Raad van de
Europese Unie

Brussel, 7 december 2018
(OR. en)

15336/18

Interinstitutioneel dossier:
2018/0331(COD)

CT 198
ENFOPOL 605
JAI 1264
COTER 175
CYBER 313
TELECOM 461
FREMP 222
AUDIO 121
DROIPEN 199
CODEC 2270

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	6 december 2018
aan:	de delegaties
nr. vorig doc.:	14978/18 + COR 1
Nr. Comdoc.:	12129/18 + ADD 1-3
Betreft:	Voorstel voor een verordening van het Europees Parlement en de Raad ter voorkoming van de verspreiding van terroristische online-inhoud - algemene oriëntatie

De Raad heeft tijdens zijn zitting van 6 december 2018 overeenstemming bereikt over de algemene oriëntatie in bijlage dezes.

Wijzigingen ten opzichte van het Commissievoorstel zijn aangegeven in ***vet cursief***, schrappingen zijn aangegeven met [...].

[…]

[…] ***Ontwerp***

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

ter voorkoming van de verspreiding van terroristische online-inhoud

[...]

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

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

Gezien het voorstel van de Europese Commissie,

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

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

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Deze verordening wil 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.

[1] PB C , , blz. .

(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, wat 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 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[2] van de Commissie, en beantwoordt aan de oproep van het Europees Parlement om de maatregelen tegen illegale en schadelijke inhoud aan te scherpen, en aan de oproep van de Europese Raad om de automatische detectie en verwijdering van inhoud die tot terroristische daden aanzet, te verbeteren.

[2] 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).

(5) De toepassing van deze verordening mag geen afbreuk doen aan de toepassing van artikel 14 van Richtlijn 2000/31/EG[3]. 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. ***Deze verordening dient niet van toepassing te zijn op activiteiten betreffende nationale veiligheid, aangezien deze onder de uitsluitende verantwoordelijkheid van elke lidstaat blijven vallen.***

(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.

---

[3] 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).

(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, ***evenals aan de persvrijheid en pluralisme in de media,*** die [...] [...] essentiële fundamenten zijn van een pluralistische, democratische samenleving 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 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 hosting-diensten 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***,*** ***en voor aanbieders van hostingdiensten om een besluit dat proactieve maatregelen of sancties oplegt, te betwisten voor de rechterlijke instantie van de lidstaat waar zij zijn gevestigd of waar zij een juridisch vertegenwoordiger hebben***.

(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[4]. Omdat de schadelijkste terroristische onlinepropaganda moet worden aangepakt, moet de definitie betrekking hebben op materiaal [...] dat aanzet tot het plegen van terroristische misdrijven of tot het bijdragen aan terroristische misdrijven, of dit aanmoedigt of verdedigt, [...] of het deelnemen aan activiteiten van een terroristische groepering bevordert. [...] ***De definitie bevat inhoud die richtsnoeren biedt voor het maken en gebruiken van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, evenals CBRN-stoffen, of voor andere methoden en technieken, met inbegrip van het selecteren van doelwitten, voor het plegen van terroristische misdrijven.*** Dergelijk [...] ***materiaal*** 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, [...] of onderzoeksdoeleinden wordt verspreid ***of als tegenargument kan dienen,*** moet voldoende worden beschermd, ***rekening houdend met een billijk evenwicht tussen de grondrechten, zoals met name de vrijheid van meningsuiting en van informatie, en de behoeften op het gebied van openbare veiligheid. Wanneer verspreid materiaal onder de redactionele verantwoordelijkheid van de aanbieder van inhoud wordt gepubliceerd, moet bij iedere beslissing om die inhoud te verwijderen, rekening worden gehouden met de journalistieke normen die in regelgeving voor de pers of de media zijn vastgelegd in overeenstemming met het Unierecht, alsook met het recht op vrijheid van meningsuiting en het recht op vrijheid en pluriformiteit van de media, zoals vervat in artikel 11 van het Handvest van de grondrechten.*** Voorts mag de uiting van radicale, polemische of controversiële standpunten in het publieke debat over gevoelige politieke vraagstukken niet als terroristische inhoud worden beschouwd.

---

[4] 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).

(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 ***en verstrekt materiaal*** opslaan en de opgeslagen informatie ***en het opgeslagen materiaal*** aan derden beschikbaar stellen, ongeacht of deze activiteit louter technisch, automatisch en passief is. [...] ***Inhoud opslaan bestaat uit het bijhouden van gegevens in het geheugen van een fysieke of virtuele server; dit sluit tussenpersonen en andere elektronische communicatiediensten in de zin van het [Europees wetboek voor elektronische communicatie] of "caching"-diensten uit van het toepassingsgebied, of andere diensten die worden aangeboden in andere lagen van de internetinfrastructuur, zoals registers en registrerende instanties, DNS (domain name system) of aanverwante diensten, zoals betalingsdiensten of beschermingsdiensten tegen DDOS- of gedistribueerde denial-of-service-aanvallen. Daarnaast moet de informatie op verzoek van de aanbieder van inhoud worden opgeslagen; enkel de diensten waarvoor de aanbieder van de inhoud de directe ontvanger is, vallen binnen het toepassingsgebied. Ten slotte wordt de opgeslagen informatie beschikbaar gesteld voor derden, waaronder wordt verstaan iedere derde gebruiker die niet de aanbieder van inhoud is. Interpersoonlijke communicatiediensten die een directe interpersoonlijke en interactieve uitwisseling van informatie tussen een eindig aantal personen mogelijk maken, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, vallen buiten het toepassingsgebied.*** Dergelijke aanbieders van ***hostingdiensten*** [...] zijn bijvoorbeeld socialemediaplatforms, videostreamingdiensten, diensten voor het delen van video- en audiobestanden en beelden, bestandsdeling en andere cloud- ***en opslag***diensten [...]. ***Deze verordening is van toepassing op het verstrekken van hostingdiensten, in plaats van op de specifieke aanbieder of zijn belangrijkste activiteit, die hostingdiensten kan combineren met andere diensten die buiten het toepassingsgebied van deze verordening vallen.***

(10a) 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 nr. 1215/2012 van het Europees Parlement en de Raad[5]. 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[6] is neergelegd, op die grond alleen niet worden beschouwd als het richten van activiteiten op een bepaald grondgebied in de Unie.

---

5 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).

6 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).

(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 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 hosting-diensten 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. ***Onverminderd de verplichting op grond van artikel 7 van deze verordening, of in het kader van [het ontwerp voor wetgeving inzake elektronisch bewijsmateriaal] om gegevens te bewaren, m***oeten de aanbieders van hostingdiensten zelf beslissen de desbetreffende inhoud al dan niet te verwijderen of de toegang daartoe onmogelijk te maken voor gebruikers in de Unie. ***Dit moet ertoe leiden dat de toegang wordt verhinderd of ten minste wordt bemoeilijkt en dat internetgebruikers die van hun diensten gebruikmaken ernstig ontmoedigd worden om zich toegang te verschaffen tot de inhoud die werd geblokkeerd***.

(13a) Het verwijderingsbevel moet zowel een classificatie van de desbetreffende inhoud als terroristische inhoud, als voldoende gegevens bevatten om de gezochte inhoud te kunnen vinden, en dit door een URL en alle andere bijkomende informatie te verstrekken, zoals een screenshot van de inhoud in kwestie. Indien daarom wordt verzocht, dient de bevoegde autoriteit een aanvullende motivering te verstrekken waarom de inhoud als terroristische inhoud wordt beschouwd. De motivering hoeft geen gevoelige informatie te bevatten die het onderzoek in het gedrang kan brengen. De motivering moet evenwel de aanbieder van hostingdiensten en, uiteindelijk, de aanbieder van inhoud in staat stellen hun recht op hoger beroep daadwerkelijk te kunnen uitoefenen.

(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. Deze 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[7].

[7] 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).

(15) [...] He***t*** [...] mechanisme voor ***doorverwijzing*** waarbij aanbieders van hostingdiensten worden gewezen op informatie ***en materiaal*** die als terroristische inhoud kunnen worden beschouwd en waarbij de aanbieder vrijwillig kan onderzoeken of dit overeenkomt ***met*** zijn eigen voorwaarden**,** ***vormt een*****[...]** ***bijzonder doeltreffende, snelle en evenredige manier om aanbieders van hostingdiensten bewust te maken van bepaalde inhoud van hun diensten*** [...]. 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[8] 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 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 laag ***risico of*** een lage mate van blootstelling aan terroristische inhoud.

---

8 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).

(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, ***"transactiegegevens" en*** [...] "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 indien 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. ***Aan terroristische inhoud blootgestelde*** aanbieders van hostingdiensten moeten jaarlijks transparantieverslagen publiceren met nuttige informatie over de maatregelen die zijn genomen in verband met de opsporing, identificatie en verwijdering van terroristische inhoud***, waar dit geen afbreuk doet aan het doel van de ingevoerde maatregelen***.

(25) Klachtenprocedures vormen een noodzakelijke waarborg tegen onjuiste - omdat die onder de vrijheid van meningsuiting en van informatie valt - verwijdering van inhoud ***als gevolg van maatregelen uit hoofde van de gebruiksvoorwaarden van de aanbieders van hostingdiensten.*** 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. De voorwaarde 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. ***Bovendien moeten aanbieders van inhoud waarvan de inhoud is verwijderd na een verwijderingsbevel, recht hebben op een doeltreffende voorziening in rechte overeenkomstig artikel 19 VEU en artikel 47 van het Handvest van de grondrechten van de Europese Unie***.

(26) ***Meer in het algemeen*** [...] vereist doeltreffende rechtsbescherming in de zin van artikel 19 VEU en artikel 47 van het Handvest van de grondrechten van de Europese Unie 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. Hiervoor is echter niet noodzakelijk een kennisgeving aan de aanbieder van inhoud vereist. 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 ***vóór*** het uitvaardigen van verwijderingsbevelen of ***wanneer*** zij door-verwijzingen aan aanbieders van hostingdiensten zenden. [...] ***Wanneer de bevoegde autoriteit besluit een verwijderingsbevel uit te vaardigen, moet zij terdege rekening houden met iedere kennisgeving van een bemoeienis met het belang van het onderzoek ("conflictoplossing"). Wanneer een bevoegde autoriteit door een bevoegde autoriteit in een andere lidstaat op de hoogte wordt gebracht van een bestaand verwijderingsbevel, moet er geen tweede bevel worden uitgevaardigd.*** 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. ***De Commissie moet een dergelijke coördinatie en samenwerking bevorderen.***

(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 en met aanbieders van hostingdiensten te faciliteren, en om dubbel werk te voorkomen, ***worden*** de lidstaten [...] ***aangemoedigd om*** gebruik te maken van ***de specifieke*** 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 waar zij 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 verstrekkingsbevel op grond van de verordening betreffende Europese bevelen tot verstrekking en tot conservatoir beslag van digitaal bewijsmateriaal in strafzaken[9].

(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***, interne of uitbestede,*** specifieke middelen waarmee verwijderingsbevelen en doorverwijzingen elektronisch kunnen worden ingediend en uit de technische [...] ***of*** persoonlijke middelen om die snel te kunnen verwerken. Het contactpunt voor de aanbieder van 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 die zijn blootgesteld aan terroristische inhoud, wat blijkt uit de ontvangst van een verwijderingsbevel,*** erop toezien 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 hosting-diensten 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. ***Omwille van de effectieve uitvoering, de spoedeisendheid en de openbare orde, moet iedere lidstaat echter bevoegd zijn voor verwijderingsbevelen en verwijzingen.***

---

9 COM(2018) 225 final.

(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. ***Aanbieders van hostingdiensten kunnen gebruik maken van een bestaande wettelijke vertegenwoordiger, op voorwaarde dat deze wettelijke vertegenwoordiger in staat is om de taken zoals vastgelegd in deze verordening uit te oefenen***.

(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***, die zowel van administratieve als van strafrechtelijke aard kunnen zijn,*** 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 de sancties rekening houden 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. ***Wanneer de aard van de inbreuk wordt beoordeeld en wordt beslist of er sancties worden opgelegd, moeten de grondrechten, zoals de vrijheid van meningsuiting, ten volle worden geëerbiedigd***. 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. Gewaarmerkte 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 ter zake, moet de Commissie ook de bevoegdheid krijgen om gedelegeerde handelingen vast te stellen tot aanvulling van deze verordening met technische voorschriften voor de elektronische middelen die de bevoegde autoriteiten moeten gebruiken voor de verzending van verwijderingsbevelen. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen geschieden in overeenstemming met de beginselen van het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven[10]. 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. ***De lidstaten mogen gebruik maken van de transparantieverslagen van de aanbieders van hostingdiensten en deze, waar nodig, aanvullen met meer gedetailleerde informatie***. 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.

---

10 PB L 123 van 12.5.2016, blz. 1.

(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 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.

3. ***Deze verordening heeft niet tot gevolg dat de verplichting tot eerbiediging van de grondrechten en de fundamentele rechtsbeginselen, zoals neergelegd in artikel 6 van het Verdrag betreffende de Europese Unie, wordt gewijzigd.***

Artikel 2

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "aanbieder van hostingdiensten": een aanbieder van diensten van de informatie-maatschappij 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: een vestiging van de aanbieder van hostingdiensten in de Unie;

Bij gebrek aan een dergelijke vestiging wordt de beoordeling van een wezenlijke band gebaseerd op specifieke feitelijke criteria, zoals:

(a) ***een*** aanzienlijk aantal gebruikers in een of meer lidstaten;

(b) **of** een toespitsing van activiteiten op een of meer lidstaten.

(4) "terroristische misdrijven": ***een van de*** in artikel 3, lid 1, […] van Richtlijn (EU) 2017/541 ***vermelde opzettelijke handelingen***;

(5) "terroristische inhoud": [...] ***materiaal dat aan de pleging van opzettelijke handelingen als vermeld in artikel 3, lid 1, punten a) tot en met i), van Richtlijn 2017/541, kan bijdragen door***:

aa) het dreigen met het plegen van een terroristisch misdrijf;

(a) het aanzetten tot of het pleiten voor het plegen van terroristische misdrijven, [...] ***waaronder*** [...] ***de verheerlijking ervan,*** waardoor het gevaar ontstaat dat dergelijke daden worden gepleegd;

(b) ***het aansporen van personen of een groep personen tot het plegen van of***[...] bijdrage***n*** [...] tot terroristische misdrijven;

(c) het bevorderen van de activiteiten van een terroristische groepering, met name door ***aansporing van personen of een groep personen tot*** [...] het deelnemen aan of het ondersteunen van ***de criminele activiteiten van*** [...] een terroristische groepering in de zin van artikel 2, lid 3, van Richtlijn (EU) 2017/541;

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 ***in de Unie***.

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 vermelden in hun voorwaarden ***dat zij geen terroristische inhoud opslaan*** en passen bepalingen ter voorkoming van de verspreiding van terroristische inhoud toe.

Artikel 4

Verwijderingsbevelen

1. De bevoegde autoriteit heeft de bevoegdheid om een [...] ***verwijderingsbevel*** 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; ***een*** [...] ***beoordeling van*** [...] ***de inhoud*** [...], ten minste met verwijzing naar de desbetreffende in artikel 2, lid 5, vermelde categorieën van terroristische inhoud;

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

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

(d) datum en tijdstip van uitvaardiging;

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

(f) 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 [...] ***aanvullende*** motivering ***waarin wordt toegelicht waarom de inhoud als terroristische inhoud wordt beschouwd***, 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. ***Zonder onnodige vertraging bevestigen*** aanbieders van hostingdiensten [...] de ontvangst en stellen zij de bevoegde autoriteit [...] 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 4 bis

Overlegprocedure voor verwijderingsbevelen

1. Op hetzelfde moment dat het verwijderingsbevel aan de aanbieder van hostingdiensten wordt toegezonden overeenkomstig artikel 4, lid 5, dient de uitvaardigende autoriteit een exemplaar van dat verwijderingsbevel in bij de in artikel 17, lid 1, onder a), bedoelde bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn voornaamste vestiging heeft.

2. In gevallen waarin de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn belangrijkste vestiging heeft, redelijke gronden heeft om aan te nemen dat het verwijderingsbevel gevolgen kan hebben voor fundamentele belangen van die lidstaat, stelt zij de uitvaardigende bevoegde autoriteit daarvan in kennis.

3. De uitvaardigende autoriteit neemt deze omstandigheden in aanmerking en trekt het verwijderingsbevel in of past het aan, indien noodzakelijk.

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 [...] informatie [...] ***over*** de redenen waarom de inhoud als terroristische inhoud wordt beschouwd, ***alsmede*** 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 [...] ***zonder onnodige vertraging*** 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, [...] ***afhankelijk van het risico en de mate van blootstelling aan terroristische inhoud***, 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) ***het opnieuw verschijnen van*** [...] inhoud die eerder is verwijderd of waartoe de toegang onmogelijk is gemaakt omdat hij als terroristische inhoud wordt beschouwd, ***op efficiënte wijze aan te pakken***;

   (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. ***De in artikel 17, lid 1, onder c) bedoelde bevoegde autoriteit beslist over de aard en het toepassingsgebied van de proactieve maatregelen, in overeenstemming met de doelstellingen van deze verordening.*** 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, [...] hetgeen nodig is [...] 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 ***die aan terroristische inhoud zijn blootgesteld,*** 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 ***het opnieuw verschijnen van*** [...] inhoud die eerder is verwijderd of waartoe de toegang onmogelijk is gemaakt omdat hij als terroristische inhoud wordt beschouwd, ***op efficiënte wijze aan te pakken***;

   (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 [...] ***zes*** weken te rekenen vanaf dat besluit. ***Wanneer dit gerechtvaardigd is, kan deze termijn met een tweede periode van zes weken worden verlengd.*** 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, [...] ***bevoegde*** *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 [...] ***bevoegde*** 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. ***Met het oog op de effectieve uitvoering van deze verordening en de voorkoming van dubbel werk kunnen d***[...]e lidstaten en de aanbieders van hostingdiensten ervoor kiezen gebruik te maken van speciale instrumenten, met inbegrip van [...] instrumenten die zijn ingesteld door [...] ***bevoegde*** 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 of lidstaten bevoegd zijn voor het onderzoek en de vervolging van strafbare feiten[...]. ***Indien het onmogelijk is de betrokken lidstaat of lidstaten te identificeren, stellen de*** aanbieders van hostingdiensten ***het contactpunt in de lidstaat krachtens artikel 14, lid 3, waar zij hun hoofdvestiging of een wettelijke vertegenwoordiger hebben, daarvan in kennis en geven zij*** [...] deze informatie [...] aan Europol door 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. ***Elke lidstaat heeft rechtsmacht voor de toepassing van de artikelen 4 en 5, ongeacht waar de aanbieder van hostingdiensten zijn hoofdvestiging heeft of een wettelijke vertegenwoordiger heeft aangewezen.***

2. Wanneer een aanbieder van hostingdiensten verzuimt een wettelijke vertegenwoordiger aan te wijzen, hebben alle lidstaten rechtsmacht. ***Indien een lidstaat besluit zijn rechtsmacht uit te oefenen, stelt hij alle andere lidstaten daarvan in kennis.***

[…] […]

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 [***twaalf*** [...] *maanden na de inwerkingtreding van deze verordening*] stellen de lidstaten de Commissie in kennis van de in lid 1 bedoelde bevoegde ***autoriteit of*** 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 [[...] *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 ***natuurlijke of*** rechtspersoon;

(d) de financiële draagkracht van de aansprakelijk geachte ***natuurlijke of*** 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 [***twaalf*** [...] 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*