorende gegevens passende technische en organisatorische waarborgen gelden.

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

AFDELING III
WAARBORGEN EN VERANTWOORDINGSPLICHT

Artikel 8
Transparantieverplichtingen

1. Aanbieders van hostingdiensten stellen in hun voorwaarden hun beleid ter voorkoming van de verspreiding van terroristische inhoud vast, met inbegrip van, waar passend, een zinvolle toelichting van de werking van proactieve maatregelen, waaronder het gebruik van automatische instrumenten.

2. Aanbieders van hostingdiensten publiceren jaarlijkse transparantieverslagen over de maatregelen die zijn genomen tegen de verspreiding van terroristische inhoud.

3. Transparantieverslagen bevatten ten minste de volgende informatie:

   (a) informatie over de maatregelen van de aanbieder van hostingdiensten met betrekking tot de opsporing, identificatie en verwijdering van terroristische inhoud;

   (b) informatie over de maatregelen van de aanbieder van hostingdiensten om te voorkomen dat inhoud die eerder is verwijderd of waartoe de toegang onmogelijk is gemaakt omdat hij als terroristische inhoud wordt beschouwd, opnieuw wordt geüpload;

   (c) aantal artikelen met terroristische inhoud die zijn verwijderd of waartoe de toegang onmogelijk is gemaakt naar aanleiding van verwijderingsbevelen, doorverwijzingen of proactieve maatregelen;

   (d) overzicht van de klachtenprocedures en uitkomsten daarvan.

Artikel 9

Waarborgen met betrekking tot het gebruik en de uitvoering van proactieve maatregelen

1. Wanneer aanbieders van hostingdiensten krachtens deze verordening automatische instrumenten gebruiken ten aanzien van inhoud die zij opslaan, voorzien zij in doeltreffende en passende waarborgen om te garanderen dat besluiten betreffende die inhoud, met name besluiten om inhoud die als terroristische inhoud wordt beschouwd, te verwijderen of de toegang daartoe onmogelijk maken, correct en goed onderbouwd zijn.

2. Waarborgen bestaan met name uit menselijk toezicht en menselijke verificatie, waar passend, en in elk geval wanneer een gedetailleerde beoordeling van de relevante context nodig is om te bepalen of de inhoud al dan niet als terroristische inhoud moet worden beschouwd.

Artikel 10

Klachtenmechanismen

1. Aanbieders van hostingdiensten stellen doeltreffende en toegankelijke mechanismen in waarmee aanbieders van inhoud wier inhoud is verwijderd of tot wier inhoud de toegang onmogelijk is gemaakt ten gevolge van een doorverwijzing krachtens artikel 5 of proactieve maatregelen krachtens artikel 6, tegen de maatregel van de aanbieder van hostingdiensten een klacht kunnen indienen en om het herstel van de inhoud kunnen verzoeken.

2. Aanbieders van hostingdiensten onderzoeken onmiddellijk elke door hen ontvangen klacht en herstellen de inhoud zonder onnodige vertraging indien die onterecht is verwijderd of indien de toegang daartoe onterecht onmogelijk is gemaakt. Zij stellen de klager in kennis van de uitkomst van het onderzoek.

Artikel 11

Informatie voor aanbieders van inhoud

1. Wanneer aanbieders van hostingdiensten terroristische inhoud hebben verwijderd of de toegang daartoe onmogelijk hebben gemaakt, stellen zij aan de aanbieder van

inhoud informatie beschikbaar over de verwijdering van terroristische inhoud of het onmogelijk maken van de toegang daartoe.

2. De aanbieder van hostingdiensten stelt de aanbieder van inhoud op diens verzoek in kennis van de redenen voor de verwijdering of het onmogelijk maken van de toegang en van de mogelijkheden tot betwisting van het besluit.

3. De verplichting uit hoofde van de leden 1 en 2 is niet van toepassing wanneer de bevoegde autoriteit besluit dat er geen openbaarmaking mag zijn om redenen van openbare veiligheid, zoals het voorkomen, onderzoeken, opsporen en vervolgen van terroristische misdrijven, zolang het nodig is, maar niet langer dan [vier] weken te rekenen vanaf dat besluit. In dat geval maakt de aanbieder van hostingdiensten geen informatie openbaar over de verwijdering van terroristische inhoud of het onmogelijk maken van de toegang daartoe.

AFDELING IV
Samenwerking tussen bevoegde autoriteiten, organen van de Unie en aanbieders van hostingdiensten

Artikel 12
Capaciteiten van bevoegde autoriteiten

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

Artikel 13
Samenwerking tussen aanbieders van hostingdiensten, bevoegde autoriteiten en, in voorkomend geval, betrokken organen van de Unie

1. De bevoegde autoriteiten in de lidstaten lichten elkaar in, coördineren en werken samen met elkaar en, in voorkomend geval, met betrokken organen van de Unie, zoals Europol, met betrekking tot verwijderingsbevelen en doorverwijzingen teneinde dubbel werk te voorkomen, de coördinatie te verbeteren en inmenging in onderzoeken in verschillende lidstaten te voorkomen.

2. De bevoegde autoriteiten in de lidstaten lichten elkaar in, coördineren en werken samen met de in artikel 17, lid 1, onder c) en d), bedoelde bevoegde autoriteit met betrekking tot krachtens artikel 6 genomen maatregelen en handhavingsmaatregelen krachtens artikel 18. De lidstaten zorgen ervoor dat de in artikel 17, lid 1, onder c) en d), bedoelde bevoegde autoriteit in het bezit is van alle relevante informatie. Daartoe voorzien de lidstaten in passende communicatiekanalen of -mechanismen om ervoor te zorgen dat de relevante informatie tijdig wordt gedeeld.

3. De lidstaten en de aanbieders van hostingdiensten kunnen ervoor kiezen gebruik te maken van speciale instrumenten, met inbegrip van, in voorkomend geval, instrumenten die zijn ingesteld door betrokken organen van de Unie, zoals Europol, om met name het volgende te faciliteren:

   (a) de verwerking van, en de feedback over, verwijderingsbevelen krachtens artikel 4;

   (b) de verwerking van, en de feedback over, doorverwijzingen krachtens artikel 5;

(c) de samenwerking met het oog op het bepalen en uitvoeren van proactieve maatregelen krachtens artikel 6.

4. Wanneer aanbieders van hostingdiensten kennis krijgen van bewijs van terroristische misdrijven, lichten zij de autoriteiten die in de betrokken lidstaat bevoegd zijn voor het onderzoek en de vervolging van strafbare feiten, of het contactpunt in de lidstaat krachtens artikel 14, lid 2, waar zij hun hoofdvestiging of een wettelijke vertegenwoordiger hebben, onmiddellijk in. In geval van twijfel kunnen aanbieders van hostingdiensten deze informatie doorgeven aan Europol met het oog op passende follow-up.

Artikel 14
Contactpunten

1. Aanbieders van hostingdiensten wijzen een contactpunt aan waardoor verwijderingsbevelen en doorverwijzingen met elektronische middelen kunnen worden ontvangen, en garanderen een snelle behandeling krachtens de artikelen 4 en 5. Zij zorgen ervoor dat deze informatie openbaar wordt gemaakt.

2. De in lid 1 bedoelde informatie specificeert de officiële taal of talen van de Unie als bedoeld in Verordening (EG) nr. 1/58, waarin het contactpunt kan worden benaderd en waarin verdere uitwisselingen met betrekking tot verwijderingsbevelen en doorverwijzingen krachtens de artikelen 4 en 5 plaatsvinden. Die informatie bevat ten minste één van de officiële talen van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging heeft of waar zijn wettelijke vertegenwoordiger krachtens artikel 16 woont of gevestigd is.

3. De lidstaten wijzen een contactpunt aan voor de behandeling van verzoeken om verduidelijking en feedback met betrekking tot de door hen uitgevaardigde verwijderingsbevelen en doorverwijzingen. Informatie over het contactpunt wordt openbaar gemaakt.

AFDELING V
UITVOERING EN HANDHAVING

Artikel 15
Rechtsmacht

1. De lidstaat waar de hoofdvestiging van de aanbieder van hostingdiensten zich bevindt, heeft rechtsmacht voor de toepassing van de artikelen 6, 18 en 21. Een aanbieder van hostingdiensten die zijn hoofdvestiging niet in een van de lidstaten heeft, wordt geacht onder de rechtsmacht van de lidstaat te vallen waar de in artikel 16 bedoelde wettelijke vertegenwoordiger woont of gevestigd is.

2. Wanneer een aanbieder van hostingdiensten verzuimt een wettelijke vertegenwoordiger aan te wijzen, hebben alle lidstaten rechtsmacht.

3. Wanneer een autoriteit van een andere lidstaat overeenkomstig artikel 4, lid 1, een verwijderingsbevel heeft uitgevaardigd, heeft die lidstaat rechtsmacht om overeenkomstig zijn nationale recht dwangmaatregelen te nemen om het verwijderingsbevel te handhaven.

Artikel 16
Wettelijke vertegenwoordiger

1. Een aanbieder van hostingdiensten die geen vestiging in de Unie heeft maar diensten in de Unie aanbiedt, wijst schriftelijk een natuurlijke persoon of rechtspersoon aan als zijn wettelijke vertegenwoordiger in de Unie voor de ontvangst, naleving en handhaving van verwijderingsbevelen, doorverwijzingen, verzoeken en besluiten van de bevoegde autoriteiten op basis van deze verordening. De wettelijke vertegenwoordiger woont of is gevestigd in een van de lidstaten waar de aanbieder van hostingdiensten de diensten aanbiedt.

2. De aanbieder van hostingdiensten belast de wettelijke vertegenwoordiger met de ontvangst, naleving en handhaving van de in lid 1 bedoelde verwijderingsbevelen, doorverwijzingen, verzoeken en besluiten namens hem. Aanbieders van hostingdiensten verlenen hun wettelijke vertegenwoordiger de nodige bevoegdheden en middelen om met de bevoegde autoriteiten samen te werken en deze besluiten en bevelen na te leven.

3. De aangewezen wettelijke vertegenwoordiger kan aansprakelijk worden gesteld voor de niet-naleving van verplichtingen uit hoofde van deze verordening, onverminderd de aansprakelijkheidsvorderingen en vorderingen in rechte die tegen de aanbieder van hostingdiensten kunnen worden ingesteld.

4. De aanbieder van hostingdiensten stelt de in artikel 17, lid 1, onder d), bedoelde bevoegde autoriteit in de lidstaat waar de wettelijke vertegenwoordiger woont of gevestigd is, in kennis van de aanwijzing. Informatie over de wettelijke vertegenwoordiger wordt openbaar gemaakt.

AFDELING VI
SLOTBEPALINGEN

Artikel 17
Aanwijzing van bevoegde autoriteiten

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

   (a) het uitvaardigen van verwijderingsbevelen krachtens artikel 4;

   (b) het opsporen, identificeren en doorverwijzen van terroristische inhoud naar aanbieders van hostingdiensten krachtens artikel 5;

   (c) het toezicht op de uitvoering van proactieve maatregelen krachtens artikel 6;

   (d) de handhaving van de verplichtingen uit hoofde van deze verordening door middel van sancties krachtens artikel 18.

2. Uiterlijk op [*zes maanden na de inwerkingtreding van deze verordening*] stellen de lidstaten de Commissie in kennis van de in lid 1 bedoelde bevoegde autoriteiten. De Commissie maakt de kennisgeving en alle wijzigingen ervan bekend in het *Publicatieblad van de Europese Unie*.

Artikel 18
Sancties

1. De lidstaten stellen regels vast inzake de sancties die van toepassing zijn bij inbreuken door de aanbieders van hostingdiensten op de verplichtingen uit hoofde

van deze verordening, en nemen alle nodige maatregelen om te garanderen dat die worden uitgevoerd. Deze sancties worden beperkt tot inbreuken op de verplichtingen uit hoofde van:

(a) artikel 3, lid 2 (voorwaarden van aanbieders van hostingdiensten);

(b) artikel 4, leden 2 en 6 (uitvoering van en feedback over verwijderingsbevelen);

(c) artikel 5, leden 5 en 6 (beoordeling van en feedback over doorverwijzingen);

(d) artikel 6, leden 2 en 4 (verslagen over proactieve maatregelen en de vaststelling van maatregelen naar aanleiding van een besluit waarbij specifieke proactieve maatregelen zijn opgelegd);

(e) artikel 7 (bewaring van gegevens);

(f) artikel 8 (transparantie);

(g) artikel 9 (waarborgen met betrekking tot proactieve maatregelen);

(h) artikel 10 (klachtenprocedures);

(i) artikel 11 (informatie voor aanbieders van inhoud);

(j) artikel 13, lid 4 (informatie over bewijs van terroristische misdrijven);

(k) artikel 14, lid 1 (contactpunten);

(l) artikel 16 (aanwijzing van een wettelijke vertegenwoordiger).

2. De vastgestelde sancties zijn doeltreffend, evenredig en afschrikkend. De lidstaten stellen de Commissie uiterlijk op [*zes maanden na de inwerkingtreding van deze verordening*] in kennis van die regels en maatregelen en stellen haar onverwijld in kennis van alle latere wijzigingen daarvan.

3. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij het bepalen van het soort en de hoogte van de sancties rekening houden met alle relevante omstandigheden, waaronder:

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

(b) de opzettelijke of nalatige aard van de inbreuk;

(c) eerdere inbreuken door de verantwoordelijk geachte rechtspersoon;

(d) de financiële draagkracht van de aansprakelijk geachte rechtspersoon;

(e) de mate waarin de aanbieder van hostingdiensten met de bevoegde autoriteiten samenwerkt.

4. De lidstaten zorgen ervoor dat bij een systematisch verzuim de verplichtingen uit hoofde van artikel 4, lid 2, na te leven, financiële sancties worden opgelegd van ten hoogste 4 % van de mondiale omzet van de aanbieder van hostingdiensten in het laatste boekjaar.

Artikel 19

Technische vereisten en wijzigingen van de modellen voor verwijderingsbevelen

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

2. De Commissie is bevoegd deze gedelegeerde handelingen tot wijziging van de bijlagen I, II en III vast te stellen, zodat doeltreffend kan worden gereageerd als verbeteringen moeten worden aangebracht aan de inhoud van de formulieren voor verwijderingsbevelen en van de formulieren die moeten worden gebruikt om informatie te verstrekken over de onmogelijkheid om het verwijderingsbevel 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 [*datum waarop deze verordening van toepassing wordt*].

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 over beter wetgeven van 13 april 2016.

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

6. Een overeenkomstig 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 deze 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 hebben genomen, en zenden die informatie elk jaar uiterlijk op [31 maart] aan de Commissie. Die informatie omvat:

   (a) informatie over het aantal uitgevaardigde verwijderingsbevelen en doorverwijzingen, het aantal artikelen met terroristische inhoud die zijn verwijderd of waartoe de toegang onmogelijk is gemaakt, met inbegrip van de overeenkomstige termijnen krachtens de artikelen 4 en 5;

   (b) informatie over de krachtens artikel 6 genomen specifieke proactieve maatregelen, met inbegrip van de hoeveelheid terroristische inhoud die is

verwijderd of waartoe de toegang onmogelijk is gemaakt en de overeenkomstige termijnen;

(c) informatie over het aantal krachtens artikel 10 ingeleide klachtenprocedures en door de aanbieders van hostingdiensten genomen maatregelen;

(d) informatie over het aantal ingeleide rechtsmiddelen en door de bevoegde autoriteiten in overeenstemming met het nationale recht en genomen besluiten.

2. Uiterlijk op [*één jaar na de datum waarop deze verordening van toepassing wordt*] 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 krachtens artikel 23 te evalueren.

Artikel 22
Uitvoeringsverslag

Uiterlijk op [*twee jaar na de inwerkingtreding van deze verordening*] brengt de Commissie aan het Europees Parlement en de Raad verslag uit over de toepassing van deze verordening. In het verslag van de Commissie wordt rekening gehouden met de informatie over monitoring uit hoofde van artikel 21 en met de 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

Niet eerder dan [*drie jaar na de datum waarop deze verordening van toepassing wordt*] verricht de Commissie een evaluatie van deze verordening en dient zij bij het Europees Parlement en de Raad een verslag in over de toepassing van deze verordening, waarin ook wordt nagegaan of de waarborgmechanismen doeltreffend werken. Waar passend, gaat het verslag vergezeld van wetgevingsvoorstellen. De lidstaten verstrekken de Commissie de informatie die nodig is om het verslag op te stellen.

Artikel 24
Inwerkingtreding

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

Zij wordt van toepassing vanaf [zes maanden na de datum van inwerkingtreding].

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

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*