EUROPESE
COMMISSIE

Straatsburg, 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken

{SEC(2018) 199 final} - {SWD(2018) 118 final} - {SWD(2018) 119 final}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Het gebruik van sociale media, webmail, berichtendiensten en applicaties ("apps") om te communiceren, te werken, sociale contacten te onderhouden en informatie te verkrijgen, is op tal van plaatsen in de wereld gemeengoed geworden. De betreffende diensten verbinden honderden miljoenen gebruikers met elkaar. Zij leveren aanzienlijke voordelen op voor het economisch en sociaal welzijn van de gebruikers, zowel in de Unie als daarbuiten. Zij kunnen echter ook worden misbruikt als instrumenten voor het plegen of faciliteren van misdrijven, waaronder ernstige misdrijven als terroristische aanslagen. Wanneer dat het geval is, bieden deze diensten en apps onderzoekers vaak het enige aanknopingspunt om te kunnen bepalen wie een strafbaar feit heeft gepleegd en bewijs te verkrijgen dat in de rechtbank kan worden gebruikt.

Omdat het internet geen grenzen kent, kunnen dergelijke diensten overal ter wereld worden aangeboden en zijn deze daarvoor niet per se afhankelijk van een fysieke infrastructuur, bedrijfsinrichting of personeel in de lidstaten waar zij worden aangeboden of binnen de interne markt in zijn geheel. Evenmin vereisen deze diensten een specifieke locatie voor de opslag van gegevens. Een dienstverlener kiest een dergelijke locatie vaak op grond van legitieme overwegingen inzake bijvoorbeeld gegevensbeveiliging, schaalvoordelen en snelle toegang. Als gevolg daarvan verlangen autoriteiten van de lidstaten in een groeiend aantal strafzaken van uiteenlopende aard[1] toegang tot gegevens die als bewijs kunnen dienen en die buiten hun land en/of door dienstverleners in andere lidstaten of derde landen zijn opgeslagen.

Met het oog op situaties waar ofwel het bewijs ofwel de dienstverlener zich elders bevindt, werden enkele tientallen jaren geleden mechanismen voor samenwerking tussen landen ontwikkeld[2]. Ondanks regelmatige hervormingen staan deze samenwerkingsmechanismen onder toenemende druk als gevolg van de groeiende behoefte aan snelle grensoverschrijdende toegang tot elektronisch bewijs. In reactie daarop heeft een aantal lidstaten en derde landen besloten om zijn nationale instrumenten uit te breiden. De fragmentatie die daarvan het gevolg is, leidt tot rechtsonzekerheid en tegenstrijdige verplichtingen en roept vragen op over de bescherming van grondrechten en procedurele waarborgen voor personen op wie dergelijke verzoeken betrekking hebben.

In 2016 riep de Raad op tot het nemen van concrete maatregelen op basis van een gemeenschappelijke EU-benadering om de wederzijdse rechtshulp efficiënter te maken, de samenwerking tussen de autoriteiten van de lidstaten en in derde landen gevestigde dienstverleners te verbeteren en oplossingen voor te stellen voor het probleem van de vaststelling en handhaving van rechtsmacht[3] in de cyberruimte[4]. Ook het Europees Parlement wees op de problemen die het thans gefragmenteerde rechtskader kan opleveren voor

---

1 Zie punten 2.1.1 en 2.3 van de effectbeoordeling.

2 In de Unie gaat het om mechanismen voor wederzijdse erkenning, thans gebaseerd op het Europees onderzoeksbevel; bij de samenwerking met derde landen gaat het om mechanismen voor wederzijdse rechtshulp.

3 De term "handhavingsjurisdictie" in dit document verwijst naar de bevoegdheid van de betrokken autoriteiten om een onderzoeksmaatregel te treffen.

4 Conclusies van de Raad van de Europese Unie inzake de verbetering van de strafrechtspraak in de cyberruimte, ST9579/16.

dienstverleners die trachten te voldoen aan verzoeken inzake rechtshandhaving en riep op tot de invoering van een Europees rechtskader, dat ook waarborgen bevat voor de rechten en vrijheden van alle betrokkenen[5].

Het onderhavige voorstel is gericht op het specifieke probleem dat het vluchtige karakter en de internationale dimensie van elektronisch bewijsmateriaal met zich brengen. Het beoogt samenwerkingsmechanismen aan te passen aan het digitale tijdperk door de rechterlijke macht en rechtshandhavingsinstanties instrumenten te bieden om de moderne communicatiewijzen van criminelen aan te pakken en moderne vormen van criminaliteit te bestrijden. Dergelijke instrumenten mogen alleen maar worden toegelaten wanneer zij gepaard gaan met krachtige mechanismen ter bescherming van de grondrechten. Dit voorstel beoogt de rechtszekerheid voor autoriteiten, dienstverleners en betrokken particulieren te verbeteren en hoge normen voor rechtshandhavingsverzoeken te handhaven, om zo de bescherming van grondrechten, transparantie en de eerbiediging van de verantwoordingsplicht te waarborgen. Het bespoedigt ook het proces inzake het veiligstellen en verkrijgen van elektronisch bewijsmateriaal dat is opgeslagen en/of wordt bewaard door dienstverleners die binnen een andere jurisdictie zijn gevestigd. Dit instrument zal bestaan naast de bestaande instrumenten voor justitiële samenwerking, die relevant blijven en kan desgewenst door de bevoegde autoriteiten worden gebruikt. Tegelijkertijd werkt de Commissie aan de versterking van de bestaande mechanismen voor justitiële samenwerking door middel van maatregelen als de instelling van een beveiligd platform voor de snelle uitwisseling van verzoeken tussen justitiële autoriteiten in de EU en de investering van 1 miljoen EUR voor de opleiding van beroepsbeoefenaren uit alle EU-lidstaten op het gebied van wederzijdse rechtshulp en samenwerking, met de nadruk op de Verenigde Staten als het derde land dat het grootste aantal verzoeken vanuit de EU ontvangt[6].

Voor de betekening, kennisgeving en uitvoering van bevelen uit hoofde van dit instrument dienen de autoriteiten zich te verlaten op de door de dienstverleners aangewezen wettelijke vertegenwoordiger. De Commissie presenteert vandaag een voorstel om ervoor te zorgen dat dergelijke wettelijke vertegenwoordigers daadwerkelijk worden aangewezen. Het biedt een gemeenschappelijke, EU-brede oplossing voor het uitbrengen van wettelijke bevelen aan dienstverleners via wettelijke vertegenwoordigers.

- **Samenhang met het bestaande EU-rechtskader op het beleidsterrein en het Verdrag van Boedapest van de Raad van Europa**

Het huidige EU-rechtskader bestaat uit Unie-samenwerkingsinstrumenten op het gebied van strafzaken, zoals Richtlijn 2014/41/EU betreffende het Europees onderzoeksbevel in strafzaken[7] (de EOB-richtlijn), de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie[8], Besluit 2002/187/JBZ van de Raad betreffende de oprichting van Eurojust[9], Verordening (EU) 2016/794 betreffende Europol[10] en

5 P8_TA(2017)0366.

6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

7 Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, PB L 130 van 1.5.2014, blz. 1.

8 Akte van de Raad van 29 mei 2000 tot vaststelling, overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie, van de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie.

9 Besluit 2002/187/JBZ van de Raad van 28 februari 2002 betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken In 2013 keurde de Commissie

Kaderbesluit 2002/465/JBZ van de Raad inzake gemeenschappelijke onderzoeksteams[11], alsook uit bilaterale overeenkomsten tussen de Unie en derde landen, zoals de overeenkomst betreffende wederzijdse rechtshulp tussen de EU en de VS[12] en de overeenkomst inzake wederzijdse rechtshulp tussen de EU en Japan[13].

Door de invoering van Europese verstrekkings- en bewaringsbevelen maakt het voorstel het gemakkelijker om in het kader van strafprocedures elektronisch bewijs veilig te stellen en te vergaren dat door dienstverleners binnen een andere jurisdictie is opgeslagen of wordt bewaard. De EOB-richtlijn, die in belangrijke mate het Verdrag inzake wederzijdse rechtshulp in strafzaken heeft vervangen, bestrijkt alle onderzoeksmaatregelen[14]. Ook toegang tot elektronisch bewijsmateriaal valt eronder, maar de EOB-richtlijn bevat geen specifieke bepalingen over dit type bewijsmateriaal[15]. Het nieuwe instrument zal niet in de plaats komen van het EOB voor het verkrijgen van elektronisch bewijsmateriaal, maar autoriteiten een aanvullend instrument bieden. Er kunnen situaties zijn, bijvoorbeeld wanneer in de ten uitvoer leggende lidstaat diverse onderzoeksmaatregelen moeten worden uitgevoerd, waarin overheidsinstanties de voorkeur zullen geven aan het EOB. De invoering van een nieuw instrument voor elektronisch bewijsmateriaal is een beter alternatief dan de wijziging van de EOB-richtlijn, vanwege de specifieke problemen waarmee het verkrijgen van elektronisch bewijs gepaard gaat en waarvan bij de overige onderzoeksmaatregelen waarop de EOB-richtlijn betrekking heeft, geen sprake is.

Om het grensoverschrijdend vergaren van elektronisch bewijsmateriaal te vergemakkelijken, zal het nieuwe instrument voortbouwen op de beginselen inzake wederzijdse erkenning. Een autoriteit in het land waar de adressaat van het bevel zich bevindt, hoeft niet rechtstreeks bij de kennisgeving of betekening en uitvoering van het bevel te worden betrokken, behalve in geval van niet-naleving, omdat dan handhaving noodzakelijk is en de bevoegde autoriteit in het land waar de vertegenwoordiger zich bevindt, zal interveniëren. Het instrument vergt dus een reeks krachtige waarborgen en bepalingen, zoals in elk geval de bekrachtiging door een justitiële autoriteit. Zo mogen Europese bevelen tot verstrekking van transactiegegevens of inhoudelijke gegevens (in tegenstelling tot abonnee- en toegangsgegevens) alleen worden uitgevaardigd voor strafbare feiten waarop in de uitvaardigende staat een maximale vrijheidsstraf staat van ten minste 3 jaar, dan wel voor specifieke, van de cyberruimte

---

een voorstel voor een verordening ter hervorming van Eurojust goed (Voorstel voor een verordening van het Europees Parlement en de Raad betreffende het EU-Agentschap voor justitiële samenwerking in strafzaken (Eurojust), COM/2013/0535 final).

10 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.

11 Kaderbesluit 2002/465/JBZ van de Raad van 13 juni 2002 inzake gemeenschappelijke onderzoeksteams.

12 Besluit 2009/820/GBVB van de Raad van 23 oktober 2009 betreffende de sluiting namens de Europese Unie van de overeenkomst betreffende uitlevering tussen de Europese Unie en de Verenigde Staten van Amerika en de overeenkomst betreffende wederzijdse rechtshulp in strafzaken tussen de Europese Unie en de Verenigde Staten van Amerika.

13 Besluit 2010/616/EU van de Raad van 7 oktober 2010 inzake de sluiting van de Overeenkomst tussen de Europese Unie en Japan betreffende wederzijdse rechtshulp in strafzaken.

14 Met uitzondering van gezamenlijke onderzoeksteams (zie artikel 3 van de EOB-richtlijn); niet alle lidstaten nemen deel aan de EOB-richtlijn (Ierland, Denemarken).

15 Met uitzondering van een verwijzing in artikel 10, lid 2, onder e), naar de identificatie van een persoon die een IP-adres heeft, ten aanzien van wie een dubbele nationaliteit niet kan worden aangevoerd als grond voor de weigering het verzoek te erkennen en uit te voeren.

afhankelijke of via de cyberruimte mogelijk gemaakte delicten of delicten op het gebied van terrorisme, als bedoeld in het voorstel.

De persoonsgegevens waarop dit voorstel betrekking heeft, zijn beschermd en mogen alleen worden verwerkt in overeenstemming met de algemene verordening gegevensbescherming (hierna "AVG" genoemd[16]) en de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten (richtlijn gegevensbescherming bij rechtshandhaving)[17]. De AVG zal op 25 mei 2018 in werking treden en de richtlijn gegevensbescherming bij rechtshandhaving moet door de lidstaten uiterlijk op 6 mei 2018 zijn omgezet.

Bij het Verdrag van Boedapest van de Raad van Europa inzake cybercriminaliteit (CETS nr. 185), dat door de meeste EU-lidstaten is geratificeerd, zijn internationale mechanismen vastgesteld voor samenwerking ter bestrijding van cybercriminaliteit[18]. Het Verdrag heeft betrekking op misdrijven die via het internet en andere computernetwerken zijn gepleegd. Het schrijft partijen ook voor om de bevoegdheden en procedures vast te stellen voor het verkrijgen van elektronisch bewijs en om elkaar wederzijdse rechtshulp te bieden, ook op andere gebieden dan cybercriminaliteit. Met name eist het Verdrag dat partijen verstrekkingsbevelen invoeren voor het verkrijgen van computergegevens van dienstverleners op hun grondgebied en abonneegegevens van dienstverleners die op hun grondgebied diensten aanbieden. Bovendien voorziet het Verdrag in bewaringsbevelen voor gevallen waarin er vermoedelijk een groot risico is dat de computergegevens verloren gaan of gewijzigd worden. De kennisgeving en betekening en de afdwingbaarheid van nationale verstrekkingsbevelen ten aanzien van dienstverleners die buiten het grondgebied van een partij bij het Verdrag zijn gevestigd, zorgt voor andere problemen. In dat verband worden thans nadere maatregelen ter verbetering van de grensoverschrijdende toegang tot elektronisch bewijsmateriaal overwogen[19].

- **Samenvatting van de voorgestelde verordening**

De voorgestelde verordening voert een dwingend Europees verstrekkingsbevel en een dwingend Europees bewaringsbevel in. Beide bevelen moeten door een justitiële autoriteit van een lidstaat worden uitgevaardigd of bekrachtigd. Een bevel kan worden uitgevaardigd met het oog op de bewaring of verstrekking van gegevens die zijn opgeslagen door een dienstverlener binnen een andere jurisdictie en die nodig zijn als bewijs in een strafrechtelijk

16 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

17 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

18 In de Strategie inzake cyberbeveiliging van de Europese Unie van 2013 werd het Verdrag van Boedapest erkend als het belangrijkste multilaterale kader voor de strijd tegen cybercriminaliteit — Gezamenlijke mededeling van de Commissie en de Hoge vertegenwoordiger van de Europese Unie voor buitenlandse zaken en veiligheidsbeleid betreffende een strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace (JOIN(2013) 1 final.

19 Tijdens haar 17e plenaire vergadering (juni 2017) stelde de commissie Cybercrimeverdrag (T-CY) de opdracht vast voor de voorbereiding van een tweede aanvullend protocol bij het Verdrag ("Tweede aanvullend protocol") dat door de T-CY moet worden voorbereid en tegen december 2019 moet zijn voltooid. Het is de bedoeling om afstand te gaan nemen van de locatie voor de opslag van gegevens als een beslissende factor.

onderzoek of een strafprocedure. Dergelijke bevelen mogen alleen worden uitgevaardigd wanneer voor hetzelfde strafbare feit in een vergelijkbare binnenlandse situatie in de uitvaardigende staat een soortgelijke maatregel beschikbaar is. De kennisgeving of betekening van beide bevelen kan plaatsvinden aan verleners van elektronische-communicatiediensten, sociale netwerken, onlinemarktplaatsen, andere aanbieders van hostingdiensten en aanbieders van internetinfrastructuur als IP-adressen en registers van domeinnamen, of, in voorkomend geval, aan hun wettelijke vertegenwoordigers. Het Europees bewaringsbevel is, net als het Europees verstrekkingsbevel, gericht tot de wettelijke vertegenwoordiger buiten de jurisdictie van de uitvaardigende lidstaat en strekt tot bewaring van de gegevens met het oog op een aansluitend verzoek deze te verstrekken, bijvoorbeeld via kanalen voor wederzijdse rechtshulp in geval van derde landen, of via een EOB tussen deelnemende lidstaten. Anders dan in wetgeving neergelegde toezichtmaatregelen of verplichtingen tot het bewaren van gegevens, waarin deze verordening niet voorziet, gaat het bij het Europees bewaringsbevel om een bevel dat door een justitiële autoriteit in een concrete strafprocedure wordt uitgevaardigd of bekrachtigd na een individuele beoordeling van de evenredigheid en noodzaak in het individuele geval. Net als het Europees verstrekkingsbevel verwijst het naar de specifieke bekende of onbekende plegers van een strafbaar feit dat al heeft plaatsgevonden. Het Europees bewaringsbevel maakt alleen de bewaring van gegevens mogelijk die reeds ten tijde van de ontvangst van het bevel zijn opgeslagen, en biedt geen toegang tot gegevens op een toekomstig tijdstip na de ontvangst van het Europees bewaringsbevel.

Beide bevelen kunnen alleen in stafprocedures worden uitgevaardigd, vanaf de aan het proces voorafgaande onderzoeksfase tot de beëindiging van de procedure bij vonnis of andere beslissing. Een bevel om abonnee- en toegangsgegevens te verstrekken, kan voor elk strafbaar feit worden uitgevaardigd; het bevel transactie- of inhoudelijke gegevens te verstrekken, kan echter alleen maar worden uitgevaardigd voor feiten waarop in de uitvaardigende staat een maximale vrijheidsstraf staat van ten minste 3 jaar, of voor specifieke delicten die in het voorstel worden genoemd en waarbij sprake is van een specifiek verband met elektronische instrumenten, en strafbare feiten waarop Richtlijn (EU) 2017/541 inzake terrorismebestrijding van toepassing is.

Gezien de verschillende niveaus van indringendheid van de met betrekking tot de verlangde gegevens opgelegde maatregelen, bevat het voorstel een aantal voorwaarden en waarborgen. Daarbij gaat het onder meer om de verplichting om vooraf de bevelen door een justitiële autoriteit te laten bekrachtigen. Het voorstel is uitsluitend van toepassing op opgeslagen gegevens. Het onderscheppen van telecommunicatiegegevens in real-time valt niet onder dit voorstel. De maatregel blijft beperkt tot wat noodzakelijk en evenredig is met het oog op de betreffende strafprocedures. Het voorstel biedt dienstverleners de mogelijkheid om waar nodig de uitvaardigende autoriteiten om toelichtingen te vragen. Wanneer de betreffende kwesties niet kunnen worden opgelost en de uitvaardigende autoriteit besluit om tot tenuitvoerlegging over te gaan, kunnen dienstverleners zich op dezelfde gronden beroepen als die waarop zij zich tegen tenuitvoerlegging door hun eigen autoriteiten verzetten. Bovendien is er een specifieke procedure ingevoerd voor situaties waarin de verplichting gegevens te verstrekken, conflicteert met een concurrerende verplichting uit hoofde van het recht van een derde land.

EU-wetgeving beschermt de rechten van de verdachten en de beschuldigden in strafprocedures en er zijn al regels ter bescherming van persoonsgegevens van kracht. Voor personen wier gegevens worden verlangd, bieden deze aanvullende waarborgen in het voorstel echter procedurele rechten in of buiten de strafprocedure. Daarbij gaat het onder meer om de mogelijkheid de rechtmatigheid, de noodzaak of de evenredigheid van het bevel

te betwisten, zonder dat de gronden worden beperkt voor de betwisting krachtens nationaal recht. De rechten uit hoofde van recht van de tenuitvoerleggingsstaat worden volledig geëerbiedigd door ervoor te zorgen dat immuniteiten en voorrechten die de verlangde gegevens in de lidstaat van de dienstverlener beschermen, in de uitvaardigende staat in aanmerking worden genomen. Dit is met name het geval wanneer zij een hoger niveau van bescherming bieden dan de wetgeving van de uitvaardigende staat.

De naleving van bevelen uit hoofde van de voorgestelde verordening is op dezelfde wijze afdwingbaar als het geval is bij vergelijkbare binnenlandse bevelen in de jurisdictie waar de dienstverlener het bevel ontvangt. De verordening bepaalt dat de lidstaten in doeltreffende en evenredige sancties moeten voorzien.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

De rechtsgrondslag voor maatregelen op dit gebied is artikel 82, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU). Artikel 82, lid 1, bepaalt dat volgens de gewone wetgevingsprocedure, maatregelen kunnen worden vastgesteld die ertoe strekken regels en procedures vast te leggen waarmee alle soorten vonnissen en rechterlijke beslissingen overal in de Unie erkend worden. Er kunnen ook maatregelen worden vastgesteld om in het kader van strafvervolging en tenuitvoerlegging van beslissingen de samenwerking tussen de justitiële of gelijkwaardige autoriteiten van de lidstaten te bevorderen.

Deze rechtsgrondslag is van toepassing op de mechanismen die onder deze verordening vallen. Artikel 82, lid 1, zorgt voor de wederzijdse erkenning van rechterlijke beslissingen waarbij een justitiële autoriteit in de uitvaardigende staat zich tot een rechtspersoon in een andere lidstaat richt en deze zelfs verplichtingen oplegt, zonder voorafgaande tussenkomst van een justitiële autoriteit in die andere lidstaat. Het Europees verstrekkings- of bewaringsbevel kan aanleiding zijn tot de tussenkomst van een justitiële autoriteit van de tenuitvoerleggingsstaat wanneer die tussenkomst noodzakelijk is voor de tenuitvoerlegging van de beslissing.

• Keuze van het instrument

Artikel 82, lid 1, VWEU geeft de EU-wetgever de mogelijkheid om verordeningen en richtlijnen vast te stellen.

Aangezien het voorstel betrekking heeft op grensoverschrijdende procedures, op welk terrein uniforme regels vereist zijn, hoeft de lidstaten geen marge te worden gelaten voor de omzetting van dergelijke regels. Een verordening is rechtstreeks van toepassing, biedt duidelijkheid en meer rechtszekerheid en voorkomt uiteenlopende interpretaties in de lidstaten en andere problemen in verband met omzetting waarmee de kaderbesluiten inzake de wederzijdse erkenning van vonnissen en rechterlijke beslissingen gepaard gingen. Voorts maakt een verordening het mogelijk om in de Unie eenzelfde verplichting op uniforme wijze op te leggen. Daarom wordt een verordening beschouwd als de meest geschikte vorm voor dit instrument inzake wederzijdse erkenning.

• Subsidiariteit

Gezien de grensoverschrijdende dimensie van de problemen die dit voorstel aanpakt, zullen de maatregelen die erin zijn opgenomen, op het niveau van de Unie moeten worden vastgesteld teneinde de doelstellingen te bereiken. Bij misdrijven waarvoor elektronisch

bewijs bestaat, gaat het vaak om situaties waarin de infrastructuur waarbinnen het elektronisch bewijs is opgeslagen en de dienstverlener die de infrastructuur beheert, zich binnen een ander nationaal rechtskader, in de Unie of daarbuiten, bevinden dan het nationale rechtskader van het slachtoffer en de pleger van het strafbaar feit. Daardoor kan het voor het bevoegde land uiterst tijdrovend en lastig zijn om zonder gemeenschappelijke minimumregels daadwerkelijk grensoverschrijdende toegang te verkrijgen tot elektronisch bewijsmateriaal. Lidstaten die alleen opereren, zouden met name op problemen stuiten bij de aanpak van de volgende kwesties:

- fragmentatie van rechtskaders in lidstaten, welke door dienstverleners die willen ingaan op verzoeken op basis van verschillende nationale wetgevingen werd aangemerkt als een groot probleem;
- verbetering van de doelmatigheid van justitiële samenwerking op basis van bestaande EU-wetgeving, met name via het EOB.

Gezien de diversiteit van juridische benaderingen, het aantal beleidsgebieden in kwestie (veiligheid, grondrechten, waaronder procedurele rechten en de bescherming van persoonsgegevens, economische kwesties) en de brede reeks belanghebbenden, is EU-wetgeving het meest passende middel om de vastgestelde problemen aan te pakken.

- **Evenredigheid**

Het voorstel bevat regels op grond waarvan een bevoegde autoriteit in de Unie een dienstverlener die in de Unie diensten aanbiedt en niet in dezelfde lidstaat is gevestigd, kan gelasten elektronisch bewijs te overleggen of te bewaren. De voornaamste aspecten van het voorstel, zoals de materiële werkingssfeer van het Europees verstrekkingsbevel, voorwaarden die courtoisie waarborgen, het sanctiemechanisme en het systeem van waarborgen en rechtsmiddelen, beperken het voorstel tot wat noodzakelijk is om de belangrijkste doelstellingen ervan te bereiken. Met name is het voorstel beperkt tot verzoeken om opgeslagen gegevens (gegevens verkregen op grond van onderschepping van telecommunicatie in real-time vallen er niet onder) en tot bevelen die in een strafprocedure zijn uitgevaardigd voor een specifiek strafbaar feit dat wordt onderzocht. Het strekt zich derhalve niet uit tot misdaadpreventie of andere soorten procedures of inbreuken (zoals administratieve procedures wegens inbreuken op rechtsregels) en verplicht dienstverleners niet ertoe om systematisch meer gegevens te verzamelen of op te slaan dan zakelijk gezien of tot naleving van andere juridische vereisten nodig is. Bovendien kan, terwijl een bevel om abonnee- en toegangsgegevens te verstrekken voor elk strafbaar feit kan worden uitgevaardigd, het bevel transactie- of inhoudelijke gegevens te verstrekken, alleen maar worden uitgevaardigd voor feiten waarop in de uitvaardigende staat een maximale vrijheidsstraf staat van ten minste 3 jaar, of voor specifieke, in het voorstel gedefinieerde, van de cyberruimte afhankelijke of via de cyberruimte mogelijk gemaakte strafbare feiten en delicten in verband met terrorisme. Tot slot verduidelijkt het voorstel de procedurele voorschriften en waarborgen die op de grensoverschrijdende toegang tot elektronisch bewijs van toepassing zijn, maar gaat het niet zover dat het nationale maatregelen harmoniseert. Het is beperkt tot wat noodzakelijk en evenredig is om tegemoet te komen aan de behoeften van rechtshandhavings- en justitiële autoriteiten in het digitale tijdperk.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

• Raadpleging van belanghebbenden

Gedurende anderhalf jaar raadpleegde de Commissie alle relevante belanghebbenden om vast te stellen wat de problemen en mogelijke oplossingen waren. Dit gebeurde aan de hand van enquêtes, die varieerden van een openbare raadpleging tot gerichte enquêtes onder de desbetreffende overheidsinstanties. Ook werden er groepsbijeenkomsten van deskundigen en bilaterale bijeenkomsten georganiseerd om de mogelijke effecten van EU-wetgeving te bespreken. Daarnaast werd door middel van conferenties waar de grensoverschrijdende toegang tot elektronisch bewijs werd besproken, feedback over het initiatief verzameld.

In het algemeen zagen de respondenten het toegenomen gebruik van informatiediensten als een probleem voor rechtshandhavingsautoriteiten, omdat de autoriteiten in kwestie vaak slecht zijn uitgerust om met onlinebewijsmateriaal om te gaan. De lengte van het proces voor het verkrijgen van bewijs wordt ook als een van de voornaamste hindernissen gezien. Andere belangrijke punten die overheidsinstanties benadrukten, betroffen onder meer het gebrek aan betrouwbare samenwerking met dienstverleners, het gebrek aan transparantie, en de rechtsonzekerheid omtrent de rechtsbevoegdheid inzake onderzoeksmaatregelen. Rechtstreekse grensoverschrijdende samenwerking tussen rechtshandhavingsinstanties en verleners van digitale diensten werd geacht toegevoegde waarde voor strafrechtelijk onderzoek te hebben. Dienstverleners en een aantal maatschappelijke organisaties wezen op de noodzaak om bij de samenwerking met overheidsinstanties voor rechtszekerheid te zorgen en om collisie te voorkomen. Wat de bezorgdheid over de impact van nieuwe EU-wetgeving op rechten betreft, waren belanghebbenden van mening dat geen enkel grensoverschrijdend instrument mag worden ingevoerd zonder specifieke waarborgen.

Uit de feedback die in het kader van aanvangseffectbeoordeling werd verzameld, bleek dat belanghebbenden van mening waren dat de aanpak van de tekortkomingen van het huidige systeem voor wederzijdse rechtshulp, dit effectiever zou maken en de rechtszekerheid zou verbeteren. Een aantal maatschappelijke organisaties was geen voorstander van wetgeving op EU-niveau inzake rechtstreekse samenwerking. Zij gaven er de voorkeur aan om EU-maatregelen te beperken tot de verbetering van procedures voor wederzijdse rechtshulp. Op dit idee zal worden voortgebouwd als onderdeel van de praktische maatregelen die de Raad in juni 2016 heeft goedgekeurd.

Uit een gerichte enquête onder overheidsfunctionarissen in de lidstaten kwam ook naar voren dat er geen gemeenschappelijke aanpak was inzake het verkrijgen van grensoverschrijdende toegang tot elektronisch bewijsmateriaal, aangezien elke lidstaat zijn eigen binnenlandse praktijk volgt. Dienstverleners reageren verschillend op verzoeken van buitenlandse rechtshandhavingsinstanties en de reactietijd varieert al naargelang de verzoekende lidstaat. Dit zorgt voor rechtsonzekerheid bij alle betrokken belanghebbenden.

De raadpleging van de belanghebbenden liet in het algemeen zien dat het huidige rechtskader gefragmenteerd en ingewikkeld is. Hierdoor kunnen vertragingen optreden tijdens de uitvoeringsfase en kan de doeltreffendheid tekortschieten van het onderzoek en de vervolging van delicten waarbij grensoverschrijdende toegang tot elektronisch bewijsmateriaal een rol speelt.

- **Effectbeoordeling**

De Raad voor regelgevingstoetsing heeft een positief advies uitgebracht inzake de effectbeoordeling[20] ter ondersteuning van dit voorstel, en heeft diverse suggesties gedaan voor verbetering[21]. Naar aanleiding van dit advies werd de effectbeoordeling gewijzigd, zodat grondrechtenkwesties in verband met de grensoverschrijdende uitwisseling van gegevens nader aan de orde werden gesteld, met name de verbanden tussen de diverse maatregelen die deel uitmaken van de voorkeursoptie. De beoordeling werd ook gewijzigd om de standpunten van belanghebbenden en lidstaten en de wijze waarop daarmee werd rekening gehouden, beter voor het voetlicht te brengen. Bovendien werd de beleidscontext herzien, zodat aanvullende verwijzingen naar diverse aspecten werden opgenomen, zoals discussies binnen groepen van deskundigen die aan de ontwikkeling van het initiatief hebben bijgedragen. De complementariteit tussen de verschillende maatregelen (met name de EOB-richtlijn, onderhandelingen over een aanvullende protocol bij het Verdrag van Budapest en de gezamenlijke herziening van de overeenkomst tussen de EU en de VS inzake wederzijdse rechtshulp) werd verduidelijkt wat betreft werkingssfeer, timing en verstrekkendheid en het basisscenario werd zo herzien dat daarin de ontwikkelingen die zich waarschijnlijk los van de vaststelling van de voorgestelde maatregelen zullen voordoen, beter tot uitdrukking komen. Tot slot werden stroomschema's toegevoegd om de procedures voor het delen van gegevens beter te beschrijven.

Er werden vier beleidsopties overwogen, naast het basisscenario (optie O): een aantal praktische maatregelen ter verbetering van zowel procedures voor justitiële samenwerking als procedures voor directe samenwerking tussen overheidsinstanties en dienstverleners (optie A: niet-wetgevend), een optie die de praktische maatregelen van optie A combineert met internationale oplossingen op bilateraal of multilateraal niveau (optie B: wetgevend), een optie die de maatregelen van optie B combineert met een Europees verstrekkingsbevel en een maatregel ter verbetering van de toegang tot databanken die gegevens over abonnees verstrekken op basis van zoekopdrachten, zoals de domeinnaam Whois (Option C: wetgevend), en een optie die alle eerder bedoelde maatregelen van optie C combineert met wetgeving inzake directe toegang tot op afstand opgeslagen gegevens (optie D: wetgevend)[22].

Wanneer er geen maatregelen worden genomen (optie O), zal het toenemend aantal verzoeken de situatie doen verslechteren. Alle andere opties dragen bij tot het bereiken van de doelstellingen van het initiatief, maar in verschillende mate. Optie A zou de doeltreffendheid van huidige procedures verbeteren, bijvoorbeeld door een verbetering van de kwaliteit van de

---

20 Werkdocument van de diensten van de Commissie – Effectbeoordeling bij het voorstel voor een verordening betreffende Europese bevelen tot verstrekking en bewaring van elektronisch bewijsmateriaal in strafzaken en het voorstel voor een richtlijn tot vaststelling van geharmoniseerde regels voor de aanstelling van wettelijke vertegenwoordigers voor het verzamelen van bewijsmateriaal in strafprocedures, SWD(2018) 118.

21 Raad voor regelgevingstoetsing – Advies over effectbeoordeling – Voorstel voor een verordening betreffende Europese bevelen tot verstrekking en bewaring van elektronisch bewijsmateriaal in strafzaken en het voorstel voor een richtlijn tot vaststelling van geharmoniseerde regels voor de aanstelling van wettelijke vertegenwoordigers voor het verzamelen van bewijsmateriaal in strafprocedures, SEC(2018) 199.

22 Zie voor bijzonderheden het werkdocument van de diensten van de Commissie – Effectbeoordeling bij het voorstel voor een verordening betreffende Europese bevelen tot verstrekking en bewaring van elektronisch bewijsmateriaal in strafzaken en het voorstel voor een richtlijn tot vaststelling van geharmoniseerde regels voor de aanstelling van wettelijke vertegenwoordigers voor het verzamelen van bewijsmateriaal in strafprocedures, SWD(2018) 118.

verzoeken, maar de ruimte voor verbetering zou beperkt worden door de structurele tekortkomingen van het huidige systeem.

Optie B zou tot meer verbeteringen leiden doordat deze internationaal geaccepteerde oplossingen zou bieden, maar het resultaat van deze internationale oplossingen zou tot op grote hoogte van derde landen afhangen. De oplossingen zijn daardoor onzeker en zullen waarschijnlijk niet zo effectief zijn en niet zoveel waarborgen bieden als een EU-oplossing.

Optie C zou duidelijk toegevoegde waarde hebben in vergelijking met de eerdere opties doordat deze ook voorziet in een intern EU-instrument inzake directe samenwerking met dienstverleners dat de meeste van de problemen zou oplossen waarvan sprake is wanneer een dienstverlener in het bezit van de betrokken gegevens is.

Het pakket oplossingen dat optie D biedt, is het ruimst. Naast de vorige maatregelen behelst deze optie een wetgevingsmaatregel inzake directe toegang in situaties waarin er geen betrokkenheid van een dienstverlener is vereist.

Het onderhavige voorstel van de Commissie is gebaseerd op de resultaten van de effectbeoordeling. Deze wetgeving zal worden aangevuld met de in de effectbeoordeling beschreven praktische maatregelen en met de verdere werkzaamheden voor de opstelling van een aanvullend protocol bij het Verdrag van Boedapest. De Commissie zal op basis van haar wetgevingsvoorstel met de VS en andere derde landen ook de mogelijkheid bespreken van toekomstige bilaterale of multilaterale overeenkomsten inzake de grensoverschrijdende toegang tot elektronisch bewijsmateriaal met bijbehorende waarborgen. Ten aanzien van maatregelen voor directe toegang en de toegang tot databanken, die deel uitmaken van optie D, stelt de Commissie thans geen wetgeving voor, maar zij zal verder nadenken over de beste manier om op deze twee punten vooruitgang te boeken.

Het initiatief zal het naar verwachting mogelijk maken onderzoek en vervolging effectiever en efficiënter te laten verlopen en tegelijkertijd de transparantie en verantwoordingsplicht verbeteren en de eerbiediging van de grondrechten waarborgen. Het zal naar verwachting ook het vertrouwen in de digitale eengemaakte markt bevorderen door de veiligheid te verbeteren en het idee te doen afnemen dat misdrijven die op of via netwerkapparatuur zijn gepleegd, niet worden gestraft.

Voor overheidsinstanties zal het initiatief naar verwachting in het begin kosten met zich brengen, die op de lange termijn zouden worden gecompenseerd door besparingen qua vaste kosten. Nationale autoriteiten zouden zich aan nieuwe procedures moeten aanpassen en opleiding moeten volgen. Daarna zouden de autoriteiten echter voordeel hebben van de stroomlijning en centralisatie en het duidelijke rechtskader voor verzoeken om toegang tot gegevens, omdat de grotere efficiëntie winst zou opleveren. Evenzo zouden landen die verzoeken ontvangen minder verzoeken hoeven te verwerken, aangezien de voorkeursoptie de druk op de kanalen voor justitiële samenwerking zou verminderen.

Dienstverleners zouden zich aan een nieuw wetgevingskader moeten aanpassen door de introductie van (nieuwe) procedures en de opleiding van hun personeel. Anderzijds zou een geharmoniseerd kader de druk kunnen doen afnemen op die dienstverleners, die thans moeten reageren op verzoeken om niet-inhoudelijke gegevens en deze aan de hand van de verschillende wetgevingen van al de lidstaten moeten beoordelen. Rechtszekerheid en standaardisering van de procedures zouden ook een positief effect moeten hebben voor kleine en middelgrote ondernemingen, aangezien daardoor de administratieve lasten zouden worden

verlicht en de concurrentie zou worden bevorderd. In zijn algemeenheid zal het initiatief naar verwachting ook voor hen besparingen opleveren.

- **Grondrechten**

Het voorstel zou op een aantal grondrechten van invloed kunnen zijn:

- rechten van de persoon wiens gegevens worden ingezien: het recht op bescherming van persoonsgegevens, het recht op eerbiediging van het privéleven en van het familie- en gezinsleven, het recht op vrijheid van meningsuiting, het recht van verdediging, en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht;
- rechten van de dienstverlener: het recht op vrijheid van ondernemerschap en het recht op een doeltreffende voorziening in rechte;
- rechten van alle burgers: het recht op vrijheid en veiligheid.

Om ervoor te zorgen dat de rechten van deze personen worden beschermd, zijn er in de voorgestelde verordening, met inachtneming van het desbetreffende acquis op het gebied van gegevensbescherming, voldoende en aanzienlijke waarborgen opgenomen.

Aangezien de bevelen alleen kunnen worden uitgevaardigd in strafprocedures en wanneer er vergelijkbare nationale situaties zijn, zowel tijdens het vooronderzoek als tijdens het proces, zijn alle strafrechtelijke procedurele waarborgen van toepassing. Deze waarborgen omvatten met name het recht op een eerlijk proces, dat is neergelegd in artikel 6 EVRM en de artikelen 47 en 48 van het Handvest van de grondrechten. Daarnaast omvatten zij ook de relevante EU-wetgeving inzake procedurele rechten in strafprocedures: Richtlijn 2010/64/EU betreffende het recht op vertolking en vertaling in strafprocedures, Richtlijn 2012/13/EU betreffende het recht op informatie over de rechten en de beschuldiging en toegang tot het dossier, Richtlijn 2013/48/EU betreffende het recht op toegang tot een advocaat en op communicatie met familieleden tijdens aanhouding en detentie, Richtlijn (EU) 2016/343 betreffende de versterking van bepaalde aspecten van het vermoeden van onschuld en van het recht om in strafprocedures bij de terechtzitting aanwezig te zijn, Richtlijn (EU) 2016/800 betreffende procedurele waarborgen voor kinderen en Richtlijn (EU) 2016/1919 betreffende rechtsbijstand voor verdachten en beklaagden in strafprocedures en voor gezochte personen in procedures ter uitvoering van een Europees aanhoudingsbevel.

Meer in het bijzonder zorgt de aan de uitvaardiging van het bevel voorafgaande tussenkomst van een justitiële autoriteit ervoor dat wordt gecontroleerd of de maatregel rechtmatig, noodzakelijk en evenredig met het geval in kwestie is. Dit zorgt er ook voor dat het bevel niet onnodig inbreuk maakt op grondrechten, waaronder die welke voortvloeien uit rechtsbeginselen als dat inzake de vertrouwelijkheid van de communicatie tussen advocaat en cliënt. De uitvaardigende autoriteit dient er in het individuele geval voor te zorgen dat de maatregel noodzakelijk en evenredig is, gelet ook op de ernst van het onderzochte strafbare feit. Het voorstel omvat ook drempels voor transactie- en inhoudelijke gegevens, die ervoor zorgen dat het Europees verstrekkingsbevel alleen zal worden gebruikt voor meer ernstige vormen van criminaliteit in verband met dergelijke gegevens.

Ook het recht op een doeltreffende voorziening in rechte voor personen om wier gegevens wordt verzocht, komt expliciet aan de orde. Tijdens het proces in de uitvaardigende staat moet ook rekening worden gehouden met de immuniteiten en voorrechten van bepaalde beroepsbeoefenaren, zoals toegewezen advocaten, alsook met de fundamentele belangen op

het gebied van nationale veiligheid of defensie in de staat van de adressaat. De toetsing door een justitiële autoriteit geldt hier als een verdere waarborg.

Aangezien het bevel een bindende maatregel is, is het ook van invloed op de rechten van dienstverleners, met name dat inzake de vrijheid van ondernemerschap. Het voorstel geeft de dienstverlener het recht om in de uitvaardigende lidstaat bepaalde vorderingen in te stellen, bijvoorbeeld wanneer het bevel niet door een justitiële autoriteit is uitgevaardigd of bekrachtigd. Wanneer het bevel voor tenuitvoerlegging is doorgegeven aan de tenuitvoerleggingsstaat, kan de tenuitvoerleggingsautoriteit besluiten om het bevel niet te erkennen of ten uitvoer te leggen wanneer na ontvangst zich een van de beperkte gronden voor bezwaar voordoet, zij het dat eerst de uitvaardigende autoriteit moet worden geraadpleegd. Mocht de procedure voor tenuitvoerlegging worden gestart, dan zal bovendien de adressaat zelf zich op een van deze beperkte gronden voor de tenuitvoerleggingsautoriteit tegen het bevel kunnen verzetten. Daarbij gaat het bijvoorbeeld om gevallen waarin het duidelijk is dat het bevel niet door een bevoegde autoriteit werd uitgevaardigd of bekrachtigd of waarin de naleving van het bevel het Handvest kennelijk zou schenden of kennelijk misbruik zou opleveren. Dit staat niet in de weg aan het recht van de adressaat op een doeltreffende voorziening in rechte tegen een beslissing waarbij een sanctie wordt opgelegd.

Een potentieel probleem in verband met EU-maatregelen op dit gebied vormt de mogelijkheid dat derde landen ertoe zouden kunnen worden gebracht wederkerige verplichtingen voor EU-dienstverleners in te voeren die niet in overeenstemming zijn met EU-voorwaarden inzake grondrechten, waaronder de inachtneming van het hoge niveau van gegevensbescherming dat het EU-acquis waarborgt. Het voorstel lost dit probleem op twee manieren op: allereerst door te zorgen voor een maatregel die krachtige waarborgen bevat en die expliciet verwijst naar de voorwaarden en waarborgen die reeds inherent aan het EU-acquis zijn en daarmee als model voor buitenlandse wetgeving dient, en ten tweede door het opnemen van een specifieke clausule inzake “tegenstijdige verplichtingen”, op grond waarvan dienstverleners kunnen vaststellen of er tegenstrijdige verplichtingen zijn en deze aan de orde kunnen stellen, en zo een toetsing door de rechter in gang kunnen zetten. Deze clausule is zo opgezet dat zowel algemene blokkeringswetten worden geëerbiedigd, zoals de Amerikaanse Electronic Communications Privacy Act (hierna “ECPA” genoemd), die openbaarmaking in verband met inhoudelijke gegevens, behoudens een beperkt aantal uitzonderingen, binnen zijn geografische werkingssfeer verbiedt, als wetten die openbaarmaking niet in het algemeen, maar in individuele gevallen verbieden. In gevallen die verband houden met de ECPA kan de toegang tot inhoudelijke gegevens thans in bepaalde situaties belet zijn, zodat de wederzijdse rechtshulp het voornaamste instrument voor de toegang tot dergelijke gegevens moet blijven. Vanwege de veranderingen die de goedkeuring van de Amerikaanse CLOUD Act[23] teweeg heeft gebracht, zou de blokkeringswet echter ingetrokken kunnen worden wanneer de EU met de VS een overeenkomst zou sluiten. Aanvullende internationale overeenkomsten met andere belangrijke partners kunnen het aantal situaties waarin sprake is van collisie, verder verkleinen.

Gelet op het bovenstaande zijn de maatregelen in dit voorstel verenigbaar met de grondrechten.

[23] Op 23 maart 2018 werd in de Verenigde Staten de Clarifying Lawful Overseas Use of Data (CLOUD) Act goedgekeurd. De CLOUD Act is hier te vinden.

4. GEVOLGEN VOOR DE BEGROTING

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

5. OVERIGE ELEMENTEN

- **Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage**

De verordening is in de Unie rechtstreeks van toepassing. Zij zal door beroepsbeoefenaars rechtstreeks worden toegepast, zonder dat binnenlandse rechtssystemen aangepast hoeven te worden.

De verordening zal worden geëvalueerd en de Commissie zal uiterlijk 5 jaar na haar inwerkingtreding bij het Europees Parlement en de Raad een verslag indienen. Op basis van de bevindingen uit het verslag, met name inzake de vraag of de verordening eventuele lacunes laat zien die in de praktijk relevant zijn, en rekening houdend met technologische ontwikkelingen, zal de Commissie beoordelen of het nodig is de werkingssfeer van de verordening te verruimen. Zo nodig zal de Commissie voorstellen indienen voor de aanpassing van deze verordening. De lidstaten zullen de Commissie de informatie verstrekken die voor de voorbereiding van het verslag nodig is. De lidstaten zullen de gegevens verzamelen die nodig zijn voor het jaarlijkse toezicht op de uitvoering van de verordening.

De Commissie zal zo nodig richtsnoeren uitbrengen voor dienstverleners ten behoeve van de naleving van de verplichtingen uit hoofde van de richtlijn.

- **Artikelsgewijze toelichting**

	VERORDENING	
	Artikel	**Overweging**
I. Onderwerp, definities en toepassingsgebied	1. Onderwerp	1-15
	2. Definities	16-23
	3. Toepassingsgebied	24-27
II. Europees verstrekkingsbevel, Europees bewaringsbevel en certificaten, wettelijke vertegenwoordiger	4. Uitvaardigende autoriteit	30.
	5. Voorwaarden voor uitvaardiging van een Europees verstrekkingsbevel	28-29, 31-35
	6. Voorwaarden voor uitvaardiging van een Europees bewaringsbevel	36.
	7. Adressaat van een Europees verstrekkingsbevel en een Europees bewaringsbevel	37.
	8. Certificaat inzake het Europees verstrekkingsbevel en inzake het Europees bewaringsbevel	38-39

	9. Uitvoering van een CEV	40-41
	10. Uitvoering van een CEB	42.
	11. Vertrouwelijkheid en gebruikersinformatie	43.
	12. Vergoeding van kosten	Geen
III. Sancties en tenuitvoerlegging	13. Sancties	Geen
	14. Tenuitvoerleggingsprocedure	44-45, 55
IV. Rechtsmiddelen	15. en 16. Toetsingsprocedure in geval van tegenstrijdige verplichtingen uit hoofde van het recht van een derde land	47-53
	17. Doeltreffende rechtsmiddelen	54.
	18. Het waarborgen van voorrechten en immuniteiten krachtens het recht van de tenuitvoerleggingsstaat	35.
V. Slotbepalingen	19. Monitoring en rapportage	58.
	20. Wijzigingen van de certificaten en de formulieren	59-60
	21. Uitoefening van bevoegdheidsdelegatie	60.
	22. Kennisgevingen	Geen
	23. Relatie met Europese onderzoeksbevelen	61.
	24. Evaluatie	62.
	25. Inwerkingtreding	Geen

Hoofdstuk 1: Onderwerp, definities en toepassingsgebied

Artikel 1: Onderwerp

Dit artikel omschrijft de algemene werkingssfeer en het doel van het voorstel, dat erin bestaat de regels vast te stellen op grond waarvan een bevoegde justitiële autoriteit in de Europese Unie een dienstverlener die in de Unie diensten aanbiedt, door middel van een Europees verstrekkings- of bewaringsbevel kan gelasten elektronisch bewijs te verstrekken of te bewaren. Deze instrumenten kunnen alleen worden gebruikt in grensoverschrijdende situaties, dat wil zeggen in situaties waarin de dienstverlener in een andere lidstaat is gevestigd of wordt vertegenwoordigd.

Deze verordening geeft de onderzoeksautoriteiten aanvullende instrumenten voor het verkrijgen van elektronisch bewijsmateriaal, zonder de bevoegdheden te beperken die het nationale recht reeds verleent om op hun grondgebied gevestigde of vertegenwoordigde

dienstverleners te dwingen. Wanneer de dienstverlener in dezelfde lidstaat is gevestigd of wordt vertegenwoordigd, dienen de autoriteiten van die lidstaat dus gebruik te maken van nationale dwangmaatregelen jegens de dienstverlener.

De gegevens waarvan de verstrekking wordt bevolen via een Europees verstrekkingsbevel, dienen de autoriteiten rechtstreeks te worden verstrekt, zonder tussenkomst van autoriteiten in de lidstaat waar de dienstverlener is gevestigd of wordt vertegenwoordigd. De verordening neemt ook afstand van de gegevenslocatie als bepalend aanknopingspunt, aangezien de opslag van gegevens in het algemeen niet tot gevolg heeft dat de staat op het grondgebied waarvan de gegevens zijn opslagen, enige controle uitoefent. Tot een dergelijke opslag wordt in de meeste gevallen alleen door de dienstverlener besloten, op grond van zakelijke overwegingen[24].

Bovendien is de verordening ook van toepassing wanneer de dienstverleners niet in de Unie zijn gevestigd of worden vertegenwoordigd, maar in de Unie diensten aanbieden. Dit komt tot uitdrukking in artikel 3, lid 1.

Wanneer in het voorstel wordt verwezen naar een dienstverlener die in een lidstaat is gevestigd of wordt vertegenwoordigd door een aangewezen wettelijke vertegenwoordiger, schept enkel de aanwijzing van een wettelijke vertegenwoordiger geen vestiging van de dienstverlener voor de toepassing van deze verordening.

Artikel 1, lid 2, herinnert eraan dat deze verordening niet mag leiden tot een wijziging van de verplichting de grondrechten en rechtsbeginselen te eerbiedingen die zijn neergelegd in artikel 6 VWEU.

Artikel 2: Definities

Dit artikel geeft definities die in het hele instrument van toepassing zijn.

De volgende soorten dienstverleners vallen onder het toepassingsgebied van de verordening: aanbieders van elektronische-communicatiediensten, aanbieders van diensten van de informatiemaatschappij voor wie de opslag van gegevens een wezenlijk onderdeel is van de aan de gebruiker verleende dienst, met inbegrip van sociale netwerken voor zover zij niet als elektronische-communicatiediensten kunnen worden aangemerkt, onlinemarktplaatsen die de transacties tussen hun gebruikers (zoals consumenten of ondernemingen) mogelijk maken en andere aanbieders van hostingdiensten en aanbieders van diensten inzake internetdomeinnamen en nummering.

Het toepassingsgebied van de verordening omvat aanbieders van elektronische-communicatiediensten als gedefinieerd [in de richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie]. Consumenten en bedrijven worden steeds afhankelijker van nieuwe onlinediensten die persoonlijke communicatie mogelijk maken, zoals Voice over IP, instant messaging en e-maildiensten, die de traditionele communicatiediensten verdringen. Dit voorstel dient dus deze diensten, naast sociale netwerken als Twitter en Facebook, via welke gebruikers inhoud kunnen delen, te omvatten.

In veel gevallen worden gegevens niet langer opgeslagen op een apparaat van een gebruiker, maar beschikbaar gemaakt via een cloudgebaseerde infrastructuur die in principe vanaf iedere

[24] De effectbeoordeling bevat nadere toelichtingen.

plek toegankelijk is. Dienstverleners hoeven niet meer binnen iedere jurisdictie gevestigd te zijn of servers te hebben, maar maken voor de opslag van gegevens en het aanbieden van hun diensten veeleer gebruik van een gecentraliseerde administratie en gedecentraliseerde systemen. Zij doen dit om de load balancing te optimaliseren en vertragingen bij het reageren op verzoeken van gebruikers om gegevens, te beperken. Netwerken voor de distributie van inhoud worden over het algemeen ingezet om sneller inhoud te leveren door die inhoud op diverse, over de hele wereld verspreid staande servers te kopiëren. Daardoor kunnen ondernemingen inhoud verstrekken vanaf de server die het dichtst bij de gebruiker is of die informatie via een minder belast netwerk kan doorgeven. Teneinde rekening te houden met deze ontwikkeling omvat de definitie cloud- en andere hostingdiensten, die een scala aan computercapaciteit bieden, zoals netwerken, servers of andere infrastructuur, opslag, apps en diensten die het mogelijk maken gegevens voor verschillende doeleinden op te slaan. Het instrument is ook van toepassing op digitale marktplaatsen die consumenten en/of ondernemingen in staat stellen om via onlineverkoop- of onlinedienstenovereenkomsten transacties af te sluiten. Dergelijke transacties worden afgesloten ofwel op de website van de onlinemarktplaats ofwel op de website van de handelaar die gebruikmaakt van de computerdiensten die de onlinemarktplaats aanbiedt. Het is daarom deze marktplaats die het elektronisch bewijsmateriaal bezit dat in de loop van een strafprocedure nodig kan zijn.

Het voorstel heeft geen betrekking op diensten waarvan de opslag van gegevens geen wezenlijk onderdeel is. Hoewel de meeste diensten die dienstverleners leveren met enige vorm van opslag gepaard gaan, met name wanneer zij online op afstand worden geleverd, kan er een onderscheid gemaakt worden met betrekking tot diensten waarvoor de opslag van gegevens geen hoofdkenmerk en dus slechts van ondergeschikt belang is, zoals juridische, architectonische diensten en ingenieurs- en accountingdiensten die online op afstand worden geboden.

Gegevens die in het bezit zijn van aanbieders van internetinfrastructuurdiensten, zoals domeinnaamregistrators en -registers en aanbieders van privacy- en proxydiensten, of regionale internetregisters van internetprotocoladressen, kunnen voor strafprocedures relevant zijn omdat zij aanwijzingen kunnen opleveren die het mogelijk maken een bij een criminele activiteit betrokken individu of entiteit te identificeren.

De categorieën gegevens die via een Europees verstrekkingsbevel door de bevoegde autoriteiten kunnen worden verkregen, omvatten abonneegegevens, toegangsgegevens, transactiegegevens (de drie categorieën die gewoonlijk gezamenlijk worden aangeduid als niet-inhoudelijke gegevens) en opgeslagen inhoudelijke gegevens. Dit onderscheid wordt in de rechtsorde van veel lidstaten en ook binnen niet-EU-rechtskaders gemaakt, zij het niet wat betreft toegangsgegevens.

Alle categorieën omvatten persoonsgegevens, zodat de waarborgen uit hoofde van het EU-acquis inzake gegevensbescherming daarop van toepassing zijn. De intensiteit van het effect op de grondrechten varieert tussen deze categorieën, met name tussen abonneegegevens enerzijds en transactie- en inhoudelijke gegevens anderzijds. Het is van essentieel belang dat het instrument op al deze categorieën van toepassing is: abonnee- en toegangsgegevens vormen vaak het beginpunt voor het verkrijgen van de eerste aanknopingspunten in een onderzoek over de identiteit van een verdachte. Transactie- en inhoudelijke gegevens kunnen daarentegen als bewijsmateriaal het meest relevant zijn. Omdat de mate waarin de grondrechten in het geding zijn, verschilt, is het gerechtvaardigd om - zoals in diverse bepalingen in de verordening het geval is - verschillende voorwaarden te verbinden aan abonneegegevens enerzijds en transactie- en inhoudelijke gegevens anderzijds.

Het is passend om toegangsgegevens in deze verordening als een specifieke gegevenscategorie te behandelen. Toegangsgegevens als hier gedefinieerd, worden met hetzelfde doel verlangd als abonneegegevens, namelijk om de gebruiker te identificeren, en de mate waarin de grondrechten in het geding zijn, komt overeen. Daarvoor moeten dus dezelfde voorwaarden gelden als voor abonneegegevens. Vandaar dat dit voorstel een nieuwe categorie gegevens introduceert, die net als abonneegegevens moeten worden behandeld wanneer hetzelfde doel wordt nagestreefd.

Artikel 2 definieert de lidstaten en autoriteiten die bij de procedure betrokken zouden kunnen zijn. Artikel 4 bevat een definitie van het begrip uitvaardigende autoriteit.

Noodsituaties zijn uitzonderlijke situaties die als regel een tijdige reactie van dienstverleners vergen en waarop speciale voorwaarden van toepassing zullen zijn. Zij worden daarom in dit artikel apart gedefinieerd.

Artikel 3: Toepassingsgebied

Dit artikel omschrijft het toepassingsgebied van het voorstel. De verordening is van toepassing op alle dienstverleners die diensten aanbieden in de Unie, met inbegrip van dienstverleners die niet in de Unie zijn gevestigd. Het actief aanbieden van diensten in de Unie, met alle daaraan verbonden voordelen, rechtvaardigt dat de verordening ook op deze dienstverleners van toepassing is en een gelijk speelveld tussen deelnemers op dezelfde markten schept. Wanneer deze dienstverleners niet onder de verordening zouden vallen, zou er bovendien een leemte ontstaan en zou het voor criminelen gemakkelijker worden buiten het toepassingsgebied van de verordening te opereren.

Om zich ervan te kunnen vergewissen of er diensten worden aangeboden, moeten de autoriteiten beoordelen of de dienstverlener rechtspersonen of natuurlijke personen in een of meer lidstaten in staat stelt om zijn diensten te gebruiken. Enkel de toegankelijkheid van de dienst (die ook het gevolg zou kunnen zijn van de toegankelijkheid van de website van de dienstverlener of een intermediair of van een e-mailadres of van andere contactgegevens), mag echter als voorwaarde voor de toepassing van deze verordening niet volstaan. Daarom is een reële link met deze lidstaten vereist om een toereikend verband te kunnen aannemen tussen de dienstverlener en het grondgebied waar hij zijn diensten aanbiedt. Van een dergelijke reële link is sprake wanneer een dienstverlener in of meer lidstaten een vestiging heeft. Wanneer er geen vestiging in de Unie is, moet de vervulling van het criterium van een reële link met de Unie worden beoordeeld op basis van het bestaan van een aanzienlijk aantal gebruikers in een of meer lidstaten, of de toespitsing van activiteiten op een of meer lidstaten. De toespitsing van activiteiten op een of meer lidstaten kan worden bepaald op basis van alle relevante omstandigheden, waaronder factoren als het gebruik van een taal of een munteenheid die in een lidstaat algemeen gangbaar is. De toespitsing van activiteiten op een lidstaat zou ook kunnen worden afgeleid uit de verkrijgbaarheid van een app in de desbetreffende app store, uit het plaatsen van lokale advertenties of uit het adverteren in de taal die in een lidstaat wordt gebruikt, uit het in het kader van de activiteiten gebruik maken van informatie die afkomstig is van personen in lidstaten of uit het beheer van relaties met cliënten, zoals het bieden van klantenservice in de taal die in een lidstaat algemeen gangbaar is. Een reële link moet ook worden aangenomen wanneer een dienstverlener zijn activiteiten richt op een of meer lidstaten, als omschreven in artikel 17, lid 1, onder c), van Verordening (EU) nr. 1215/2012 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken.

Het Europees verstrekkingsbevel en het Europees bewaringsbevel zijn onderzoeksmaatregelen die alleen kunnen worden genomen in het kader van strafrechtelijk onderzoek of een strafprocedure en voor concrete strafbare feiten. De link met een concreet onderzoek onderscheidt deze maatregelen van in de wetgeving omschreven preventieve maatregelen of verplichtingen tot bewaring van gegevens en waarborgt de toepassing van de procedurele rechten die in strafprocedures gelden. De bevoegdheid een onderzoek te starten inzake een specifiek strafbaar feit is dus een noodzakelijke voorwaarde voor de toepasselijkheid van de verordening.

Een aanvullende voorwaarde is dat de verlangde gegevens betrekking hebben op de door de dienstverlener in de Unie aangeboden diensten.

Hoofdstuk 2: Europees verstrekkingsbevel, Europees bewaringsbevel en certificaten

Artikel 4: Uitvaardigende autoriteit

Bij de uitvaardiging van een Europees verstrekkings- of bewaringsbevel moet altijd een justitiële autoriteit zijn betrokken, hetzij als uitvaardigende, hetzij als bekrachtigende autoriteit. Voor bevelen tot het verstrekken van transactie- of inhoudelijke gegevens is de tussenkomst van een rechter of rechtbank vereist. Voor abonnee- of toegangsgegevens volstaat de tussenkomst van een openbaar aanklager.

Artikel 5: Voorwaarden voor het uitvaardigen van een Europees verstrekkingsbevel

Artikel 5 bevat de voorwaarden voor de uitvaardiging van een Europees verstrekkingsbevel. Deze moeten door de uitvaardigende justitiële autoriteit worden beoordeeld.

Een Europees verstrekkingsbevel mag alleen worden uitgevaardigd wanneer dat in het individuele geval noodzakelijk en evenredig is. Bovendien mag het alleen worden uitgevaardigd wanneer een soortgelijke maatregel in een vergelijkbare binnenlandse situatie in de uitvaardigende staat beschikbaar zou zijn.

Bevelen tot het verstrekken van abonnee- en toegangsgegevens kunnen alleen worden uitgevaardigd in geval van strafbare feiten. Voor transactie- en inhoudelijke gegevens dienen strengere eisen te gelden, teneinde de meer gevoelige aard van dergelijke gegevens en de daarmee gepaard gaande hogere mate van ingrijpendheid van bevelen inzake dergelijke gegevens ten opzichte van abonnee- en toegangsgegevens, tot uitdrukking te brengen. Bevelen kunnen daarom alleen maar worden uitgevaardigd voor strafbare feiten waarop een maximale vrijheidsstraf staat van ten minste 3 jaar. Een drempel op basis van de maximale vrijheidsstraf maakt een meer evenredige aanpak mogelijk, net als een aantal andere *ex-ante*- en *ex-post*voorwaarden en waarborgen die ervoor zorgen dat het evenredigheidsbeginsel en de rechten van de betrokken personen worden geëerbiedigd.

Tegelijkertijd mag een drempel echter geen afbreuk doen aan de doeltreffendheid van het instrument en het gebruik ervan door beroepsbeoefenaars. Lidstaten passen diverse maximumstraffen toe al naargelang hun nationale systeem. Nationale strafwetboeken variëren en zijn niet geharmoniseerd. Dit geldt zowel voor de strafbare feiten als voor de straffen die daarop staan. Nationale strafwetboeken variëren ook wat betreft de drempels voor het verkrijgen van transactie- of inhoudelijke gegevens: sommige lidstaten stellen geen specifieke drempel vast; andere voorzien in een lijst van stafbare feiten. Een drempel van drie jaar beperkt het toepassingsgebied van het instrument tot meer ernstige delicten, zonder de mogelijkheden voor het gebruik ervan door beroepsbeoefenaars buitensporig in te perken.

Deze drempel sluit een brede reeks misdrijven van het toepassingsgebied uit, al naargelang het strafwetboek van de betrokken lidstaat (in een aantal lidstaten zijn dat bijvoorbeeld deelname aan de activiteiten van een georganiseerde criminele groep en ontvoering, maar ook strafbare feiten als kleine diefstal, fraude en geweldpleging, waarvoor het gebruik van een grensoverschrijdend bevel tot verstrekking van meer gevoelige gegevens onevenredig kan worden geacht). Anderzijds worden met een drempel van drie jaar misdrijven omvat die een effectievere aanpak vergen, zoals het lidmaatschap van een criminele organisatie, financiering van terroristische groepen, ondersteuning of propageren van een criminele organisatie, opleiding voor het plegen van terroristische strafbare feiten, bepaalde strafbare feiten met terroristisch oogmerk en voorbereiding van een strafbaar feit met terroristisch oogmerk, of voorbereiding van gijzeling, welke misdrijven in geval van toepassing van een hogere drempel uitgesloten zouden zijn, afhankelijk van de betrokken lidstaat. Deze drempel is gekozen om in alle lidstaten te zorgen voor een evenwicht tussen de efficiëntie van strafrechtelijk onderzoek en de bescherming van rechten en inachtneming van het evenredigheidsbeginsel Een drempel heeft ook het voordeel dat hij gemakkelijk in de praktijk kan worden toegepast.

Bovendien kan een bevel tot verstrekking van transactie- of inhoudelijke gegevens ook worden uitgevaardigd voor in de bepaling genoemde specifieke, geharmoniseerde strafbare feiten, waarvoor bewijs meestal alleen in elektronische vorm beschikbaar zal zijn. Dit rechtvaardigt dat de verordening ook wordt toegepast in gevallen waarin de maximale vrijheidsstraf onder de bovengenoemde drempel ligt; anders zouden deze strafbare feiten niet naar behoren kunnen worden onderzocht, wat tot straffeloosheid zou kunnen leiden. De strafbare feiten zijn neergelegd in specifieke bepalingen van: i) Kaderbesluit 2001/413/JBZ van de Raad betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten, ii) Richtlijn 2011/93/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad en iii) Richtlijn 2013/40/EU over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad. Bevelen kunnen ook worden uitgevaardigd voor strafbare feiten die worden genoemd in Richtlijn (EU) 2017/541 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Richtlijn 2005/671/JBZ van de Raad. Sommige van deze stafbare feiten kennen minimale maximumdrempels van ten minste 1 jaar, andere van 2 jaar, maar de maximumdrempel is altijd minimaal 1 jaar.

Het artikel noemt ook de verplichte informatie die in het Europees verstrekkingsbevel moet zijn opgenomen zodat de dienstverlener kan vaststellen welke gegevens worden verlangd en deze kan verstrekken. De motivering waarom de maatregel noodzakelijk en evenredig is, maakt ook onderdeel van het Europees verstrekkingsbevel uit.

Het Europees verstrekkingsbevel wordt ten uitvoer gelegd door de afgifte van een certificaat inzake het Europees verstrekkingsbevel (CEV) (zie artikel 8), dat wordt vertaald en naar de dienstverlener wordt gestuurd. Het CEV bevat dezelfde verplichte informatie als het bevel, met uitzondering van de motivering van de noodzaak en de evenredigheid van de maatregel of verdere bijzonderheden over de zaak.

In gevallen waarin de verlangde gegevens worden opgeslagen of verwerkt als onderdeel van een door een dienstverlener aan een onderneming verstrekte infrastructuur, als regel in geval van hosting- of softwarediensten, dient een verzoek van de onderzoeksautoriteiten primair aan de onderneming zelf gericht te zijn. Daarvoor kan een EOB-procedure of een procedure inzake een verzoek om wederzijdse rechtshulp nodig zijn wanneer de onderneming geen

dienstverlener is die onder deze verordening valt. Een Europees verstrekkingsbevel kan alleen aan een dienstverlener worden gericht wanneer het niet passend zou zijn om het verzoek aan de onderneming te richten, met name wanneer dat het onderzoek in gevaar zou kunnen brengen, bijvoorbeeld wanneer de onderneming zelf het voorwerp van onderzoek is.

Alvorens een Europees verstrekkingsbevel uit te vaardigen, moet de uitvaardigende autoriteit ook rekening houden met de mogelijke immuniteiten en voorrechten uit hoofde van het recht van de lidstaat van de dienstverlener of enig ander gevolg voor de fundamentele belangen van die lidstaat, zoals de nationale veiligheid en verdediging. Deze bepaling heeft als doel ervoor te zorgen dat in de uitvaardigende lidstaat rekening wordt gehouden met immuniteiten en voorrechten die de gegevens beschermen die in de lidstaat van de dienstverlener worden gezocht, met name wanneer die bescherming beter is dan die welke het recht van de uitvaardigende lidstaat biedt.

Artikel 6: Voorwaarden voor het uitvaardigen van een Europees bewaringsbevel

Voor een Europees bewaringsbevel gelden vergelijkbare voorwaarden als voor het Europees verstrekkingsbevel. Het kan overeenkomstig de andere in artikel 6 genoemde voorwaarden voor elk strafbaar feit worden uitgevaardigd. Het heeft als doel te voorkomen dat relevante gegevens worden verwijderd, gewist of gewijzigd in situaties waarin het bewerkstelligen van de verstrekking van deze gegevens meer tijd kan kosten, bijvoorbeeld omdat er gebruik zal worden gemaakt van kanalen voor justitiële samenwerking. Aangezien bijvoorbeeld het EOB in het algemeen kan worden uitgevaardigd voor elk strafbaar feit zonder dat daarvoor drempels gelden, mag het Europees bewaringsbevel evenmin worden beperkt. Anders zou dit instrument niet effectief zijn. Om de onderzoeksautoriteiten in staat te stellen snel te handelen en gezien het feit dat het aansluitende verzoek het desbetreffende verzoek om de gegevens te verstrekken zal zijn, waarbij alle voorwaarden opnieuw worden onderzocht, mag het Europees bewaringsbevel ook door een openbaar aanklager worden uitgevaardigd of bekrachtigd.

Artikel 7: Adressaat van een Europees verstrekkingsbevel of een Europees bewaringsbevel

Europese verstrekkings- en bewaringsbevelen moeten worden gericht tot een wettelijke vertegenwoordiger die door de dienstverlener is aangewezen voor het verzamelen van bewijsmateriaal in strafprocedures overeenkomstig de richtlijn tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures. De doorgifte vindt plaats in de vorm van een certificaat inzake het Europees verstrekkingsbevel (“CEV”) of een certificaat inzake het Europees bewaringsbevel (“CEB”) als bedoeld in artikel 8. Deze wettelijke vertegenwoordiger is verantwoordelijk voor de ontvangst en tijdige en volledige uitvoering van het certificaat. Zodoende kunnen dienstverleners zelf bepalen hoe zij de door de autoriteiten van de lidstaat bevolen verstrekking van de gegevens regelen.

Wanneer er geen wettelijke vertegenwoordiger is aangewezen, kunnen bevelen aan iedere vestiging van de dienstverlener in de Unie worden gericht. Deze terugvaloptie beoogt de doeltreffendheid van het systeem te verzekeren ingeval de dienstverlener (nog) geen specifieke vertegenwoordiger heeft aangewezen, bijvoorbeeld wanneer er geen verplichting overeenkomstig de richtlijn is om een wettelijke vertegenwoordiger aan te wijzen, omdat de dienstverlener slechts in één lidstaat is gevestigd en actief is, of in gevallen waarin er nog geen verplichting een wettelijke vertegenwoordiger te benoemen van kracht is, in de periode voor het verstrijken van de termijn voor omzetting van de richtlijn.

In geval van niet-naleving door de wettelijke vertegenwoordiger zijn er twee situaties waarin de uitvaardigende autoriteit zich tot eender welke vestiging van de dienstverlener in de Unie mag richten: in noodgevallen als gedefinieerd in artikel 9, lid 2, en in gevallen waarin de wettelijke vertegenwoordiger niet voldoet aan zijn verplichtingen uit hoofde van de artikelen 9 en 10 en waarin de uitvaardigende autoriteit van mening is dat er een duidelijk gevaar is dat de gegevens verloren zullen gaan.

Artikel 8: Certificaat inzake het Europees verstrekkingsbevel en inzake het Europees bewaringsbevel

Het CEV en het CEB dienen om de bevelen door te geven aan de adressaat als gedefinieerd in artikel 7. Bijlage I en II bij de verordening bevatten modellen voor beide certificaten; deze moeten worden vertaald in een van de officiële talen van de lidstaat waar de adressaat is gevestigd. De dienstverlener kan verklaren dat bevelen ook in andere officiële talen van de Unie worden aanvaard. De certificaten hebben als doel al de aan de adressaat door te geven noodzakelijke informatie te verstrekken in een standaardformaat, met zo min mogelijk bronnen van fouten, waardoor de gegevens eenvoudig kunnen worden vastgesteld en waarbij vrije tekst zo veel mogelijk wordt vermeden, zodat de vertaalkosten worden gereduceerd. De volledige motivering van de noodzaak en evenredigheid of verdere bijzonderheden over de zaak worden in het certificaat niet opgenomen, teneinde het onderzoek niet in gevaar te brengen. Daaraan bestaat alleen behoefte als onderdeel van het bevel zelf, opdat de verdachte naderhand tijdens de strafprocedure in de gelegenheid is zich daartegen te verzetten.

Een aantal dienstverleners heeft al platforms opgericht voor de indiening van verzoeken door rechtshandhavingsinstanties. De verordening staat aan het gebruik van deze platforms niet in de weg, aangezien dit veel voordelen biedt, zoals de mogelijkheid van een eenvoudige echtverklaring en een veilige doorgifte van de gegevens. Deze platforms moeten het echter mogelijk maken het CEV en het CEB in te dienen in het formaat waarin de bijlagen I en II voorzien, zonder dat aanvullende gegevens in verband met het bevel worden gevraagd.

Door de lidstaten of de Unie opgerichte platforms kunnen ook voorzien in beveiligde middelen voor doorgifte en echtverklaring van de bevelen en het verzamelen van statistische gegevens faciliteren. Ook moet een eventuele uitbreiding van het eCodex- en het Siriusplatform worden overwogen, zodat deze een beveiligde verbinding met dienstverleners hebben voor de doorgifte van het CEV en het CEB en, in voorkomend geval, van de reacties van de dienstverleners.

Artikel 9: Uitvoering van een CEV

Artikel 9 verplicht adressaten om op CEV's te reageren en introduceert dwingende termijnen. De normale termijn is 10 dagen, maar autoriteiten kunnen een kortere termijn vaststellen wanneer dat gerechtvaardigd is. Bovendien bedraagt de termijn 6 uur in noodgevallen, waarvan sprake is wanneer er een onmiddellijke bedreiging is voor iemands leven of fysieke integriteit of voor een kritieke infrastructuur.

De bepaling zorgt ook voor de mogelijkheid van een dialoog tussen de adressaat en de uitvaardigende autoriteit. Wanneer het CEV onvolledig of kennelijk onjuist is, of niet genoeg informatie bevat om de dienstverlener in staat te stellen uitvoering te geven aan het CEV, dient de adressaat contact op te nemen met de uitvaardigende autoriteit en om opheldering te vragen, waarbij hij gebruik moet maken van het formulier in bijlage III. De adressaat dient de uitvaardigende autoriteit ook te informeren wanneer hij de gegevens niet kan verstrekken

omdat er sprake is van overmacht of het feitelijk onmogelijk is. Dat is bijvoorbeeld het geval wanneer iemand wiens gegevens worden verlangd geen afnemer van de betreffende dienst was of de gegevens — bijvoorbeeld uit hoofde van andere privacyverplichtingen — door de dienstverlener rechtmatig zijn gewist voordat hij of zijn wettelijke vertegenwoordiger het bevel ontving. De uitvaardigende autoriteit moet van deze omstandigheden op de hoogte zijn om snel te kunnen reageren, het elektronisch bewijsmateriaal eventueel van een andere dienstverlener te kunnen verkrijgen en te voorkomen dat zij een procedure voor tenuitvoerlegging begint wanneer dat geen enkele zin zou hebben.

Wanneer de adressaat de informatie niet, niet volledig of niet op tijd verstrekt op andere gronden dan de hiervoor genoemde, moet hij de uitvaardigende autoriteit over deze gronden informeren via het in bijlage III opgenomen formulier. Een adressaat kan dus elk onderwerp inzake de uitvoering van het CEV bij de uitvaardigende autoriteit te berde brengen. Dit biedt de uitvaardigende autoriteit de mogelijkheid het CEV in een vroeg stadium, vóór de tenuitvoerleggingsfase, te corrigeren of heroverwegen.

Wanneer de gegevens niet onmiddellijk worden verstrekt, met name wanneer een dialoog is gestart tussen de adressaat en de uitvaardigende autoriteit, en daardoor de termijnen van artikel 9, lid 1, niet meer in acht worden genomen, is de dienstverlener zodra hij het CEV ontvangt, verplicht de gegevens te bewaren teneinde te voorkomen dat deze verloren gaan, mits de gegevens afgebakend kunnen worden. De bewaring kan geschieden ten behoeve van het CEV na opheldering daarvan of een volgend verzoek om wederzijdse rechtshulp of EOB dat in plaats van het oorspronkelijke CEV zal worden toegezonden.

Artikel 10: Uitvoering van een CEB

De uitvoering van een CEB vereist dat de gegevens die beschikbaar zijn op het tijdstip van ontvangst van het bevel, worden bewaard. Dienstverleners moeten de gegevens zo lang bewaren als nodig is om de gegevens op verzoek te kunnen verstrekken, mits de uitvaardigende autoriteit binnen 60 dagen na uitvaardiging van het bevel bevestigt dat zij het aansluitende verzoek om verstrekking heeft ingeleid. Dit houdt in dat op zijn minst een aantal formele stappen zijn genomen, zoals de verzending van een verzoek om wederzijdse rechtshulp ter vertaling.

Anderzijds mogen verzoeken om bewaring alleen plaatsvinden of voortduren zo lang als nodig is om een aansluitend verzoek om deze gegevens te verstrekken mogelijk te maken. Om onnodige of te lange bewaring te vermijden, moet de autoriteit die het Europees bewaringsbevel heeft uitgevaardigd, zodra een besluit is genomen om een bevel tot verstrekking of een verzoek om justitiële samenwerking achterwege te laten of in te trekken, de adressaat daarvan op de hoogte stellen.

Deze bepaling zorgt ook voor de mogelijkheid van een dialoog tussen de adressaat en de uitvaardigende autoriteit, analoog aan het bepaalde in artikel 9. Wanneer het CEB onvolledig of kennelijk onjuist is, of niet genoeg informatie bevat om de dienstverlener in staat te stellen uitvoering te geven aan het CEB, dient de adressaat contact op te nemen met de uitvaardigende autoriteit en om opheldering te vragen, waarbij hij gebruik moet maken van het formulier in bijlage III. De adressaat dient de uitvaardigende autoriteit ook te informeren wanneer hij de gegevens niet kan verstrekken omdat er sprake is van omstandigheden die als overmacht worden beschouwd, of dat feitelijk dan wel om andere redenen niet mogelijk is.

Artikel 11: Vertrouwelijkheid en gebruikersinformatie

De vertrouwelijkheid van het lopend onderzoek, met in begrip van de vertrouwelijkheid van het feit dat er een bevel is uitgevaardigd ter verkrijging van relevante gegevens, moet worden beschermd. Bij dit artikel is teruggegrepen op artikel 19 van de EOB-richtlijn. Het voorziet in de verplichting van de adressaat en, indien niet dezelfde persoon, de dienstverlener, om de vertrouwelijkheid van het CEV of CEB te bewaren, met name door zich te onthouden van het informeren van de persoon wiens gegevens worden verlangd wanneer de uitvaardigende autoriteit daarom, met inachtneming van artikel 23 van de algemene verordening gegevensbescherming, verzoekt teneinde het onderzoek van strafbare feiten te waarborgen.

Anderzijds is het van belang, onder meer met het oog op de aanwending van rechtsmiddelen, dat de persoon wiens gegevens werden verlangd, geïnformeerd wordt. Wanneer de dienstverlener dit ondanks het verzoek van de uitvaardigende autoriteit nalaat, dient de uitvaardigende autoriteit de betrokken persoon overeenkomstig artikel 13 van de richtlijn gegevensbescherming bij rechtshandhaving te informeren zodra het onderzoek niet langer in gevaar kan worden gebracht en daarbij informatie te verstrekken over de beschikbare rechtsmiddelen. Dergelijke informatie wordt alleen verstrekt in geval van een Europees verstrekkingsbevel en niet in geval van een Europees bewaringsbevel, omdat er bij dat laatste bevel minder gevolgen voor de betrokken rechten zijn.

Artikel 12: Vergoeding van kosten

Dienstverleners kunnen ook vergoeding van hun kosten vorderen van de uitvaardigende staat in overeenstemming met het nationale recht van die staat, wanneer dat recht in vergelijkbare binnenlandse gevallen ten aanzien van binnenlandse bevelen daarin voorziet. Dit garandeert een gelijke behandeling van dienstverleners tot wie een binnenlands bevel is gericht en dienstverleners tot wie door dezelfde lidstaat een CEV is gericht, wanneer die lidstaat ervoor heeft gekozen om bepaalde dienstverleners te vergoeden. Anderzijds harmoniseert de voorgestelde verordening de vergoeding van kosten niet, aangezien lidstaten in dat opzicht uiteenlopende keuzes hebben gemaakt.

De kostenvergoeding kan rechtstreeks door de dienstverlener worden gevorderd of via zijn wettelijke vertegenwoordiger. De kosten kunnen slechts eenmaal worden vergoed.

Hoofdstuk 3: Sancties en tenuitvoerlegging

Artikel 13: Sancties

De lidstaten zorgen ervoor dat er doeltreffende, evenredige en afschrikkende geldboetes kunnen worden opgelegd wanneer dienstverleners hun verplichtingen uit hoofde van artikel 9, 10 of 11 niet nakomen. Dit laat nationale rechtsregels onverlet die in de oplegging van strafrechtelijke sancties in dergelijke situaties voorziet.

Artikel 14: Procedure voor tenuitvoerlegging

Artikel 14 voorziet in een procedure voor de tenuitvoerlegging van bevelen in geval van niet-naleving, met de hulp van de lidstaat waar de adressaat van het doorgegeven certificaat is gevestigd. Afhankelijk van wie de eerste adressaat was, is dit ofwel de lidstaat van de dienstverlener ofwel de lidstaat van de wettelijke vertegenwoordiger. De uitvaardigende autoriteit stelt het volledige bevel, met inbegrip van de motivering inzake de noodzaak en de evenredigheid, vergezeld van het certificaat, in handen van de bevoegde autoriteit in de

tenuitvoerleggingsstaat, die het in overeenstemming met zijn nationale wetgeving ten uitvoer legt, zo nodig met gebruikmaking van de in artikel 13 genoemde sancties. Wanneer het bevel voor tenuitvoerlegging is doorgegeven aan de tenuitvoerleggingsstaat , kan de tenuitvoerleggingsautoriteit besluiten om het bevel niet te erkennen en niet ten uitvoer te leggen wanneer zij na ontvangst van mening is dat zich een van de beperkte gronden voor bezwaar voordoet, zij het dat eerst de uitvaardigende autoriteit moet worden geraadpleegd. Mocht de procedure voor tenuitvoerlegging worden ingesteld, dan zal bovendien de adressaat zelf voor de tenuitvoerleggingsautoriteit bezwaar kunnen maken tegen het bevel. De adressaat kan dit doen op basis van eender welke van deze gronden, met uitzondering van immuniteiten en voorrechten, maar met inbegrip van gevallen waarin het duidelijk is dat het bevel niet werd uitgevaardigd of bekrachtigd door een bevoegde autoriteit of dat naleving kennelijk in strijd zou zijn met het Handvest van de grondrechten van de Europese Unie of kennelijk misbruik zou opleveren. Een bevel bijvoorbeeld waarbij de verstrekking wordt gevraagd van inhoudelijke gegevens met betrekking tot een onbepaalde kring van personen in een geografisch gebied of zonder link met concrete strafprocedures, zou op kennelijke wijze de voorwaarden negeren voor de uitvaardiging van een Europees verstrekkingsbevel als vermeld in deze verordening, wat reeds uit de inhoud van het certificaat zelf zou blijken. Andere gronden kunnen alleen worden aangevoerd door degene wiens gegevens worden verlangd, in het kader van de rechtsmiddelen waarover hij zelf in de uitvaardigende lidstaat beschikt (zie artikel 17 hieronder). Bovendien moeten dienstverleners een rechtsmiddel kunnen instellen tegen de beslissing van de tenuitvoerleggingsautoriteit die hun een straf oplegt.

De tenuitvoerleggingsprocedure bevat een aantal termijnen voor de tenuitvoerleggingsautoriteit en de uitvaardigende autoriteit ter vermijding van verdere vertragingen tijdens deze procedure.

Hoofdstuk 4: Rechtsmiddelen

Artikelen 15 en 16: Toetsingsprocedure in geval van tegenstrijdige verplichtingen uit hoofde van het recht van een derde land

De artikelen 15 en 16 voorzien in een toetsingsprocedure voor het geval dienstverleners met een hoofdvestiging in derde landen met tegenstrijdige verplichtingen te maken krijgen. Deze bepalingen zijn ook van groot belang om de bescherming van individuele rechten en internationale courtoisie te waarborgen. Door het stellen van een hoge norm, moeten zij derde landen aanmoedigen om een vergelijkbaar niveau van bescherming te bieden. Zo ook kan in de tegenovergestelde situatie, waarin autoriteiten van een derde land van een dienstverlener in de EU gegevens willen verkrijgen over een EU-burger, het recht van de EU of van lidstaten ter bescherming van de grondrechten, zoals het acquis inzake gegevensbescherming, zich tegen openbaarmaking verzetten. De Europese Unie gaat ervan uit dat derde landen, net zoals dit voorstel, dergelijke verboden eerbiedigen.

De procedure van artikel 15 kan door de adressaat in gang worden gezet wanneer de opvolging van een Europees verstrekkingsbevel een inbreuk zou inhouden op de rechtsregels van een derde land die de openbaarmaking van de gegevens verbiedt omdat de bescherming van de grondrechten van de betrokken personen of de fundamentele belangen van het derde land in verband met de nationale veiligheid of defensie, daartoe nopen. De adressaat moet de uitvaardigende autoriteit door middel van een gemotiveerd bezwaar op de hoogte stellen van de gronden voor zijn conclusie dat er sprake van tegenstrijdige verplichtingen is. Een dergelijk gemotiveerd bezwaar kan niet alleen worden gebaseerd op het feit dat het recht van het derde land dergelijke bepalingen niet kent, noch alleen op het feit dat de gegevens in een derde land zijn opgeslagen. Het gemotiveerd bezwaar moet worden opgeworpen in

aansluiting op de procedure van artikel 9, lid 5, inzake de kennisgeving van het voornemen van niet-nakoming, met gebruikmaking van het formulier in bijlage III.

De uitvaardigende autoriteit dient haar eigen bevel op grond van dit gemotiveerd bezwaar te heroverwegen. Wanneer de uitvaardigende autoriteit besluit om het bevel in te trekken, eindigt de procedure. Wanneer de uitvaardigende autoriteit het bevel in stand wil houden, wordt de zaak doorverwezen naar de bevoegde rechtbank van haar lidstaat. De rechtbank beoordeelt dan op basis van het gemotiveerd bezwaar en met inachtneming van alle relevante feiten van het geval, of het recht van het derde land op het geval in kwestie van toepassing is en – wanneer dat het geval is – of er in het geval in kwestie sprake van tegenstrijdigheid is. Bij deze beoordeling moet de rechtbank in aanmerking nemen of het recht van het derde land niet zozeer de grondrechten of fundamentele belangen van het derde land op het gebied van nationale veiligheid of verdediging beoogt te beschermen, maar er kennelijk op is gericht andere belangen te beschermen of illegale activiteiten af te schermen tegen verzoeken van rechtshandhavingsinstanties in het kader van strafrechtelijk onderzoek.

Wanneer de rechtbank besluit dat er in feite sprake is van strijdigheid met verplichtingen uit hoofde van wetgeving ter bescherming van grondrechten van personen of fundamentele belangen van het derde land op het gebied van nationale veiligheid of verdediging, moet de rechtbank het betrokken derde land om een advies verzoeken via de nationale centrale autoriteiten van dat derde land. Wanneer het geraadpleegde derde land bevestigt dat de tegenstrijdigheid reëel is en bezwaar maakt tegen de uitvoering van het bevel, moet de rechtbank het bevel intrekken.

Wanneer de tegenstrijdigheid zich voordoet op grond van andere wetgeving van derde landen die niet strekt tot bescherming van de bescherming van de grondrechten van personen of fundamentele belangen van het derde land op het gebied van nationale veiligheid of verdediging, dan neemt de rechtbank haar besluit op basis van een afweging van de belangen die voor en tegen de instandhouding van het bevel pleiten.

De in artikel 9 genoemde voorwaarden, met name de verplichting tot het bewaren van gegevens in het zesde lid, gelden ook in situaties waarin er tegenstrijdige verplichtingen voorvloeien uit het recht van een derde land. Wanneer de rechtbank tot de conclusie komt dat het bevel in stand moet blijven, worden de uitvaardigende autoriteit en de dienstverlener daarover geïnformeerd met het oog op de uitvoering ervan. Wanneer het bevel wordt ingetrokken, kan een afzonderlijk Europees bewaringsbevel worden uitgevaardigd, om te garanderen dat de gegevens beschikbaar zijn wanneer deze via een verzoek om wederzijdse rechtshulp kunnen worden verkregen.

Aangezien het Europees bewaringsbevel op zich niet leidt tot openbaarmaking van gegevens en derhalve geen aanleiding geeft tot soortgelijke bezwaren, is de toetsingsprocedure beperkt tot het Europees verstrekkingsbevel.

Artikel 17: Doeltreffende rechtsmiddelen

Deze bepaling zorgt ervoor dat personen op wie het Europees verstrekkingsbevel betrekking heeft, over doeltreffende rechtsmiddelen beschikken. Van deze rechtsmiddelen wordt gebruik gemaakt in de uitvaardigende staat overeenkomstig het nationale recht. Verdachten en beklaagden maken gewoonlijk tijdens de strafprocedure van hun rechtsmiddelen gebruik. Er is niet voorzien in specifieke rechtsmiddelen met betrekking tot het Europees bewaringsbevel, dat op zich geen openbaarmaking van gegevens mogelijk maakt, tenzij het wordt gevolgd door een Europees verstrekkingsbevel of een ander instrument dat tot openbaarmaking leidt, op grond waarvan dan specifieke rechtsmiddelen openstaan.

Personen van wie de gegevens worden gevraagd zonder dat zij verdachte of beklaagde in een strafprocedure zijn, dienen ook over rechtsmiddelen te beschikken in de uitvaardigende staat. Al deze rechten doen geen afbreuk aan eventuele andere middelen uit hoofde van de richtlijn gegevensbescherming bij rechtshandhaving en de algemene verordening gegevensbescherming.

Anders dan in het geval van dienstverleners geldt, beperkt de verordening de eventuele gronden waarop al deze personen de rechtmatigheid van het bevel kunnen aanvechten, niet. Deze gronden omvatten de noodzaak en de evenredigheid van het bevel.

De benutting van rechtsmiddelen in de uitvaardigende lidstaat vormt geen onevenredige belasting voort de betrokken personen. Net als in geval van bevelen waarvan de opvolging via andere vormen van justitiële samenwerking wordt afgedwongen, zijn de rechtbanken van de uitvaardigende staat het best in staat om de rechtmatigheid te beoordelen van door hun eigen autoriteiten uitgevaardigde Europese verstrekkingsbevelen en om de verenigbaarheid daarvan met hun eigen nationale recht te beoordelen. Bovendien kan de adressaat tijdens de tenuitvoerleggingsfase afzonderlijk bezwaar maken tegen de tenuitvoerlegging van het CEV of het CEB in zijn lidstaat van ontvangst op grond van een reeks in de verordening genoemde gronden (zie artikel 14 hiervoor).

Artikel 18: Het waarborgen van voorrechten en immuniteiten krachtens het recht van de ontvangende staat

Deze bepaling streeft hetzelfde doel na als artikel 5, lid 7, dat erin bestaat ervoor te zorgen dat er in de uitvaardigende lidstaat rekening wordt gehouden met de immuniteiten en voorrechten die de in de lidstaat van de dienstverlener gezochte gegevens beschermen, met name wanneer er verschillen tussen die lidstaten bestaan, alsook met de fundamentele belangen van die lidstaat, onder meer op het gebied van nationale veiligheid en defensie. Artikel 18 bepaalt dat de rechtbank van de uitvaardigende staat daarmee rekening moet houden alsof zijn eigen nationale recht erin had voorzien. Vanwege de verschillen tussen lidstaten bij de beoordeling van de relevantie en toelaatbaarheid van bewijsmateriaal, laat de bepaling de rechter enige speelruimte ten aanzien van de wijze waarop ermee rekening wordt gehouden.

Hoofdstuk 5: Slotbepalingen

Artikel 19: Monitoring en rapportage

Op grond van dit artikel moeten de lidstaten specifieke informatie verstrekken met betrekking tot de toepassing van de verordening, teneinde de Commissie bij te staan in de uitoefening van haar taken uit hoofde van artikel 24. De Commissie dient een gedetailleerd programma vast te stellen voor de monitoring van de output, resultaten en effecten van deze verordening.

Artikel 20: Wijzigingen van de certificaten en de formulieren

De certificaten en formulieren in de bijlagen I, II en III bij dit voorstel zullen het eenvoudiger maken om uitvoering te geven aan een CEV en een CEB. Daarom moet het in de toekomst mogelijk zijn om de inhoud van het certificaat en het formulier zo snel mogelijk te verbeteren wanneer dat eventueel nodig mocht zijn. Een wijziging van de drie bijlagen via de gewone wetgevingsprocedure strookt niet met dit vereiste en deze bijlagen zijn niet-essentiële onderdelen van de wetgevingshandelingen, waarvan de belangrijkste elementen in artikel 8 zijn omschreven. Daarom bevat artikel 20 een snellere en flexibelere wijzigingsprocedure via de vaststelling van gedelegeerde handelingen.

Artikel 21: Uitoefening van bevoegdheidsdelegatie

In dit artikel worden de voorwaarden vastgesteld waaronder de Commissie bevoegd is om gedelegeerde handelingen vast te stellen om te voorzien in de noodzakelijke wijzigingen van het certificaat en de formulieren die als bijlage aan het voorstel zijn toegevoegd. Het bevat een standaardprocedure voor de vaststelling van dergelijke gedelegeerde handelingen.

Artikel 22: Kennisgevingen

De lidstaten zijn verplicht de Commissie mee te delen welke instanties bevoegd zijn bevelen uit te vaardigen en ten uitvoer te leggen en welke rechtbanken bevoegd zijn met redenen omklede bezwaren van dienstverleners in behandeling te nemen in geval van collisie.

Artikel 23: Relatie met Europese onderzoeksbevelen

Met deze bepaling wordt verduidelijkt dat de verordening autoriteiten van lidstaten niet verhindert om overeenkomstig Richtlijn 2014/41/EU Europese onderzoeksbevelen uit te vaardigen voor het verkrijgen van digitaal bewijsmateriaal.

Artikel 24: Evaluatie

In dit artikel wordt bepaald dat de Commissie een evaluatie van deze verordening moet uitvoeren, in overeenstemming met de richtsnoeren voor betere regelgeving van de Commissie en overeenkomstig punt 22 van het Interinstitutioneel Akkoord van 13 april 2016[25]. 5 jaar na de inwerkingtreding van de voorgestelde verordening brengt de Commissie verslag uit aan het Europees Parlement en de Raad over de resultaten van de evaluatie, met inbegrip van een evaluatie van de noodzaak om het toepassingsgebied ervan uit te breiden tot diensten die nog niet worden bestreken, maar die voor onderzoek belangrijker kunnen worden.

Artikel 25: Inwerkingtreding

De voorgestelde verordening zal in werking treden op de twintigste dag na die van haar bekendmaking in het Publicatieblad. De verordening is vervolgens van toepassing vanaf zes maanden na de inwerkingtreding ervan.

[25] Interinstitutioneel Akkoord tussen het Europees Parlement, de Raad van de Europese Unie en de Europese Commissie over beter wetgeven van 13 April 2016; PB L 123 van 12.5.2016, blz. 1.

2018/0108 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 82, lid 1,

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[26],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) De Unie heeft zich ten doel gesteld een ruimte van vrijheid, veiligheid en recht te ontwikkelen. Met het oog op de geleidelijke totstandbrenging van die ruimte dient de Unie maatregelen te nemen op het gebied van de justitiële samenwerking in strafzaken die berust op het beginsel van de wederzijdse erkenning van rechterlijke uitspraken en beslissingen, dat sinds de Europese Raad van Tampere op 15 en 16 oktober 1999 algemeen beschouwd wordt als een hoeksteen van de justitiële samenwerking in strafzaken in de Unie.

(2) Maatregelen om elektronisch bewijsmateriaal te verkrijgen en te bewaren worden steeds belangrijker voor onderzoek en vervolging in strafzaken in de hele Unie. Doeltreffende mechanismen om elektronisch bewijsmateriaal te verkrijgen, zijn van essentieel belang om criminaliteit te bestrijden, maar moeten tegelijk aan voorwaarden worden onderworpen met het oog op de volledige eerbiediging van de grondrechten en -beginselen die zijn erkend in het Handvest van de grondrechten van de Europese Unie zoals dat in de Verdragen is verankerd, en met name de beginselen van noodzakelijkheid en evenredigheid, en het recht op eerlijke rechtsbedeling, gegevensbescherming, briefgeheim en bescherming van de persoonlijke levenssfeer.

(3) In de Gezamenlijke verklaring van de EU-ministers van Justitie en Binnenlandse Zaken en van de vertegenwoordigers van de EU-instellingen over de terreuraanslagen op 22 maart 2016 in Brussel werd benadrukt dat bij voorrang manieren moesten worden gezocht om sneller en doeltreffender digitaal bewijsmateriaal te verkrijgen en veilig te stellen, en dat concrete maatregelen moesten worden vastgesteld om deze zaak aan te pakken.

(4) In zijn conclusies van 9 juni 2016 onderstreepte de Raad dat digitaal bewijsmateriaal steeds belangrijker wordt voor de strafvervolging, dat de bescherming van de

[26] PB C van , blz. .

cyberruimte tegen misbruik en criminele activiteiten van groot belang is voor onze economieën en samenlevingen, en dat rechtshandhavings- en gerechtelijke instanties en daarom doeltreffende middelen moeten hebben om criminele handelingen in de cyberruimte op te sporen en te vervolgen.

(5) In de gezamenlijke mededeling over weerbaarheid, afschrikking en defensie van 13 september 2017[27] heeft de Commissie erop gewezen dat doeltreffend onderzoek naar en vervolging van cybercriminaliteit belangrijke afschrikmiddelen tegen cyberaanvallen zijn en dat het huidige procedurele kader beter moet aansluiten bij het internettijdperk. De huidige procedures kunnen de snelheid van cyberaanvallen soms niet aan, waardoor er een bijzondere behoefte aan snelle grensoverschrijdende samenwerking is ontstaan.

(6) Het Europees Parlement heeft deze bezorgdheid verwoord in zijn resolutie over de strijd tegen cybercriminaliteit van 3 oktober 2017[28], waarin wordt gewezen op de problemen die het momenteel versnipperde wettelijke kader kan opleveren voor dienstverleners die willen voldoen aan verzoeken van rechtshandhavingsautoriteiten en waarin de Commissie wordt verzocht een voorstel voor een Europees rechtskader voor e-bewijs voor te leggen met voldoende waarborgen voor de rechten en vrijheden van alle betrokkenen.

(7) Op een netwerk gebaseerde diensten kunnen vanuit om het even welke plaats worden geleverd en vereisen geen fysieke infrastructuur, gebouwen of personeel in het betrokken land. Als gevolg daarvan wordt relevant bewijsmateriaal vaak opgeslagen buiten de staat waar het onderzoek wordt gevoerd, of door een buiten die staat gevestigde dienstverlener. Vaak is er geen ander verband tussen de in de betrokken staat onderzochte zaak en de staat van de plaats van opslag of van de belangrijkste vestiging van de dienstverlener.

(8) Als gevolg van dit ontbrekende verband worden verzoeken om justitiële samenwerking vaak gericht aan landen die een groot aantal dienstverleners hosten, maar verder geen enkele link hebben met de betrokken zaak. Voorts is het aantal verzoeken sterk toegenomen in het licht van de steeds vaker gebruikte netwerkdiensten, die van nature grensoverschrijdend zijn. Als gevolg daarvan duurt het verkrijgen van elektronisch bewijsmateriaal door middel van justitiële samenwerking vaak erg lang, zelfs langer dan aanknopingspunten beschikbaar zijn. Bovendien is er geen duidelijk kader voor samenwerking met dienstverleners, terwijl bepaalde dienstverleners uit derde landen directe verzoeken om niet-inhoudelijke gegevens aanvaarden, zoals toegestaan op grond van hun toepasselijk nationaal recht. Als gevolg daarvan doen alle lidstaten een beroep op het kanaal voor samenwerking met dienstverleners wanneer dat voorhanden is, en gebruiken zij verschillende nationale instrumenten, voorwaarden en procedures. Bovendien hebben sommige lidstaten voor inhoudelijke gegevens unilaterale maatregelen genomen, terwijl andere een beroep blijven doen op justitiële samenwerking.

(9) Het versnipperde rechtskader levert problemen op voor dienstverleners die willen voldoen aan verzoeken van rechtshandhavingsautoriteiten. Er is derhalve behoefte aan een Europees rechtskader voor elektronisch bewijsmateriaal om dienstverleners die onder het toepassingsgebied van het instrument vallen, te verplichten om autoriteiten

[27] JOIN(2017) 450 final.
[28] 2017/2068(INI).

direct te antwoorden, zonder de betrokkenheid van een justitiële autoriteit van de lidstaat van de dienstverlener.

(10) Krachtens deze verordening uitgevaardigde bevelen dienen te worden gericht aan daartoe aangewezen wettelijke vertegenwoordigers van dienstverleners. Wanneer een in de Unie gevestigde dienstverlener geen wettelijke vertegenwoordiger heeft aangewezen, kunnen de bevelen worden gericht aan elke vestiging van de betrokken dienstverlener in de Unie. Deze terugvaloptie beoogt de doeltreffendheid van het systeem te verzekeren in geval de dienstverlener (nog) geen specifieke vertegenwoordiger heeft aangewezen.

(11) Het mechanisme van de Europese bevelen tot verstrekking en bewaring van elektronisch bewijsmateriaal in strafzaken kan alleen werken op basis van een hoog niveau van wederzijds vertrouwen tussen de lidstaten, wat een essentiële voorwaarde vormt voor de goede werking van dit instrument.

(12) Deze verordening eerbiedigt de grondrechten en neemt de beginselen in acht die met name in het Handvest van de grondrechten van de Europese Unie zijn erkend. Het gaat onder meer om het recht op vrijheid en veiligheid, het recht op eerbiediging van het privéleven en het familie- en gezinsleven, de bescherming van persoonsgegevens, de vrijheid van ondernemerschap, het recht op eigendom, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het vermoeden van onschuld en de rechten van verdediging, het legaliteitsbeginsel en evenredigheidsbeginsel, en het recht om niet tweemaal in een strafrechtelijke procedure voor hetzelfde strafbare feit te worden berecht of gestraft. Ingeval de uitvaardigende lidstaat over aanwijzingen beschikt dat in een andere lidstaten mogelijk een parallelle strafprocedure wordt gevoerd, raadpleegt hij de autoriteiten van deze lidstaat overeenkomstig Kaderbesluit 2009/948/JBZ van de Raad[29].

(13) Met het oog op de volledige eerbiediging van de grondrechten verwijst deze verordening uitdrukkelijk naar de noodzakelijke normen betreffende de verkrijging van persoonsgegevens, de verwerking van die gegevens, de rechterlijke toetsing van het gebruik van de onderzoeksmaatregel waarin dit instrument voorziet en de beschikbare rechtsmiddelen.

(14) Deze verordening moet worden toegepast onverminderd de procedurele rechten in strafzaken die zijn vastgesteld bij de Richtlijnen 2010/64/EU[30], 2012/13/EU[31], 2013/48/EU[32], 2016/343[33], 2016/800[34] en 2016/1919[35] van het Europees Parlement en de Raad.

---

29 Kaderbesluit 2009/948/JBZ van de Raad van 30 november 2009 over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures (PB L 328 van 15.12.2009, blz. 42).

30 Richtlijn 2010/64/EU van het Europees Parlement en de Raad van 20 oktober 2010 betreffende het recht op tolk- en vertaaldiensten in strafprocedures (PB L 280 van 26.10.2010, blz. 1).

31 Richtlijn 2012/13/EU van het Europees Parlement en de Raad van 22 mei 2012 betreffende het recht op informatie in strafprocedures (PB L 142 van 1.6.2012, blz. 1).

32 Richtlijn 2013/48/EU van het Europees Parlement en de Raad van 22 oktober 2013 betreffende het recht op toegang tot een advocaat in strafprocedures en in procedures ter uitvoering van een Europees aanhoudingsbevel en het recht om een derde op de hoogte te laten brengen vanaf de vrijheidsbeneming en om met derden en consulaire autoriteiten te communiceren tijdens de vrijheidsbeneming (PB L 294 van 6.11.2013, blz. 1).

33 Richtlijn 2016/343/EU van het Europees Parlement en de Raad van 9 maart 2016 betreffende de versterking van bepaalde aspecten van het vermoeden van onschuld en van het recht om in strafprocedures bij de terechtzitting aanwezig te zijn (PB L 65 van 11.3.2016, blz. 1).

(15) Bij dit instrument worden de regels vastgesteld op grond waarvan een bevoegde justitiële autoriteit in de Europese Unie een dienstverlener die in de Unie diensten aanbiedt, door middel van een Europees verstrekkings- of bewaringsbevel kan gelasten elektronisch bewijs te verstrekken of te bewaren. Deze verordening is van toepassing op alle gevallen waarin de dienstverlener in een andere lidstaat is gevestigd of vertegenwoordigd. Voor binnenlandse situaties waarin de bij deze verordening ingestelde instrumenten niet kunnen worden gebruikt, mag de verordening geen beperking inhouden van de bevoegdheden die het nationale recht de nationale bevoegde instanties reeds biedt om op hun grondgebied gevestigde of vertegenwoordigde dienstverleners te dwingen.

(16) De voor strafrechtelijke procedures meest relevante dienstverleners zijn aanbieders van elektronische-communicatiediensten en specifieke aanbieders van diensten van de informatiemaatschappij die contacten tussen gebruikers mogelijk maken. Bijgevolg dienen beide groepen onder deze verordening te vallen. Aanbieders van elektronische-communicatiediensten worden omschreven in het voorstel voor een richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie. Het gaat onder meer om persoonlijke communicatie zoals diensten op het gebied van voice-over-IP, instant messaging en e-mail. De hier opgenomen categorieën diensten van de informatiemaatschappij zijn die waarvoor de opslag van gegevens een wezenlijk onderdeel is van de aan de gebruiker verleende dienst, en hebben met name betrekking op sociale netwerken voor zover zij niet als elektronische-communicatiediensten kunnen worden aangemerkt, onlinemarktplaatsen die transacties tussen hun gebruikers (zoals consumenten of ondernemingen) mogelijk maken en andere hostingdiensten, ook wanneer de dienst via cloud computing wordt verleend. Diensten van de informatiemaatschappij waarvoor de opslag van gegevens geen bepalend onderdeel is van de aan de gebruiker verleende dienst, en slechts van ondergeschikt belang is, zoals juridische, architectonische, ingenieurs- en accountingdiensten die online op afstand worden verleend, dienen van het toepassingsgebied van deze verordening te worden uitgesloten, zelfs indien zij onder de definitie van diensten van de informatiemaatschappij kunnen vallen, overeenkomstig Richtlijn (EU) 2015/1535.

(17) In veel gevallen worden gegevens niet langer opgeslagen of verwerkt op een apparaat van een gebruiker, maar beschikbaar gemaakt via een cloudgebaseerde infrastructuur die overal vandaan toegankelijk is. Om deze diensten aan te bieden, hoeven dienstverleners niet in een specifiek rechtsgebied te zijn gevestigd of over servers te beschikken. De toepassing van deze verordening mag derhalve niet afhangen van de werkelijke plaats waar de dienstverlener is gevestigd of de opslag- of verwerkingsvoorzieningen zijn gelegen.

(18) Aanbieders van internetinfrastructuurdiensten die verband houden met de toewijzing van namen en nummers, zoals registrators en registers van domeinnamen en aanbieders van privacy- en proxydiensten, of regionale internetregisters van internetprotocol("IP")adressen, zijn met name van belang voor de identificatie van actoren achter kwaadwillige of gecompromitteerde websites. Zij zijn in het bezit van

---

34 Richtlijn (EU) 2016/800 van het Europees Parlement en de Raad van 11 mei 2016 betreffende procedurele waarborgen voor kinderen die verdachte of beklaagde zijn in een strafprocedure (PB L 132 van 21.5.2016, blz. 1).

35 Richtlijn 2016/1919/EU van het Europees Parlement en de Raad van 26 oktober 2016 betreffende rechtsbijstand voor verdachten en beklaagden in strafprocedures en voor gezochte personen in procedures ter uitvoering van een Europees aanhoudingsbevel (PB L 297 van 4.11.2016, blz. 1).

gegevens die voor strafprocedures bijzonder relevant zijn, aangezien dat de identificatie mogelijk maakt van individuen of entiteiten die schuilgaan achter websites die voor criminele activiteiten worden gebruikt, of slachtoffers van criminele activiteiten in het geval van een gecompromitteerde website die door criminelen is gekaapt.

(19) Deze verordening regelt alleen het verzamelen van opgeslagen gegevens, dat wil zeggen de gegevens waarover een dienstverlener beschikt op het moment van ontvangst van het certificaat inzake het Europees verstrekkingsbevel of inzake het Europees bewaringsbevel. Zij legt geen algemene verplichting tot bewaring van gegevens op, en staat evenmin toe dat gegevens worden onderschept of gegevens worden verkregen die zijn opgeslagen na de ontvangst van een certificaat inzake het verstrekkings- of bewaringsbevel. De gegevens moeten worden verstrekt, ongeacht of zij zijn versleuteld.

(20) De categorieën van gegevens die onder deze verordening vallen, omvatten abonneegegevens toegangsgegevens, transactiegegevens (de drie categorieën die worden aangeduid als niet-inhoudelijke gegevens) en inhoudelijke gegevens. Dit onderscheid wordt, zij het niet wat betreft toegangsgegevens, in de wetgeving van veel lidstaten gemaakt, alsook in het rechtskader van VS, dat dienstverleners toestaat op vrijwillige basis niet-inhoudelijke gegevens te delen met buitenlandse rechtshandhavingsinstanties.

(21) Het is passend om toegangsgegevens in deze verordening als een specifieke gegevenscategorie te behandelen. Toegangsgegevens worden met hetzelfde doel verlangd als abonneegegevens, namelijk om de daarachter schuilgaande gebruiker te identificeren, en de grondrechten zijn bij beide categorieën in vergelijkbare mate in het geding. Toegangsgegevens worden doorgaans geregistreerd als onderdeel van een registratie van gebeurtenissen (met andere woorden een serverlog), ter aanduiding van de aanvang en de beëindiging van een toegangssessie van een gebruiker inzake een dienst. Het gaat vaak om een individueel IP-adres (statisch of dynamisch) of andere identificator die de tijdens de toegangssessie gebruikte netwerkinterface aanwijst. Indien de gebruiker onbekend is, dienen deze gegevens vaak te worden verkregen voordat abonneegegevens betreffende die identificator kunnen worden opgevraagd bij de dienstverlener.

(22) Transactiegegevens daarentegen worden doorgaans verlangd om informatie te verkrijgen over de contacten en verblijfplaats van de gebruiker en kunnen dienen om een profiel van een betrokkene op te stellen. Toegangsgegevens op zich kunnen niet dienen voor een soortgelijk doel; zij onthullen bijvoorbeeld geen enkele informatie over gesprekspartners van de gebruiker. Vandaar dat dit voorstel een nieuwe categorie gegevens introduceert, die net als abonneegegevens moeten worden behandeld wanneer het verkrijgen van deze gegevens eenzelfde doel heeft.

(23) Alle gegevenscategorieën bevatten persoonsgegevens en vallen dus onder de waarborgen van het gegevensbeschermingsacquis van de Unie, maar de intensiteit van het effect op de grondrechten varieert, met name tussen abonneegegevens en toegangsgegevens enerzijds en transactiegegevens en inhoudelijke gegevens anderzijds. Terwijl abonneegegevens en toegangsgegevens nuttig zijn om in een onderzoek de eerste aanwijzingen te verkrijgen over de identiteit van een verdachte, zijn transactiegegevens en inhoudelijke gegevens het meest relevant als bewijsmateriaal. Het is derhalve van essentieel belang dat het instrument op al deze gegevenscategorieën van toepassing is. Omdat de mate waarin de grondrechten in het

geding zijn, verschilt, worden verschillende voorwaarden verbonden aan het verkrijgen van abonnee- en toegangsgegevens enerzijds en transactiegegevens en inhoudelijke gegevens anderzijds.

(24) Het Europees verstrekkingsbevel en het Europees bewaringsbevel zijn onderzoeksmaatregelen die uitsluitend mogen worden genomen in het kader van een specifieke strafprocedure tegen de specifieke bekende of nog onbekende daders van een concreet strafbaar feit dat reeds heeft plaatsgevonden, na een individuele beoordeling van de evenredigheid en noodzaak in het individuele geval.

(25) Deze verordening doet geen afbreuk aan de onderzoeksbevoegdheden van autoriteiten in burgerlijke of administratieve procedures, ook wanneer deze procedures tot sancties kunnen leiden.

(26) Deze verordening dient van toepassing te zijn op dienstverleners die diensten aanbieden in de Unie, en de bevelen waarin deze verordening voorziet, mogen alleen worden uitgevaardigd voor gegevens die betrekking hebben op in de Unie aangeboden diensten. Diensten die uitsluitend buiten de Unie worden aangeboden, vallen niet binnen het toepassingsgebied van deze verordening, zelfs niet indien de dienstverlener in de Unie is gevestigd.

(27) Om te bepalen of een dienstverlener diensten aanbiedt in de Unie, dient te worden nagegaan of de dienstverlener rechtspersonen of natuurlijke personen in een of meer lidstaten in staat stelt om zijn diensten te gebruiken. Enkel de toegankelijkheid van een online-interface, zoals de toegankelijkheid van de website van de dienstverlener of een intermediair of van een e-mailadres en van andere contactgegevens, in een of meer lidstaten afzonderlijk, mag echter niet voldoende zijn om de toepassing van deze verordening te rechtvaardigen.

(28) Ook een reële link met de Unie dient relevant te zijn om het toepassingsgebied van deze verordening te bepalen. Een dergelijke reële link met de Unie moet worden geacht te bestaan wanneer de dienstverlener een vestiging heeft in de Unie. Wanneer er geen vestiging in de Unie is, moet de vervulling van het criterium van een reële link worden beoordeeld op basis van het bestaan van een aanzienlijk aantal gebruikers in een of meer lidstaten, of de toespitsing van activiteiten op een of meer lidstaten. De toespitsing van activiteiten op een of meer lidstaten kan worden bepaald op basis van alle relevante omstandigheden, waaronder factoren als het gebruik van een taal of een munteenheid die in een lidstaat algemeen gangbaar is, of de mogelijkheid om goederen of diensten te bestellen. De toespitsing van activiteiten op een lidstaat zou ook kunnen worden afgeleid uit de beschikbaarheid van een applicatie ("app") in de desbetreffende nationale app store, uit het feit dat er plaatselijk wordt geadverteerd of wordt geadverteerd in de taal die in die lidstaat wordt gebruikt, of uit de wijze van beheer van relaties met cliënten, zoals het verstrekken van klantenservice in de taal die in die lidstaat algemeen gangbaar is. Een reële link moet ook worden aangenomen wanneer een dienstverlener zijn activiteiten richt op een of meer lidstaten, als omschreven in artikel 17, lid 1, onder c), van Verordening (EU) nr. 1215/2012 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken[36]. Het verlenen van de dienst met het enkele doel om het

[36] 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).

in Verordening (EU) 2018/302[37] neergelegde discriminatieverbod na te leven, kan daarentegen niet, op die grond alleen, worden beschouwd als het richten of toespitsen van activiteiten op een bepaald grondgebied binnen de Unie.

(29) Een Europees verstrekkingsbevel mag alleen worden uitgevaardigd indien dit noodzakelijk en evenredig is. Bij de beoordeling daarvan moet ermee rekening worden gehouden of het bevel wel beperkt is tot wat noodzakelijk is voor het bereiken van het legitieme doel relevante en noodzakelijke gegevens te verkrijgen om uitsluitend in het individuele geval als bewijsmateriaal te dienen.

(30) Bij het uitvaardigen van een Europees verstrekkings- of bewaringsbevel moet steeds een rechterlijke instantie betrokken zijn, hetzij tijdens de uitvaardigingsprocedure, hetzij tijdens de bekrachtigingsprocedure. Gelet op het gevoeliger karakter van transactiegegevens en inhoudelijke gegevens is bij de uitvaardiging of bekrachtiging van Europese verstrekkingsbevelen betreffende deze gegevens rechterlijke toetsing vereist. Aangezien abonnee- en toegangsgegevens minder gevoelig zijn, kunnen Europese verstrekkingsbevelen voor openbaarmaking van die gegevens ook door bevoegde openbare aanklagers worden uitgevaardigd of bekrachtigd.

(31) Om dezelfde reden moet een onderscheid worden gemaakt met betrekking tot het materiële toepassingsgebied van deze verordening: Bevelen tot verstrekking van abonnee- en toegangsgegevens kunnen voor alle strafbare feiten worden uitgevaardigd, terwijl striktere voorwaarden dienen te gelden voor toegang tot transactiegegevens en inhoudelijke gegevens in verband met het gevoeliger karakter van deze gegevens. Een drempel maakt een meer evenredige aanpak mogelijk, net als een aantal andere in de verordening voorstel opgenomen ex-ante- en ex-postvoorwaarden en waarborgen ter eerbiediging van het evenredigheidsbeginsel en de rechten van de betrokken personen. Een drempel mag echter geen beperking vormen voor de doeltreffendheid van het instrument en het gebruik ervan door beroepsbeoefenaars. Wanneer alleen bevelen mogen worden uitgevaardigd voor onderzoek naar feiten waarop een maximumgevangenisstraf van ten minste drie jaar staat, blijft het toepassingsgebied van het instrument beperkt tot ernstiger misdrijven, zonder dat de mogelijkheden voor het gebruik ervan door beroepsbeoefenaars buitensporig worden ingeperkt. Op die manier wordt een groot aantal strafbare feiten die de lidstaten blijkens de lagere maximumstraffen als minder ernstig beschouwen, van het toepassingsgebied uitgesloten. Een drempel heeft ook het voordeel dat hij gemakkelijk in de praktijk kan worden toegepast.

(32) Er zijn specifieke strafbare feiten waarbij het bewijsmateriaal doorgaans uitsluitend beschikbaar is in elektronische vorm, die een bijzonder vluchtig karakter heeft. Dit is het geval bij cybergerelateerde criminaliteit, ook die welke eventueel op zich niet als ernstig wordt beschouwd, maar die uitgebreide of aanzienlijke schade kan berokkenen, met name in gevallen waarin de individuele gevolgen gering zijn, maar de algehele schade omvangrijk is. In de meeste gevallen waarin het strafbaar feit door middel van een informatiesysteem wordt gepleegd, zou de toepassing van dezelfde drempel als voor andere soorten strafbare feiten, hoofdzakelijk tot straffeloosheid leiden. Dit rechtvaardigt dat de verordening ook wordt toegepast op strafbare feiten waarop

[37] 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).

minder dan 3 jaar gevangenisstraf staat. Daarnaast geldt voor aanvullende terrorismegerelateerde strafbare feiten als omschreven in Richtlijn (EU) 2017/541 de minimumdrempel van 3 jaar maximumstraf niet.

(33) Daarnaast moet ook worden bepaald dat het Europees verstrekkingsbevel alleen mag worden uitgevaardigd wanneer voor hetzelfde strafbare feit in een vergelijkbare binnenlandse situatie in de uitvaardigende staat een soortgelijk bevel beschikbaar is.

(34) In gevallen waarin de verlangde gegevens worden opgeslagen of verwerkt als onderdeel van een infrastructuur die door een dienstverlener wordt verstrekt aan een bedrijf of een andere entiteit die geen natuurlijke persoon is, doorgaans in het geval van hostingdiensten, dient het Europees verstrekkingsbevel uitsluitend te worden gebruikt wanneer andere onderzoeksmaatregelen tegen het bedrijf of de entiteit niet aangewezen zijn, met name wanneer daarmee het onderzoek zou kunnen worden geschaad. Dit is met name van belang wanneer het gaat om grotere entiteiten, zoals ondernemingen of overheidsinstellingen, die gebruikmaken van de diensten van dienstverleners voor de verschaffing van hun IT-bedrijfsinfrastructuur of -diensten of een combinatie van beide. De eerste adressaat van een Europees verstrekkingsbevel dient in dergelijke situaties het bedrijf of de andere entiteit te zijn. Dat bedrijf of deze andere entiteit is mogelijk geen dienstverlener die binnen het toepassingsgebied van deze verordening valt. In gevallen waarin het echter niet opportuun is het bevel aan die entiteit te richten, bijvoorbeeld omdat zij wordt verdacht van betrokkenheid bij de betreffende zaak of er aanwijzingen zijn voor collusie met het oog op het onderzoek, dienen de bevoegde autoriteiten het bevel om de gewenste gegevens te verstrekken, te kunnen richten tot de dienstverlener die de betrokken infrastructuur levert. Deze bepaling doet geen afbreuk aan het recht om de dienstverlener te bevelen de gegevens te bewaren.

(35) Voorrechten en immuniteiten, die zowel betrekking kunnen hebben op categorieën personen (zoals diplomaten) als op specifiek beschermde relaties (zoals de vertrouwelijkheid van de communicatie tussen advocaat en cliënt), worden ook vermeld in andere instrumenten inzake wederzijdse erkenning, zoals het Europees onderzoeksbevel. Het bereik en de gevolgen ervan verschillen naargelang van het toepasselijke nationale recht waarmee rekening moet worden gehouden op het tijdstip van de uitvaardiging van het bevel, aangezien de uitvaardigende autoriteit het bevel slechts kan uitvaardigen indien een soortgelijk bevel beschikbaar zou zijn in een vergelijkbare binnenlandse situatie. Naast dit basisbeginsel moet in de uitvaardigende staat met voorrechten en immuniteiten die in de lidstaat van de dienstverlener toegangsgegevens, transactiegegevens en inhoudelijke gegevens beschermen, zoveel mogelijk op dezelfde wijze rekening worden gehouden als wanneer zij krachtens het nationale recht van de uitvaardigende staat zouden gelden. Dit is met name relevant indien het recht van de lidstaat waar het bevel aan de dienstverlener of zijn wettelijke vertegenwoordiger wordt geadresseerd, in een hoger niveau van bescherming voorziet dan het recht van de uitvaardigende staat. De bepaling zorgt ook voor bescherming van de gevallen waarin de openbaarmaking van de gegevens de fundamentele belangen van die lidstaat, zoals nationale veiligheid en defensie, zou kunnen aantasten. Als extra waarborg dient met deze aspecten niet alleen rekening te worden gehouden bij het uitvaardigen van het bevel, maar ook daarna, wanneer de relevantie en de ontvankelijkheid van de betrokken gegevens in de relevante fase van de strafprocedure worden beoordeeld en, wanneer een tenuitvoerleggingsprocedure plaatsvindt, door een tenuitvoerleggingsautoriteit.

(36) Het Europees bewaringsbevel kan voor elk strafbaar feit worden uitgevaardigd. Het heeft als doel te voorkomen dat relevante gegevens worden verwijderd, gewist of gewijzigd in situaties waarin het bewerkstelligen van de verstrekking van deze gegevens meer tijd kan kosten, bijvoorbeeld omdat er gebruik zal worden gemaakt van kanalen voor justitiële samenwerking.

(37) Europese verstrekkings- en bewaringsbevelen dienen te worden gericht aan de door de dienstverlener aangewezen wettelijke vertegenwoordiger. Wanneer er geen wettelijke vertegenwoordiger is aangewezen, kunnen bevelen aan een vestiging van de dienstverlener in de Unie worden gericht. Dit kan het geval zijn wanneer er geen wettelijke verplichting voor de dienstverlener bestaat om een wettelijke vertegenwoordiger aan te wijzen. Ingeval de wettelijke vertegenwoordiger zijn verplichting in noodsituaties niet nakomt, kan het Europees verstrekkings- of bewaringsbevel ook worden gericht aan de dienstverlener, naast of in plaats van handhaving van het oorspronkelijke bevel overeenkomstig artikel 14. Ingeval de wettelijke vertegenwoordiger zijn verplichting niet nakomt in andere situaties dan noodsituaties, maar waarin er duidelijke risico's bestaan dat gegevens verloren zullen gaan, kan een Europees verstrekkings- of bewaringsbevel ook worden gericht aan elke vestiging van de dienstverlener in de Unie. Vanwege deze verschillende mogelijke scenario’s, wordt de algemene term "adressaat" in de bepalingen gebruikt. Wanneer een verplichting, zoals die inzake vertrouwelijkheid, niet alleen geldt voor de adressaat, maar ook voor de dienstverlener, indien deze niet de adressaat is, wordt dit in de betrokken bepaling vermeld.

(38) Europese verstrekkings- en bewaringsbevelen dienen aan de dienstverlener te worden doorgegeven door middel van een certificaat inzake het Europees verstrekkingsbevel (CEV) of een certificaat inzake het Europees bewaringsbevel (CEB), dat dient te worden vertaald. De certificaten dienen dezelfde verplichte informatie te bevatten als de bevelen, met uitzondering van de gronden voor de noodzaak en de evenredigheid van de maatregel of verdere bijzonderheden over de zaak, teneinde het onderzoek niet in gevaar te brengen. Aangezien deze echter onderdeel vormen van het bevel zelf, kunnen zij door de verdachte later tijdens de strafprocedure worden aangevochten. Waar nodig dient een certificaat te worden vertaald in (één van) de officiële ta(a)l(en) van de lidstaat van de adressaat, of in een andere officiële taal die de dienstverlener heeft aangegeven te zullen aanvaarden.

(39) De bevoegde uitvaardigende autoriteit dient het CEV of het CEB rechtstreeks aan de adressaat door te geven, op zodanige wijze dat dit schriftelijk kan worden vastgelegd en de dienstverlener de echtheid ervan kan vaststellen, zoals bij aangetekende brief, beveiligde e-mail en platforms of andere beveiligde kanalen, met inbegrip van die welke door de dienstverlener ter beschikking worden gesteld, in overeenstemming met de regels voor de bescherming van persoonsgegevens.

(40) De gevraagde gegevens dienen binnen 10 dagen na ontvangst van het CEV aan de autoriteiten te worden doorgegeven. De dienstverlener dient kortere termijnen in acht te nemen in noodgevallen en wanneer de uitvaardigende autoriteit andere redenen aangeeft om af te wijken van de termijn van 10 dagen. Naast het onmiddellijke gevaar dat de gevraagde gegevens worden gewist, kunnen ook met een lopend onderzoek verband houdende omstandigheden een dergelijke reden vormen, bijvoorbeeld wanneer de gevraagde gegevens verband houden met andere dringende onderzoeksmaatregelen die niet kunnen worden uitgevoerd zonder de ontbrekende gegevens of anderszins daarvan afhangen.

(41) Om dienstverleners in staat te stellen formele problemen aan te pakken, is het nodig te voorzien in een procedure voor de communicatie tussen de dienstverlener en de uitvaardigende rechterlijke autoriteit in gevallen waarin het CEV mogelijk onvolledig is, kennelijke fouten bevat of onvoldoende informatie bevat voor de uitvoering van het bevel. Mocht de dienstverlener om een andere reden de informatie niet volledig of niet op tijd verstrekken, bijvoorbeeld omdat hij van oordeel is dat er sprake is van een conflict met een verplichting krachtens het recht van een derde land, of omdat hij meent dat het Europees verstrekkingsbevel niet is uitgevaardigd overeenkomstig de voorwaarden van deze verordening, dient hij zich te wenden tot de uitvaardigende autoriteit en passende redenen aan te voeren. Derhalve moet de communicatieprocedure voorzien in ruime mogelijkheden voor de correctie of heroverweging van het CEV door de uitvaardigende autoriteit in een vroeg stadium. Om de beschikbaarheid van de gegevens te garanderen, moet de dienstverlener de gegevens bewaren als hij kan vaststellen welke gegevens worden gezocht.

(42) Na ontvangst van een certificaat inzake het Europees bewaringsbevel ("CEB") moet de dienstverlener de gevraagde gegevens ten hoogste 60 dagen bewaren, tenzij de uitvaardigende autoriteit de dienstverlener in kennis stelt van het feit dat zij de procedure heeft aangevangen voor de uitvaardiging van een aansluitend verstrekkingsverzoek, in welk geval de bewaring moet worden voortgezet. De termijn van 60 dagen moet de indiening van een officieel verzoek mogelijk maken. Dit houdt in dat er op zijn minst een aantal formele stappen moeten zijn genomen, zoals het versturen van een verzoek om wederzijdse rechtshulp ter vertaling. Na ontvangst van die informatie moeten de gegevens worden bewaard zolang dat nodig is in afwachting van de verstrekking van de gegevens in het kader van een aansluitend verstrekkingsverzoek.

(43) Dienstverleners en hun wettelijke vertegenwoordigers dienen de vertrouwelijkheid te waarborgen en moeten, wanneer de uitvaardigende autoriteit daarom verzoekt, ervan afzien de persoon wiens gegevens worden verlangd, te informeren, teneinde het strafonderzoek te beschermen, in overeenstemming met artikel 23 van Verordening (EU) 2016/679[38]. Gebruikersinformatie is echter een essentieel element om toetsing en beroep in rechte mogelijk te maken en dient, wanneer er geen risico bestaat dat de lopende onderzoeken in gevaar worden gebracht, door de autoriteit te worden verstrekt indien de dienstverlener werd gevraagd de gebruiker niet in kennis te stellen, overeenkomstig de nationale maatregel tot omzetting van artikel 13 van Richtlijn (EU) 2016/680[39].

(44) Ingeval de adressaat het bevel niet naleeft, kan de uitvaardigende autoriteit het volledige bevel, met inbegrip van de motivering van de noodzaak en de evenredigheid, vergezeld van het certificaat, doorgeven aan de bevoegde autoriteit van de lidstaat waar de adressaat van het certificaat verblijft of is gevestigd. Deze lidstaat dient het ten uitvoer te leggen overeenkomstig zijn nationaal recht. De lidstaten moeten

---

38 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

39 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens, en intrekking van het Kaderbesluit van de Raad 2008/977/JBZ (PB L 119 van 4.5.2016, blz. 89).

voorzien in doeltreffende, evenredige en afschrikkende geldelijke sancties in geval van inbreuk op de verplichtingen uit hoofde van deze verordening.

(45) De tenuitvoerleggingsprocedure is een procedure waarin de adressaat bezwaar kan maken tegen de tenuitvoerlegging op basis van een beperkt aantal gronden. De tenuitvoerleggingsautoriteit kan weigeren het bevel te erkennen en ten uitvoer te leggen op basis van dezelfde gronden, of indien er krachtens zijn nationaal recht voorrechten en immuniteiten van toepassing zijn of de openbaarmaking de fundamentele belangen van de staat, zoals nationale veiligheid en defensie, zou kunnen aantasten. De tenuitvoerleggingsautoriteit moet de uitvaardigende autoriteit raadplegen alvorens op basis van deze gronden het bevel te erkennen of ten uitvoer te leggen. In geval van niet-naleving kunnen de autoriteiten sancties opleggen. Deze sancties moeten evenredig zijn, ook in het licht van specifieke omstandigheden, zoals herhaalde of systematische niet-naleving.

(46) Onverminderd hun verplichtingen inzake gegevensbescherming mogen dienstverleners niet aansprakelijk worden gesteld in de lidstaten voor schade van hun gebruikers of derden die uitsluitend voortkomt uit het te goeder trouw naleven van een CEV of een CEB.

(47) Naast de personen van wie de gegevens worden gevraagd, kunnen ook de dienstverleners en derde landen door de onderzoeksmaatregel worden getroffen. Om de courtoisie ten aanzien van de soevereine belangen van derde landen te waarborgen, de betrokkene te beschermen en tegenstrijdige verplichtingen voor dienstverleners aan te pakken, voorziet dit instrument in een mechanisme voor rechterlijke toetsing wanneer de naleving van een Europees verstrekkingsbevel dienstverleners zou beletten een wettelijke verplichting uit hoofde van het recht van een derde staat na te leven.

(48) Te dien einde moet een adressaat, wanneer hij van mening is dat het Europees verstrekkingsbevel in het specifieke geval zou leiden tot de schending van een wettelijke verplichting die voortvloeit uit het recht van een derde land, de uitvaardigende autoriteit door middel van een gemotiveerd bezwaar informeren met gebruikmaking van de daarvoor bestemde formulieren. De uitvaardigende autoriteit moet dan het Europees verstrekkingsbevel toetsen in het licht van het gemotiveerde bezwaar, rekening houdend met dezelfde criteria die de bevoegde rechtbank in acht zou moeten nemen. Wanneer de autoriteit besluit het bevel in stand te houden, dient de procedure te worden doorverwezen naar de bevoegde rechtbank, zoals aangewezen door de desbetreffende lidstaat, die vervolgens het bevel beoordeelt.

(49) Om te bepalen of er sprake is van een tegenstrijdige verplichting in de specifieke omstandigheden van de onderzochte zaak, dient de bevoegde rechter waar nodig een beroep te doen op passende externe deskundigheid, bijvoorbeeld wanneer bij de toetsing vragen rijzen over de uitlegging van het recht van het betrokken derde land. Dit kan onder meer door de centrale autoriteiten van dat land te raadplegen.

(50) Deskundigheid op het gebied van uitlegging zou ook kunnen worden verkregen door middel van adviezen van deskundigen, indien deze beschikbaar zijn. Informatie en jurisprudentie over de uitlegging van het recht van derde landen en over collusieprocedures? in de lidstaten dienen beschikbaar te worden gesteld op een centraal platform, zoals het Siriusproject en/of het Europees justitieel netwerk. Op die manier kunnen rechterlijke instanties gebruik maken van de ervaring en deskundigheid die andere rechtbanken hebben opgedaan inzake dezelfde of soortgelijke kwesties. Dit mag niet beletten dat de derde staat waar nodig opnieuw wordt geraadpleegd.

(51) Wanneer er sprake is van tegenstrijdige verplichtingen, dient de rechtbank te bepalen of de tegenstrijdige bepalingen van het derde land de openbaarmaking van de betrokken gegevens beletten omdat de bescherming van de grondrechten van de betrokken personen of de fundamentele belangen van het derde land in verband met de nationale veiligheid of defensie, daarom vragen. Bij deze beoordeling moet de rechtbank in aanmerking nemen of het recht van het derde land niet zozeer de grondrechten of fundamentele belangen van het derde land op het gebied van nationale veiligheid of verdediging beoogt te beschermen, als wel er kennelijk op is gericht andere belangen te beschermen of illegale activiteiten af te schermen tegen verzoeken om rechtshandhaving in het kader van strafrechtelijk onderzoek. Wanneer de rechtbank tot de conclusie komt dat tegenstrijdige bepalingen van het derde land de openbaarmaking van de betrokken gegevens beletten omdat de bescherming van de fundamentele rechten van de betrokken personen of de fundamentele belangen van het derde land in verband met de nationale veiligheid of defensie, daarom vragen, dient zij het derde land te raadplegen via zijn centrale autoriteiten, die al bijna overal ter wereld in het kader van wederzijdse rechtshulp bestaan. De rechtbank dient een termijn vast te stellen waarbinnen het derde land bezwaar moet maken tegen de uitvoering van het Europees verstrekkingsbevel; indien de autoriteiten van het derde land niet reageren binnen de (verlengde) termijn, ondanks een aanmaning waarin zij in kennis worden gesteld van de gevolgen van het niet verstrekken van een antwoord, houdt de rechtbank het bevel in stand. Indien de autoriteiten van het derde land bezwaar maken tegen de openbaarmaking, dient de rechtbank het bevel in te trekken.

(52) In alle andere gevallen van tegenstrijdige verplichtingen die geen verband houden met fundamentele rechten van de betrokkene of fundamentele belangen van het derde land in verband met de nationale veiligheid of defensie, dient de rechtbank bij haar beslissing over het al dan niet in stand houden van het Europees verstrekkingsbevel een aantal elementen af te wegen die bedoeld zijn voor het vaststellen van de sterkte van de band met een van de twee betrokken jurisdicties, de respectieve belangen bij het verkrijgen van de gegevens of juist het voorkomen van de openbaarmaking daarvan, en de mogelijke gevolgen van de naleving van het bevel voor de dienstverlener. Belangrijk bij cybergerelateerde strafbare feiten is dat de plaats waar het strafbare feit werd gepleegd, zowel de plaats(en) omvat waar de handeling werd verricht, als de plaats(en) waar de effecten van het strafbare feit zijn ingetreden.

(53) De in artikel 9 bedoelde voorwaarden zijn ook van toepassing wanneer er sprake is van tegenstrijdige verplichtingen die voortvloeien uit het recht van een derde land. Tijdens deze procedure dienen de gegevens te worden bewaard. Indien het bevel wordt ingetrokken, kan een nieuw bewaringsbevel worden uitgevaardigd waarmee de uitvaardigende autoriteit de verstrekking van gegevens via andere kanalen, zoals wederzijdse rechtshulp, kan pogen te verkrijgen.

(54) Het is van essentieel belang dat alle personen wier gegevens worden opgevraagd in het kader van een strafrechtelijk onderzoek of een strafprocedure, toegang hebben tot een doeltreffende voorziening in rechte, overeenkomstig artikel 47 van het Handvest van de grondrechten van de Europese Unie. Voor verdachten en beklaagden dient het recht op een doeltreffende voorziening in rechte te worden uitgeoefend tijdens de strafprocedure. Dit kan van invloed zijn op de ontvankelijkheid of, naar gelang van het geval, het gewicht in de procedure van het op die manier verkregen bewijsmateriaal. Bovendien genieten zij alle procedurele waarborgen die op hen van toepassing zijn, zoals het recht op informatie. Andere personen die geen verdachte of beklaagde zijn, dienen ook recht te hebben op een doeltreffende voorziening in rechte. Daarom moet

ten minste worden voorzien in de mogelijkheid om de rechtmatigheid van een Europees verstrekkingsbevel te betwisten, met inbegrip van de noodzaak en de evenredigheid van het bevel. Deze verordening mag geen beperking inhouden van de mogelijke gronden tot betwisting van de rechtmatigheid van het bevel. Van deze rechtsmiddelen dient gebruik te worden gemaakt in de uitvaardigende staat overeenkomstig het nationale recht. Regels inzake voorlopige maatregelen moeten door het nationale recht worden beheerst.

(55) Bovendien kan de adressaat tijdens de tenuitvoerleggingsprocedure en bij de daaropvolgende voorziening in rechte, de tenuitvoerlegging van een Europees verstrekkings- of bewaringsbevel op een beperkt aantal gronden aanvechten, waaronder het feit dat het niet door een bevoegde autoriteit is uitgevaardigd of bekrachtigd of het feit dat het kennelijk in strijd is met het Handvest van de grondrechten van de Europese Unie of kennelijk misbruik oplevert. Een bevel bijvoorbeeld, waarbij wordt gevraagd inhoudelijke gegevens te verstrekken met betrekking tot een onbepaalde kring van personen in een geografisch gebied of zonder link met concrete strafprocedures zou op kennelijke wijze de voorwaarden negeren voor de uitvaardiging van een Europees verstrekkingsbevel.

(56) De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. Krachtens artikel 8, lid 1, van het Handvest van de grondrechten van de Europese Unie en artikel 16, lid 1, van het VWEU heeft eenieder recht op bescherming van zijn persoonsgegevens. Bij de implementatie van deze verordening dienen de lidstaten ervoor te zorgen dat persoonsgegevens worden beschermd en uitsluitend mogen worden verwerkt overeenkomstig Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680.

(57) De krachtens deze verordening verkregen persoonsgegevens moeten uitsluitend worden verwerkt als dat nodig is voor en in verhouding staat tot de doeleinden inzake het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties en de uitoefening van de rechten van de verdediging. De lidstaten moeten er met name voor zorgen dat een passend gegevensbeschermingsbeleid en passende gegevensbeschermingsmaatregelen van toepassing zijn op de doorgifte van persoonsgegevens door bevoegde autoriteiten aan dienstverleners voor de toepassing van deze verordening, met inbegrip van maatregelen om de beveiliging van de gegevens te waarborgen. Dienstverleners moeten ervoor zorgen dat dit ook het geval is voor de doorgifte van persoonsgegevens aan bevoegde autoriteiten. Alleen bevoegde personen mogen via een authenticatieprocedure toegang hebben tot informatie die persoonsgegevens bevat. Het gebruik dient te worden overwogen van mechanismen die authenticiteit waarborgen, zoals aangemelde nationale systemen voor elektronische identificatie of vertrouwensdiensten, overeenkomstig 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.

(58) De Commissie moet een evaluatie van deze verordening uitvoeren, die dient te zijn gebaseerd op de vijf criteria doelmatigheid, doeltreffendheid, relevantie, samenhang en meerwaarde voor de EU, en de basis dient te vormen voor effectbeoordelingen van opties voor eventuele verdere maatregelen. Er dient regelmatig informatie te worden verzameld, waarmee bij de evaluatie van deze verordening rekening kan worden gehouden.

(59) Het gebruik van vooraf vertaalde standaardformulieren vergemakkelijkt de samenwerking en de uitwisseling van informatie tussen de justitiële autoriteiten en dienstverleners, zodat zij elektronisch bewijsmateriaal sneller en doeltreffender kunnen beveiligen en doorgeven, en tegelijkertijd op een gebruikersvriendelijke manier kunnen voldoen aan de nodige veiligheidsvoorschriften. Dit leidt tot lagere vertaalkosten en draagt bij tot een hoge kwaliteit. Op dezelfde wijze zouden antwoordformulieren een gestandaardiseerde uitwisseling van informatie mogelijk moeten maken, met name wanneer dienstverleners niet in staat zijn om het bevel na te leven, omdat de account niet bestaat of omdat er geen gegevens beschikbaar zijn. De formulieren zouden ook het verzamelen van statistische gegevens moeten vergemakkelijken.

(60) Teneinde doeltreffend te voorzien in een eventuele behoefte aan verbetering van de inhoud van een CEV, een CEB of van het formulier dat moet worden gebruikt om informatie te verstrekken over de onmogelijkheid om het CEV of CEB uit te voeren, moet, overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie, aan de Commissie de bevoegdheid worden gedelegeerd om handelingen vast te stellen tot wijziging van de bijlagen I, II en III bij deze verordening. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen plaatsvinden in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel akkoord van 13 april 2016 over beter wetgeven[40]. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

(61) De op deze verordening gebaseerde maatregelen mogen niet prevaleren boven Europese onderzoeksbevelen overeenkomstig Richtlijn 2014/41/EU van het Europees Parlement en de Raad[41] voor het verkrijgen van elektronische bewijsmateriaal. De autoriteiten van de lidstaten dienen het instrument te kiezen dat het best past bij hun situatie; het is mogelijk dat zij de voorkeur geven aan het gebruik van het Europees onderzoeksbevel wanneer zij een reeks van verschillende soorten onderzoeksmaatregelen verlangen, met inbegrip van, maar niet beperkt tot de verstrekking van elektronisch bewijsmateriaal uit een andere lidstaat.

(62) Als gevolg van technologische ontwikkelingen kunnen binnen een paar jaar nieuwe vormen van communicatie gangbaar zijn of kunnen er leemtes ontstaan in de toepassing van deze verordening. Daarom is het belangrijk te voorzien in een evaluatie van de toepassing ervan.

(63) Daar de doelstelling van deze verordening, namelijk het beter grensoverschrijdend veiligstellen en verkrijgen van elektronisch bewijsmateriaal, niet voldoende door de lidstaten kan worden verwezenlijkt gelet op het grensoverschrijdende karakter ervan, maar beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde

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

[41] Richtlijn 2014/41/EU van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken, PB L 130 van 1.5.2014, blz. 1.

subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel, gaat deze verordening niet verder dan nodig is om deze doelstellingen te verwezenlijken.

(64) Overeenkomstig artikel 3 van het Protocol betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie is gehecht, *[heeft het Verenigd Koninkrijk/Ierland laten weten dat het wenst deel te nemen aan de aanneming en toepassing van deze verordening] of [neemt het Verenigd Koninkrijk/Ierland, onverminderd artikel 4 van dat protocol, niet deel aan de aanneming van deze verordening, die derhalve niet bindend is voor, noch van toepassing is op deze lidstaat.]*.

(65) Overeenkomstig de artikelen 1 en 2 van Protocol nr. 22 betreffende de positie van Denemarken, gehecht aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, neemt Denemarken niet deel aan de vaststelling van deze verordening, die derhalve niet bindend is voor, noch van toepassing is op deze lidstaat.

(66) De Europese Toezichthouder voor gegevensbescherming werd geraadpleegd in overeenstemming met artikel 28, lid 2, van Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad[42] en heeft op [...] advies uitgebracht[43],

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Hoofdstuk 1: Onderwerp, definities en toepassingsgebied

Artikel 1
Onderwerp

1. Bij deze verordening worden de regels vastgesteld op grond waarvan een autoriteit van een lidstaat een dienstverlener die in de Unie diensten aanbiedt, kan bevelen elektronisch bewijsmateriaal te verstrekken of te bewaren, ongeacht de locatie van de gegevens. Deze verordening doet geen afbreuk aan de bevoegdheden van de nationale autoriteiten om op hun grondgebied gevestigde of vertegenwoordigde dienstverleners te dwingen om soortgelijke nationale maatregelen na te leven.

2. Deze verordening geldt onverminderd de verplichting tot eerbiediging van de grondrechten en de rechtsbeginselen die zijn neergelegd in artikel 6 VEU, inclusief het recht op verdediging van personen tegen wie een strafprocedure loopt, en laat alle verplichtingen die in dat verband op de rechtshandhavingsautoriteiten of rechterlijke autoriteiten rusten, onverlet.

---

42 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

43 PB C van , blz. .

Artikel 2
Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "Europees verstrekkingsbevel": een bindende beslissing van een uitvaardigende autoriteit van een lidstaat waarbij een dienstverlener die in de Unie diensten aanbiedt en in een andere lidstaat is gevestigd of vertegenwoordigd, wordt gedwongen elektronisch bewijsmateriaal te verstrekken;

(2) "Europees bewaringsbevel": een bindende beslissing van een uitvaardigende autoriteit van een lidstaat waarbij een dienstverlener die in de Unie diensten aanbiedt en in een andere lidstaat is gevestigd of vertegenwoordigd, wordt gedwongen elektronisch bewijsmateriaal te bewaren met het oog op een aansluitend verzoek om verstrekking;

(3) "dienstverlener": een natuurlijke of rechtspersoon die een of meer van de volgende categorieën diensten aanbiedt:

(a) elektronische-communicatiediensten zoals omschreven in artikel 2, lid 4, van de [richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie];

(b) diensten van de informatiemaatschappij zoals omschreven in artikel 1, lid 1, onder b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad[44], waarbij gegevensopslag een wezenlijk onderdeel is van de aan de gebruiker aangeboden dienst, met inbegrip van sociale netwerken, onlinemarktplaatsen die transacties tussen hun gebruikers mogelijk maken, en andere hostingdiensten;

(c) diensten in verband met internet domeinnamen en IP-nummering, zoals aanbieders van IP-adressen, domeinnaamregistrators en -registers en aanverwante privacy- en proxydiensten;

(4) "diensten aanbieden in de Unie":

(a) natuurlijke of rechtspersonen in een of meer lidstaten in staat stellen om gebruik te maken van de onder punt 3) hierboven vermelde diensten; en

(b) waarbij er een reële link is met de onder a) bedoelde lidsta(a)t(en);

(5) "vestiging": de daadwerkelijke uitoefening van een economische activiteit voor onbepaalde tijd door middel van een duurzame infrastructuur van waaruit diensten worden verleend, of een duurzame infrastructuur van waaruit de activiteiten worden beheerd;

(6) "elektronisch bewijsmateriaal": bewijsmateriaal dat op het tijdstip van ontvangst van een certificaat inzake het verstrekkings- of bewaringsbevel door of namens een dienstverlener in elektronische vorm is opgeslagen en dat bestaat uit opgeslagen abonneegegevens, toegangsgegevens, transactiegegevens en inhoudelijke gegevens;

(7) "abonneegegevens": gegevens die betrekking hebben op:

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

(a) de identiteit van een abonnee of klant, zoals opgegeven naam, geboortedatum, postadres of geografisch adres, facturatie- en betalingsgegevens, telefoonnummer of e-mailadres;

(b) de aard en de duur van de dienst, met inbegrip van technische gegevens en gegevens ter identificatie van gerelateerde technische maatregelen of interfaces die worden gebruikt door of verstrekt aan de abonnee of klant, en gegevens met betrekking tot de validering van het gebruik van de dienst, met uitzondering van wachtwoorden of andere authenticatiemiddelen die in plaats van een wachtwoord worden gebruikt en door een gebruiker worden verstrekt of op zijn verzoek worden gecreëerd;

(8) "toegangsgegevens": gegevens die verband houden met de aanvang en de beëindiging van een toegangssessie van een gebruiker inzake een dienst, die strikt noodzakelijk zijn voor het uitsluitende doel de gebruiker van de dienst te identificeren, zoals de datum en het tijdstip van het gebruik, of het inloggen in en het uitloggen uit de dienst, samen met het IP-adres dat door de aanbieder van een internettoegangsdienst aan de gebruiker van de dienst is toegewezen, gegevens ter identificatie van de gebruikte interface en de gebruikers-ID. Daaronder vallen ook elektronische-communicatiemetagegevens zoals gedefinieerd in artikel 4, lid 3, onder c), van [de verordening betreffende de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie];

(9) "transactiegegevens": gegevens in verband met de verlening van een dienst die door een dienstverlener wordt aangeboden, die dienen om achtergrondinformatie of aanvullende informatie over die dienst te verstrekken en door een informatiesysteem van de dienstverlener zijn gegenereerd of verwerkt, zoals de herkomst en de bestemming van een bericht of een ander type interactie, gegevens betreffende de locatie van het apparaat, de datum, het tijdstip, de duur, de omvang, de route, de vorm, het gebruikte protocol en het type compressie, tenzij die gegevens toegangsgegevens zijn. Daaronder vallen ook elektronische-communicatiemetagegevens zoals gedefinieerd in artikel 4, lid 3, onder c), van [de verordening betreffende de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie];

(10) "inhoudelijke gegevens": andere gegevens dan abonneegegevens, toegangsgegevens of transactiegegeven die in digitale vorm zijn opgeslagen, zoals tekst, spraak, video, beelden en geluid;

(11) "informatiesysteem": informatiesysteem zoals gedefinieerd in artikel 2, onder a), van Richtlijn 2013/40/EU van het Europees Parlement en de Raad[45].

(12) "uitvaardigende staat": de lidstaat waar het Europees verstrekkingsbevel of het Europees bewaringsbevel is uitgevaardigd;

(13) "tenuitvoerleggingsstaat": de lidstaat waar de adressaat van het Europees verstrekkingsbevel of het Europees bewaringsbevel verblijft of is gevestigd en waaraan het Europees verstrekkingsbevel en het certificaat inzake het Europees verstrekkingsbevel of het Europees bewaringsbevel en het certificaat inzake het Europees bewaringsbevel voor tenuitvoerlegging worden doorgegeven;

---

[45] Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PB L 218 van 14.8.2013, blz. 8).

(14) "tenuitvoerleggingsautoriteit": de bevoegde autoriteit in de tenuitvoerleggingsstaat waaraan het Europees verstrekkingsbevel en het certificaat inzake het Europees verstrekkingsbevel of het Europees bewaringsbevel en het certificaat inzake het Europees bewaringsbevel door de uitvaardigende autoriteit voor tenuitvoerlegging worden doorgegeven;

(15) "noodgevallen": situaties waarin sprake is van een onmiddellijke bedreiging voor iemands leven of fysieke integriteit of voor een kritieke infrastructuur in de zin van artikel 2, onder a), van Richtlijn 2008/114/EG van de Raad[46].

Artikel 3
Toepassingsgebied

1. Deze verordening is van toepassing op dienstverleners die diensten aanbieden in de Unie.

2. Het Europees verstrekkingsbevel en het Europees bewaringsbevel kunnen uitsluitend voor strafprocedures worden uitgevaardigd, zowel in de fase vóór het proces als tijdens het proces. De bevelen kunnen ook worden uitgevaardigd in een procedure betreffende een strafbaar feit waarvoor een rechtspersoon in de uitvaardigende staat aansprakelijk kan zijn of kan worden bestraft.

3. De bevelen waarin deze verordening voorziet, kunnen uitsluitend worden uitgevaardigd voor gegevens die betrekking hebben op in de Unie aangeboden diensten zoals gedefinieerd in artikel 2, punt 3.

Hoofdstuk 2: Europees verstrekkingsbevel, Europees bewaringsbevel en certificaten

Artikel 4
Uitvaardigende autoriteit

1. Een Europees verstrekkingsbevel voor abonneegegevens en toegangsgegevens kan worden uitgevaardigd door:

   (a) een in de zaak bevoegde rechter, rechtbank, onderzoeksrechter of openbare aanklager; of

   (b) iedere andere door de uitvaardigende staat aangeduide bevoegde autoriteit, die in de zaak in kwestie optreedt als strafrechtelijke onderzoeksautoriteit en overeenkomstig het nationale recht bevoegd is opdracht te geven tot bewijsgaring. Een dergelijk Europees verstrekkingsbevel wordt, nadat is nagegaan of het voldoet aan de krachtens deze verordening geldende voorwaarden voor de uitvaardiging van een Europees verstrekkingsbevel, bekrachtigd door een rechter, rechtbank, onderzoeksrechter of openbare aanklager in de uitvaardigende staat.

[46] Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (PB L 345 van 23.12.2008, blz. 75).

2. Een Europees verstrekkingsbevel inzake transactiegegevens en inhoudelijke gegevens kan uitsluitend worden uitgevaardigd door:

(a) een in de zaak bevoegde rechter, rechtbank of onderzoeksrechter; of

(b) iedere andere door de uitvaardigende staat aangeduide bevoegde autoriteit, die in de zaak in kwestie optreedt als strafrechtelijke onderzoeksautoriteit en overeenkomstig het nationale recht bevoegd is opdracht te geven tot bewijsgaring. Een dergelijk Europees verstrekkingsbevel wordt, nadat is nagegaan of het voldoet aan de krachtens deze verordening geldende voorwaarden voor de uitvaardiging van een Europees verstrekkingsbevel, bekrachtigd door een rechter, rechtbank of onderzoeksrechter in de uitvaardigende staat.

3. Een Europees bewaringsbevel kan worden uitgevaardigd door:

(a) een in de zaak bevoegde rechter, rechtbank, onderzoeksrechter of openbare aanklager; of

(b) iedere andere door de uitvaardigende staat aangeduide bevoegde autoriteit, die in de zaak in kwestie optreedt als strafrechtelijke onderzoeksautoriteit en overeenkomstig het nationale recht bevoegd is opdracht te geven tot bewijsgaring. Een dergelijk Europees bewaringsbevel wordt, nadat is nagegaan of het voldoet aan de krachtens deze verordening geldende voorwaarden voor de uitvaardiging van een Europees bewaringsbevel, bekrachtigd door een rechter, rechtbank, onderzoeksrechter of openbare aanklager in de uitvaardigende staat.

4. Wanneer het bevel overeenkomstig lid 1, onder b), lid 2, onder b), en lid 3, onder b), door een rechterlijke autoriteit is bekrachtigd, kan deze autoriteit ook als een uitvaardigende autoriteit worden beschouwd voor de doorgifte van het certificaat inzake het Europees verstrekkingsbevel en het certificaat inzake het Europees bewaringsbevel.

Artikel 5

Voorwaarden voor het uitvaardigen van een Europees verstrekkingsbevel

1. Een uitvaardigende autoriteit kan een Europees verstrekkingsbevel slechts uitvaardigen wanneer alle in dit artikel beschreven voorwaarden zijn vervuld.

2. Het Europees verstrekkingsbevel is noodzakelijk en evenredig met het oog op de in artikel 3, lid 2, bedoelde procedures en kan slechts worden uitgevaardigd indien een soortgelijke maatregel beschikbaar zou zijn voor hetzelfde strafbare feit in een vergelijkbare binnenlandse situatie in de uitvaardigende staat.

3. Europese verstrekkingsbevelen inzake abonneegegevens of toegangsgegevens kunnen voor alle strafbare feiten worden uitgevaardigd.

4. Europese verstrekkingsbevelen inzake transactiegegevens of inhoudelijke gegevens, kunnen slechts worden uitgevaardigd

(a) voor strafbare feiten waarop in de uitvaardigende staat een vrijheidsstraf staat met een maximum van ten minste 3 jaar, of

(b) voor de volgende strafbare feiten, indien zij geheel of gedeeltelijk zijn gepleegd door middel van een informatiesysteem:

– strafbare feiten zoals gedefinieerd in de artikelen 3, 4 en 5 van Kaderbesluit 2001/413/JHA van de Raad[47];

– strafbare feiten zoals gedefinieerd in de artikelen 3 tot en met 7 van Richtlijn 2011/93/EU van het Europees Parlement en de Raad;[48]

– strafbare feiten zoals gedefinieerd in de artikelen 3 tot en met 8 van Richtlijn 2013/40/EU van het Europees Parlement en de Raad;

(c) voor strafbare feiten zoals gedefinieerd in de artikelen 3 tot en met 12, en artikel 14 van Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad.[49]

5. Het Europees verstrekkingsbevel bevat de volgende informatie:

(a) de uitvaardigende autoriteit en, in voorkomende geval, de bekrachtigende autoriteit;

(b) de in artikel 7 bedoelde adressaat van het Europees verstrekkingsbevel;

(c) de personen om wier gegevens wordt verzocht, behalve wanneer het bevel als enig doel heeft een persoon te identificeren;

(d) de categorie van de gevraagde gegevens (abonneegegevens, toegangsgegevens, transactiegegevens of inhoudelijke gegevens);

(e) in voorkomend geval, de tijdsspanne waarop de te verstrekken gegevens betrekking hebben;

(f) de toepasselijke strafrechtelijke bepalingen van de uitvaardigende staat;

(g) in geval van nood of van een verzoek om eerdere openbaarmaking, de redenen daarvoor;

(h) in gevallen waarin de verlangde gegevens worden opgeslagen of verwerkt als onderdeel van een infrastructuur die door een dienstverlener wordt verstrekt aan een bedrijf of een andere entiteit die geen natuurlijke persoon is, een bevestiging dat het bevel overeenkomstig lid 6 is uitgevaardigd;

(i) de gronden voor de noodzaak en de evenredigheid van de maatregel.

6. In gevallen waarin de verlangde gegevens worden opgeslagen of verwerkt als onderdeel van een infrastructuur die door een dienstverlener wordt verstrekt aan een bedrijf of een andere entiteit die geen natuurlijke persoon is, kan het Europees verstrekkingsbevel uitsluitend worden gericht aan de dienstverlener wanneer onderzoeksmaatregelen tegen het bedrijf of de entiteit niet aangewezen zijn, met name omdat zij het onderzoek zouden kunnen schaden.

7. Indien de uitvaardigende autoriteit redenen heeft om aan te nemen dat de gevraagde transactiegegevens of inhoudelijke gegevens worden beschermd door krachtens het

---

47 Kaderbesluit 2001/413/JBZ van de Raad van 28 mei 2001 betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten (PB L 149 van 2.6.2001, blz. 1).

48 Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PB L 335 van 17.12.2011, blz. 1).

49 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).

recht van de lidstaat waar het bevel aan de dienstverlener wordt geadresseerd, verleende voorrechten en immuniteiten, of dat de openbaarmaking ervan de fundamentele belangen van die lidstaat zou kunnen schaden, onder meer op het gebied van nationale veiligheid en defensie, zoekt de uitvaardigende autoriteit opheldering alvorens het Europees verstrekkingsbevel uit te vaardigen, onder meer door de bevoegde autoriteiten van de betrokken lidstaat te raadplegen, hetzij rechtstreeks hetzij via Eurojust of het Europees justitieel netwerk. Indien de uitvaardigende autoriteit van oordeel is dat de gevraagde toegangsgegevens, transactiegegevens of inhoudelijke gegevens door dergelijke voorrechten en immuniteiten worden beschermd of dat de openbaarmaking ervan de fundamentele belangen van de andere lidstaat zou schaden, vaardigt zij geen Europees verstrekkingsbevel uit.

Artikel 6

Voorwaarden voor het uitvaardigen van een Europees bewaringsbevel

1. Een uitvaardigende autoriteit kan slechts een Europees bewaringsbevel uitvaardigen wanneer alle in dit artikel beschreven voorwaarden zijn vervuld.

2. Het kan worden uitgevaardigd indien zulks noodzakelijk en evenredig is om te voorkomen dat gegevens worden verwijderd, gewist of gewijzigd, met het oog op een aansluitend verzoek tot verstrekking van die gegevens door middel van wederzijdse rechtshulp, een Europees onderzoeksbevel of een Europees verstrekkingsbevel. Europese bevelen tot bewaring van gegevens kunnen voor alle strafbare feiten worden uitgevaardigd.

3. Het Europees bewaringsbevel bevat de volgende informatie:

   (a) de uitvaardigende autoriteit en, indien van toepassing, de bekrachtigende autoriteit;

   (b) de in artikel 7 bedoelde adressaat van het Europees bewaringsbevel;

   (c) de personen wier gegevens moeten worden bewaard, behalve wanneer het bevel als enig doel heeft een persoon te identificeren;

   (d) de categorie van de te bewaren gegevens (abonneegegevens, toegangsgegevens, transactiegegevens of inhoudelijke gegevens);

   (e) in voorkomend geval, de tijdsspanne waarop de te bewaren gegevens betrekking hebben;

   (f) de toepasselijke strafrechtelijke bepalingen van de uitvaardigende staat;

   (g) de gronden voor de noodzaak en de evenredigheid van de maatregel.

Artikel 7

Adressaat van een Europees verstrekkingsbevel en een Europees bewaringsbevel

1. Het Europees verstrekkingsbevel en het Europees bewaringsbevel worden rechtstreeks gericht aan een wettelijke vertegenwoordiger die door de dienstverlener is aangewezen voor bewijsgaring in strafprocedures.

2. Wanneer er geen specifieke wettelijke vertegenwoordiger is aangesteld, kunnen het Europees verstrekkingsbevel en het Europees bewaringsbevel worden gericht aan iedere vestiging van de dienstverlener in de Unie.

3. Wanneer de wettelijke vertegenwoordiger een CEV niet uitvoert in een noodgeval overeenkomstig artikel 9, lid 2, kan het CEV aan iedere vestiging van de dienstverlener in de Unie worden gericht.

4. Wanneer de wettelijke vertegenwoordiger zijn verplichtingen uit hoofde van de artikelen 9 of 10 niet nakomt en de uitvaardigende autoriteit van oordeel is dat er een ernstig risico bestaat dat gegevens verloren zullen gaan, kunnen het Europees verstrekkingsbevel en het Europees bewaringsbevel worden gericht aan iedere vestiging van de dienstverlener in de Unie.

Artikel 8

Certificaat inzake het Europees verstrekkingsbevel en inzake het Europees bewaringsbevel

1. Een Europees verstrekkings- of bewaringsbevel wordt aan de in artikel 7 gedefinieerde adressaat doorgegeven door middel van een certificaat inzake het Europees verstrekkingsbevel (CEV) of een certificaat inzake het Europees bewaringsbevel (CEB).

   De uitvaardigende of bekrachtigende autoriteit vult het in bijlage I opgenomen CEV of het in bijlage II opgenomen CEB in, ondertekent het en verklaart de inhoud ervan nauwkeurig en correct.

2. Het CEV of CEB wordt rechtstreeks doorgegeven op zodanige wijze dat dit schriftelijk kan worden vastgelegd en de adressaat de echtheid ervan kan vaststellen.

   Wanneer dienstverleners, lidstaten of organen van de Unie speciale platforms of andere beveiligde kanalen hebben ingesteld voor het afhandelen van verzoeken om gegevens van gerechtelijke autoriteiten en rechtshandhavingsautoriteiten, kan de uitvaardigende autoriteit er ook voor kiezen het certificaat via deze kanalen door te geven.

3. Het CEV bevat de in artikel 5, lid 5, onder a) tot en met h), vermelde informatie, met inbegrip van informatie die voorde adressaat toereikend is om de uitvaardigende autoriteit te identificeren en daarmee contact op te nemen. De gronden voor de noodzaak en de evenredigheid van de maatregel of nadere bijzonderheden over de onderzoeken worden er niet in opgenomen.

4. Het CEB bevat de in artikel 6, lid 3, onder a) tot en met h), vermelde informatie, met inbegrip van informatie die voor de adressaat toereikend is om de uitvaardigende autoriteit te identificeren en daarmee contact op te nemen. De gronden voor de noodzaak en de evenredigheid van de maatregel of nadere bijzonderheden over de onderzoeken worden er niet in opgenomen.

5. Zo nodig wordt het CEV of CEB vertaald in een officiële taal van de Unie die door de adressaat wordt aanvaard. Als er geen specifieke taal is opgegeven, wordt het CEV of CEB vertaald in een van de officiële talen van de lidstaat waar de wettelijke vertegenwoordiger verblijft of is gevestigd.

Artikel 9

Uitvoering van een CEV

1. Na ontvangst van het CEV zorgt de adressaat ervoor dat de gevraagde gegevens rechtstreeks aan de in het CEV vermelde uitvaardigende autoriteit of rechtshandhavingsautoriteiten worden toegezonden uiterlijk 10 dagen na ontvangst

van het CEV, tenzij de uitvaardigende autoriteit redenen opgeeft voor eerdere openbaarmaking.

2. In noodgevallen geeft de adressaat de gevraagde gegevens onverwijld door, uiterlijk binnen 6 uur na ontvangst van het CEV.

3. Indien de adressaat zijn verplichting niet kan nakomen omdat het CEV onvolledig is, kennelijke fouten bevat of niet voldoende informatie bevat voor de uitvoering van het CEV, informeert de adressaat de in het CEV vermelde uitvaardigende autoriteit onverwijld en verzoekt hij deze om opheldering door gebruik te maken van het formulier in bijlage III. Hij stelt de uitvaardigende autoriteit ervan in kennis of een identificatie en bewaring zoals bedoeld lid 6 mogelijk was. De uitvaardigende autoriteit reageert onverwijld, en uiterlijk binnen 5 dagen. De in de leden 1 en 2 bedoelde termijnen zijn niet van toepassing totdat opheldering is verschaft.

4. Indien de adressaat zijn verplichting niet kan nakomen vanwege overmacht of vanwege een feitelijke onmogelijkheid die niet aan de adressaat of, indien niet dezelfde persoon, de dienstverlener kan worden toegerekend, met name omdat de persoon van wie de gegevens worden verlangd, niet diens klant is, of de gegevens werden gewist voordat het CEV werd ontvangen, stelt de adressaat de in het CEV genoemde uitvaardigende autoriteit daarvan onverwijld in kennis met vermelding van de redenen, door gebruik te maken van het formulier in bijlage III. Als de relevante voorwaarden zijn vervuld, trekt de uitvaardigende autoriteit het CEV in.

5. In alle gevallen waarin de adressaat de gevraagde informatie om andere redenen niet, niet volledig of niet binnen de gestelde termijn verstrekt, stelt hij de uitvaardigende autoriteit onverwijld en uiterlijk binnen de termijnen die zijn vastgelegd in leden 1 en 2 in kennis van die redenen, door gebruik te maken van het formulier in bijlage III. De uitvaardigende autoriteit beoordeelt het bevel in het licht van de door de dienstverlener verstrekte informatie en stelt zo nodig een nieuwe termijn vast waarbinnen de dienstverlener de gegevens dient te verstrekken.

   Indien de adressaat van mening is dat het CEV niet kan worden uitgevoerd omdat op grond van enkel de informatie in het CEV blijkt dat het kennelijk in strijd is met het Handvest van de grondrechten van de Europese Unie of kennelijk misbruik oplevert, zendt de adressaat het formulier in bijlage III ook naar de bevoegde tenuitvoerleggingsautoriteit in de lidstaat van de adressaat. In dergelijke gevallen kan de bevoegde tenuitvoerleggingsautoriteit de uitvaardigende autoriteit om opheldering verzoeken over het Europees verstrekkingsbevel, hetzij rechtstreeks, hetzij via Eurojust of het Europees justitieel netwerk.

6. De adressaat bewaart de gevraagde gegevens indien hij deze niet onmiddellijk verstrekt, tenzij aan de hand van de informatie in het CEV niet kan worden bepaald welke gegevens worden gevraagd, in welk geval hij overeenkomstig lid 3 om opheldering verzoekt. De bewaring wordt gehandhaafd totdat de gegevens worden verstrekt, ongeacht of dit gebeurt op basis van het opgehelderde Europees verstrekkingsbevel en het bijbehorende certificaat dan wel via andere kanalen, zoals wederzijdse rechtshulp. Indien het niet langer noodzakelijk is de gegevens te verstrekken en te bewaren, stelt de uitvaardigende autoriteit, en in voorkomend geval overeenkomstig artikel 14, lid 8, de tenuitvoerleggingsautoriteit, de adressaat daarvan onverwijld in kennis.

Artikel 10
Uitvoering van een CEB

1. Na ontvangst van het CEB bewaart de adressaat onverwijld de gevraagde gegevens. De bewaring wordt beëindigd na 60 dagen, tenzij de uitvaardigende autoriteit bevestigt dat een begin is gemaakt met het aansluitende verstrekkingsverzoek.

2. Indien de uitvaardigende autoriteit binnen de in lid 1 vastgestelde termijn bevestigt dat een begin is gemaakt met het aansluitende verstrekkingsverzoek, bewaart de adressaat de gegevens zolang als nodig is om de gegevens te verstrekken zodra van het aansluitende verzoek kennis is gegeven of dat verzoek is betekend.

3. Indien de bewaring niet langer noodzakelijk is, stelt de uitvaardigende autoriteit de adressaat daarvan onverwijld in kennis.

4. Indien de adressaat zijn verplichting niet kan nakomen omdat het certificaat onvolledig is, kennelijke fouten bevat of niet voldoende informatie bevat voor de uitvoering van het CEB, informeert de adressaat de in het CEB vermelde uitvaardigende autoriteit onverwijld en verzoekt hij deze om opheldering door gebruik te maken van het formulier in bijlage III. De uitvaardigende autoriteit reageert onverwijld, en uiterlijk binnen 5 dagen. De adressaat zorgt ervoor dat zijnerzijds de noodzakelijke opheldering kan worden ontvangen, zodat kan worden voldaan aan zijn in lid 1 genoemde verplichting.

5. Indien de adressaat zijn verplichting niet kan nakomen vanwege overmacht of vanwege een feitelijke onmogelijkheid die niet aan de adressaat of, indien niet dezelfde persoon, de dienstverlener kan worden toegerekend, met name omdat de persoon van wie de gegevens worden verlangd, niet diens klant is, of de gegevens werden gewist voordat het bevel werd ontvangen, neemt hij onverwijld contact op met de in het CEB genoemde uitvaardigende autoriteit met vermelding van de redenen, door gebruik te maken van het formulier in bijlage III. Als deze voorwaarden zijn vervuld, trekt de uitvaardigende autoriteit het CEB in.

6. In alle gevallen waarin de adressaat de gevraagde informatie om andere, in het formulier in bijlage III opgesomde redenen niet bewaart, stelt hij de uitvaardigende autoriteit onverwijld in kennis van die redenen, door gebruik te maken van het formulier in bijlage III. De uitvaardigende autoriteit beoordeelt het bevel in het licht van de door de dienstverlener gegeven rechtvaardiging.

Artikel 11
Vertrouwelijkheid en gebruikersinformatie

1. Adressaten en, indien niet dezelfde personen, dienstverleners, nemen de nodige maatregelen om de vertrouwelijkheid van het CEV of CEB en van de verstrekte of bewaarde gegevens te garanderen en zien ervan af, wanneer de uitvaardigende autoriteit daarom verzoekt, de persoon wiens gegevens worden verlangd, daarover te informeren teneinde het betrokken strafonderzoek niet te belemmeren.

2. Indien de uitvaardigende autoriteit de adressaat heeft verzocht de persoon wiens gegevens worden verlangd, daarover niet te informeren, stelt de uitvaardigende autoriteit de persoon wiens gegevens via het CEV worden verlangd, onverwijld in kennis van de verstrekking. Deze informatie kan worden opgeschort zolang als noodzakelijk en evenredig is om de betrokken strafprocedure niet te belemmeren.

3. Wanneer de uitvaardigende autoriteit de betrokkene in kennis stelt, verstrekt zij ook informatie over alle beschikbare rechtsmiddelen als bedoeld in artikel 17.

Artikel 12
Vergoeding van kosten

De dienstverlener kan aanspraak maken op vergoeding van zijn kosten door de uitvaardigende staat, indien het nationale recht van de uitvaardigende staat daarin voorziet voor binnenlandse bevelen in soortgelijke omstandigheden, in overeenstemming met deze nationale bepalingen.

Hoofdstuk 3: Sancties en tenuitvoerlegging

Artikel 13
Sancties

Zonder afbreuk te doen aan nationale rechtsregels die voorzien in het opleggen van strafrechtelijke sancties, stellen de lidstaten de regels vast inzake geldelijke sancties die van toepassing zijn op inbreuken op de verplichtingen uit hoofde van de artikelen 9, 10 en 11 van deze verordening en nemen zij alle nodige maatregelen om ervoor te zorgen dat deze worden uitgevoerd. De vastgestelde sancties zijn doeltreffend, evenredig en afschrikkend. De lidstaten stellen de Commissie onverwijld van deze regels en deze maatregelen in kennis en doen dit eveneens bij alle eventuele latere wijzigingen ervan.

Artikel 14
Procedure voor tenuitvoerlegging

1. Indien de adressaat een CEV niet binnen de termijn naleeft of een CEB niet naleeft, zonder redenen op te geven die door de uitvaardigende autoriteit worden aanvaard, kan de uitvaardigende autoriteit het Europees verstrekkingsbevel met het CEV of het Europees bewaringsbevel met het CEB, alsook het door de adressaat ingevulde formulier van bijlage III en alle andere relevante documenten met het oog op de tenuitvoerlegging ervan doorgeven aan de bevoegde autoriteit in de tenuitvoerleggingsstaat, op zodanige wijze dat dit schriftelijk kan worden vastgelegd en de tenuitvoerleggingsstaat de echtheid ervan kan vaststellen. Daartoe vertaalt de uitvaardigende autoriteit het bevel, het formulier en alle andere begeleidende documenten in een van de officiële talen van deze lidstaat en stelt zij de adressaat in kennis van de overdracht.

2. Na ontvangst erkent de tenuitvoerleggingsautoriteit zonder verdere formaliteiten een overeenkomstig lid 1 doorgegeven Europees verstrekkings- of bewaringsbevel en neemt zij de nodige maatregelen voor de tenuitvoerlegging ervan, tenzij de tenuitvoerleggingsautoriteit van oordeel is dat een van de in de leden 4 of 5 opgenomen gronden van toepassing is, dat de betrokken gegevens worden beschermd door een immuniteit of voorrecht krachtens het nationaal recht, of dat de openbaarmaking ervan de fundamentele belangen van de staat, zoals nationale veiligheid en defensie, zou kunnen aantasten. De tenuitvoerleggingsautoriteit neemt onverwijld en uiterlijk vijf werkdagen na ontvangst van het bevel, de beslissing tot erkenning van het bevel.

3. Indien de tenuitvoerleggingsautoriteit het bevel erkent, verplicht zij de adressaat formeel de betrokken verplichting na te komen en informeert zij de adressaat over de mogelijkheid bezwaar te maken tegen de tenuitvoerlegging op basis van een van de in de leden 4 en 5 vermelde gronden en over de toepasselijke sancties in geval van niet-naleving, en stelt zij een termijn vast voor de naleving van het bevel of het maken van bezwaar.

4. De adressaat kan alleen op de volgende gronden bezwaar maken tegen de tenuitvoerlegging van het Europees verstrekkingsbevel:

   (a) het Europees verstrekkingsbevel is niet uitgevaardigd of bekrachtigd door een uitvaardigende autoriteit als bedoeld in artikel 4;

   (b) het Europees verstrekkingsbevel is niet uitgevaardigd voor een strafbaar feit als bedoeld in artikel 5, lid 4;

   (c) de adressaat kon het CEV niet naleven wegens een feitelijke onmogelijkheid of overmacht, of omdat het CEV kennelijke fouten bevat;

   (d) het Europees verstrekkingsbevel heeft geen betrekking op gegevens die door of namens de dienstverlener zijn opgeslagen op het tijdstip van ontvangst van het CEV;

   (e) de dienst valt niet onder deze verordening;

   (f) op basis van enkel de informatie in het CEV blijkt dat het kennelijk in strijd is met het Handvest of kennelijk misbruik oplevert.

5. De adressaat kan alleen op de volgende gronden bezwaar maken tegen de tenuitvoerlegging van het Europees bewaringsbevel:

   (a) het Europees bewaringsbevel is niet uitgevaardigd of bekrachtigd door een uitvaardigende autoriteit als bedoeld in artikel 4;

   (b) de dienstverlener kon het CEB niet naleven wegens een feitelijke onmogelijkheid of overmacht, of omdat het CEB kennelijke fouten bevat;

   (c) het Europees bewaringsbevel heeft geen betrekking op gegevens die door of namens de dienstverlener zijn opgeslagen ten tijde van de uitvaardiging van het CEB;

   (d) de dienst valt niet onder het toepassingsgebied van deze verordening;

   (e) op basis van enkel de informatie in het CEB blijkt dat het CEB kennelijk in strijd is met het Handvest of kennelijk misbruik oplevert.

6. In het geval van een bezwaar van de adressaat beslist de tenuitvoerleggingsautoriteit of het bevel ten uitvoer wordt gelegd op basis van de informatie die is verstrekt door de adressaat en, zo nodig, aanvullende informatie die overeenkomstig lid 7 is verkregen van de uitvaardigende autoriteit.

7. Alvorens te beslissen het bevel niet te erkennen of ten uitvoer te leggen overeenkomstig de leden 2 en 6, raadpleegt de tenuitvoerleggingsautoriteit de uitvaardigende autoriteit op eender welke passende wijze. Zo nodig verzoekt zij de uitvaardigende autoriteit om nadere informatie. De uitvaardigende autoriteit beantwoordt een dergelijk verzoek binnen vijf werkdagen.

8. De uitvaardigende autoriteit en de adressaat worden onmiddellijk in kennis gesteld van alle beslissingen, op zodanige wijze dat het schriftelijk kan worden vastgelegd.

9. Indien de tenuitvoerleggingsautoriteit de gegevens van de adressaat verkrijgt, geeft zij deze binnen twee werkdagen door aan de uitvaardigende autoriteit, tenzij de betrokken gegevens worden beschermd door een immuniteit of voorrecht krachtens haar eigen nationale recht of zij fundamentele belangen van haar staat, zoals nationale veiligheid en defensie, kunnen aantasten. In dat geval stelt zij de uitvaardigende autoriteit in kennis van de redenen waarom de gegevens niet worden doorgegeven.

10. Indien de adressaat niet voldoet aan zijn verplichtingen in het kader van een erkend bevel waarvan de uitvoerbaarheid door de tenuitvoerleggingsautoriteit werd bevestigd, legt die autoriteit een geldboete op overeenkomstig haar nationaal recht. Tegen de beslissing tot oplegging van een geldboete is een doeltreffende voorziening in rechte beschikbaar.

Hoofdstuk 4: Rechtsmiddelen

Artikel 15
Toetsingsprocedure in geval van tegenstrijdige verplichtingen op grond van grondrechten of fundamentele belangen van een derde land

1. Indien de adressaat van mening is dat de naleving van het Europees verstrekkingsbevel in strijd zou zijn met de toepasselijke wetgeving van een derde land die openbaarmaking van de betrokken gegevens verbiedt omdat de bescherming van de grondrechten van de betrokken personen of de fundamentele belangen van het derde land in verband met de nationale veiligheid of defensie, daartoe nopen, stelt hij de uitvaardigende autoriteit in kennis van de redenen waarom het Europees verstrekkingsbevel niet wordt uitgevoerd overeenkomstig de in artikel 9, lid 5, bedoelde procedure.

2. Het gemotiveerde bezwaar bevat alle relevante informatie over het recht van het derde land, over de toepasselijkheid ervan op de betrokken zaak en over de aard van de tegenstrijdige verplichting. Het bezwaar kan niet worden gebaseerd op het feit dat er in het toepasselijke recht van het derde land geen vergelijkbare bepalingen bestaan betreffende de voorwaarden, formaliteiten en procedures voor het uitvaardigen van een verstrekkingsbevel, noch op de enkele omstandigheid dat de gegevens in een derde land zijn opgeslagen.

3. De uitvaardigende autoriteit toetst het Europees verstrekkingsbevel aan de hand van het gemotiveerde bezwaar. Indien de uitvaardigende autoriteit voornemens is het Europees verstrekkingsbevel in stand te houden, verzoekt zij de bevoegde rechtbank in haar lidstaat om een toetsing. De uitvoering van het bevel wordt opgeschort in afwachting van de voltooiing van de toetsingsprocedure.

   De bevoegde rechtbank gaat eerst na of er sprake is van een conflict, op basis van een onderzoek van de vraag of

   (a) het recht van het derde land van toepassing is op basis van de specifieke omstandigheden van de betrokken zaak, en zo ja,

   (b) het recht van het derde land, wanneer het op de specifieke omstandigheden van de betrokken zaak wordt toegepast, openbaarmaking van de betrokken gegevens verbiedt.

4. Bij deze beoordeling moet de rechtbank in aanmerking nemen of het recht van het derde land niet zozeer de grondrechten of fundamentele belangen van het derde land op het gebied van nationale veiligheid of verdediging beoogt te beschermen, als wel er kennelijk op is gericht andere belangen te beschermen of illegale activiteiten af te schermen tegen verzoeken om rechtshandhaving in het kader van strafrechtelijk onderzoek.

5. Indien de bevoegde rechtbank vaststelt dat er geen sprake is van een relevant conflict in de zin van de leden 1 en 4, houdt zij het bevel in stand. Indien de bevoegde rechtbank vaststelt dat er sprake is van een relevant conflict in de zin van de leden 1 en 4, zendt zij alle relevante feitelijke en juridische informatie over de zaak, met inbegrip van haar beoordeling, via haar nationale centrale autoriteit naar de centrale autoriteiten in het betrokken derde land, met een termijn van 15 dagen om te reageren. Op gemotiveerd verzoek van de centrale autoriteit van het derde land kan deze termijn met 30 dagen worden verlengd.

6. Indien de centrale autoriteit van het derde land de bevoegde rechtbank binnen de termijn meedeelt dat zij bezwaar maakt tegen de uitvoering van het Europees verstrekkingsbevel in de betrokken zaak, trekt de bevoegde rechtbank het bevel in en stelt zij de uitvaardigende autoriteit en de adressaat daarvan in kennis. Indien binnen de (verlengde) termijn geen bezwaar is ontvangen, zendt de bevoegde rechtbank een herinnering waarin de centrale autoriteit van het derde land 5 dagen extra krijgt om te reageren en waarin zij deze in kennis stelt van de gevolgen van het uitblijven van een reactie. Indien binnen deze extra termijn geen bezwaar is ontvangen, houdt de bevoegde rechtbank het bevel in stand.

7. Indien de bevoegde rechtbank oordeelt dat het bevel in stand moet worden gehouden, stelt zij de uitvaardigende autoriteit en de adressaat daarvan in kennis, waarna laatstgenoemde tot de uitvoering van het bevel overgaat.

Artikel 16

Toetsingsprocedure in geval van tegenstrijdige verplichtingen op andere gronden

1. Indien de adressaat van mening is dat de naleving van het Europees verstrekkingsbevel in strijd zou zijn met de toepasselijke wetgeving van een derde land die openbaarmaking van de betrokken gegevens verbiedt op andere dan de in artikel 15 genoemde gronden, stelt hij de uitvaardigende autoriteit in kennis van de redenen waarom het Europees verstrekkingsbevel niet wordt uitgevoerd overeenkomstig de in artikel 9, lid 5, bedoelde procedure.

2. Het gemotiveerde bezwaar bevat alle relevante informatie over het recht van het derde land, over de toepasselijkheid ervan op de betrokken zaak en over de aard van de tegenstrijdige verplichting. Het bezwaar kan niet worden gebaseerd op het feit dat er in het toepasselijke recht van het derde land geen vergelijkbare bepalingen bestaan betreffende de voorwaarden, formaliteiten en procedures voor het uitvaardigen van een verstrekkingsbevel, noch op de enkele omstandigheid dat de gegevens in een derde land zijn opgeslagen.

3. De uitvaardigende autoriteit toetst het Europees verstrekkingsbevel aan de hand van het gemotiveerde bezwaar. Indien de uitvaardigende autoriteit voornemens is het Europees verstrekkingsbevel in stand te houden, verzoekt zij de bevoegde rechtbank

in haar lidstaat om een toetsing. De uitvoering van het bevel wordt opgeschort in afwachting van de voltooiing van de toetsingsprocedure.

4. De bevoegde rechtbank gaat eerst na of er sprake is van een conflict, op basis van een onderzoek van de vraag of

   (a) het recht van het derde land van toepassing is op basis van de specifieke omstandigheden van de betrokken zaak, en zo ja,

   (b) het recht van het derde land, wanneer het op de specifieke omstandigheden van de betrokken zaak wordt toegepast, openbaarmaking van de betrokken gegevens verbiedt,

5. Wanneer de bevoegde rechtbank vaststelt dat er geen sprake is van een relevant conflict in de zin van de leden 1 en 4, houdt zij het bevel in stand. Indien de bevoegde rechtbank vaststelt dat het recht van het derde land, wanneer het op de specifieke omstandigheden van de onderzochte zaak wordt toegepast, openbaarmaking van de betrokken gegevens verbiedt, bepaalt de bevoegde rechtbank of het bevel in stand wordt gehouden of wordt ingetrokken, met name op basis van de volgende factoren:

   (a) het belang dat wordt beschermd door het relevante recht van het derde land, met inbegrip van het belang van het derde land bij niet-openbaarmaking van de gegevens;

   (b) de mate van verbondenheid van de strafzaak waarvoor het bevel werd uitgevaardigd met één van beide rechtsgebieden, zoals onder meer blijkt uit:

   de locatie, de nationaliteit en de woonplaats van de persoon wiens gegevens worden verlangd en/of van het/de slachtoffer(s),

   de plaats waar het betrokken strafbaar feit werd gepleegd;

   (c) de mate van verbondenheid tussen de dienstverlener en het betrokken derde land; in dit verband volstaat de locatie waar de gegevens zijn opgeslagen, op zichzelf niet om een wezenlijke mate van verbondenheid aan te tonen;

   (d) de belangen van de staat waar het onderzoek wordt gevoerd bij het verkrijgen van het betrokken bewijsmateriaal, op basis van de ernst van het strafbare feit en het belang van een spoedige bewijsverkrijging;

   (e) de mogelijke gevolgen voor de adressaat of de dienstverlener van het naleven van het Europees verstrekkingsbevel, met inbegrip van de sancties die kunnen worden opgelegd.

6. Indien de bevoegde rechtbank beslist het bevel in te trekken, stelt zij de uitvaardigende autoriteit en de adressaat daarvan in kennis. . Indien de bevoegde rechtbank oordeelt dat het bevel in stand moet worden gehouden, stelt zij de uitvaardigende autoriteit en de adressaat daarvan in kennis, waarna laatstgenoemde tot de uitvoering overgaat.

Artikel 17
Doeltreffende rechtsmiddelen

1. Verdachten en beklaagden wier gegevens werden verkregen via een Europees verstrekkingsbevel hebben recht op doeltreffende rechtsmiddelen tegen het Europees

verstrekkingsbevel tijdens de strafprocedure waarvoor het bevel werd uitgevaardigd, onverminderd de rechtsmiddelen die krachtens Richtlijn (EU) 2016/680 en Verordening (EU) 2016/679 beschikbaar zijn.

2. Indien de persoon van wie de gegevens werden verkregen, geen verdachte of beklaagde is in een strafprocedure waarvoor het bevel werd uitgevaardigd, heeft deze persoon recht op doeltreffende rechtsmiddelen tegen een Europees verstrekkingsbevel in de uitvaardigende staat, onverminderd de rechtsmiddelen die krachtens Richtlijn (EU) 2016/680 en Verordening (EU) 2016/679 beschikbaar zijn.

3. Dit recht op een doeltreffende voorziening in rechte wordt uitgeoefend voor een rechtbank in de uitvaardigende staat overeenkomstig het nationale recht van die staat en omvat de mogelijkheid om de rechtmatigheid van de maatregel aan te vechten, met inbegrip van de noodzaak en de evenredigheid daarvan.

4. Onverminderd het bepaalde in artikel 11 neemt de uitvaardigende autoriteit passende maatregelen om ervoor te zorgen dat informatie wordt verstrekt over de mogelijkheden uit hoofde van het nationale recht om rechtsmiddelen in te stellen en ervoor te zorgen dat deze doeltreffend kunnen worden ingezet.

5. Dezelfde termijnen of andere voorwaarden als gelden voor het instellen van een rechtsmiddel in soortgelijke nationale zaken zijn hier van toepassing en wel zodanig dat de doeltreffende uitoefening van die rechtsmiddelen voor de betrokken personen is gewaarborgd.

6. Onverminderd de nationale procedurele voorschriften zorgen de lidstaten ervoor dat, bij het beoordelen van het door middel van het Europees verstrekkingsbevel verkregen bewijsmateriaal, de rechten van de verdediging en het eerlijke verloop van de procedures tijdens een strafprocedure in de uitvaardigende staat worden geëerbiedigd.

Artikel 18
Het waarborgen van voorrechten en immuniteiten krachtens het recht van de tenuitvoerleggingsstaat

Indien door het Europees verstrekkingsbevel verkregen transactiegegevens of inhoudelijke gegevens worden beschermd door immuniteiten en voorrechten krachtens het recht van de lidstaat van de adressaat, of indien deze gegevens de fundamentele belangen van die lidstaat aantasten, zoals nationale veiligheid en defensie, zorgt de rechtbank in de uitvaardigingsstaat ervoor dat tijdens de strafprocedure waarvoor het bevel werd uitgevaardigd, bij de beoordeling van de relevantie en de ontvankelijkheid van het betrokken bewijsmateriaal met deze gronden rekening wordt gehouden alsof zij krachtens het nationale recht zouden gelden. De rechter kan de autoriteiten van de betrokken lidstaat, het Europees justitieel netwerk in strafzaken of Eurojust raadplegen.

Hoofdstuk 5: Slotbepalingen

Artikel 19
Monitoring en rapportage

1. Uiterlijk *[datum waarop deze verordening van toepassing wordt]* stelt de Commissie een gedetailleerd programma op voor de monitoring van de outputs, resultaten en effecten van deze verordening. In het monitoringprogramma wordt vermeld met

welke middelen en op welke tijdstippen gegevens en ander noodzakelijke bewijsstukken zullen worden verzameld. In het programma wordt tevens aangegeven welke actie de Commissie en de lidstaten moeten ondernemen om de gegevens en andere bewijsstukken te verzamelen en te analyseren.

2. In ieder geval stellen de lidstaten uitgebreide statistieken op van bij de bevoegde instanties verzamelde gegevens, die zij actualiseren.. Elk jaar worden de verzamelde gegevens over het voorgaande kalenderjaar uiterlijk op 31 maart aan de Commissie toegezonden en deze omvatten:

   (a) het aantal uitgevaardigde CEV's en CEB's per categorie gevraagde gegevens, soort dienstverleners aan wie een bevel is geadresseerd en soort situatie (noodgeval of niet);

   (b) het aantal uitgevoerde en niet-uitgevoerde CEV's per categorie gevraagde gegevens, soort dienstverleners aan wie een bevel is geadresseerd en soort situatie (noodgeval of niet);

   (c) voor uitgevoerde CEV's, de gemiddelde duur voor het verkrijgen van de gevraagde gegevens vanaf het moment van uitvaardiging van het CEV, per categorie gevraagde gegevens, soort dienstverleners aan wie een bevel is geadresseerd en soort situatie (noodgeval of niet);

   (d) het aantal voor tenuitvoerlegging aan een tenuitvoerleggingslidstaat doorgegeven en ontvangen Europese verstrekkingsbevelen, per categorie gevraagde gegevens, soort dienstverleners aan wie een bevel is geadresseerd en soort situatie (noodgeval of niet) en het aantal van die bevelen dat is uitgevoerd;

   (e) het aantal rechtsmiddelen dat is ingesteld tegen Europese verstrekkingsbevelen in de uitvaardigende staat en in de tenuitvoerleggingsstaat per categorie gevraagde gegevens.

Artikel 20
Wijzigingen van de certificaten en de formulieren

De Commissie stelt overeenkomstig artikel 21 gedelegeerde handelingen vast tot wijziging van de bijlagen I, II en III teneinde doeltreffend te voorzien in een eventuele behoefte aan verbetering van de inhoud van de formulieren voor het CEV en het CEB en van de formulieren die moeten worden gebruikt om informatie te verstrekken over de onmogelijkheid om het CEV of CEB uit te voeren.

Artikel 21
Uitoefening van 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 20 bedoelde delegatie van bevoegdheden wordt met ingang van *[de datum waarop deze verordening van toepassing wordt]* toegekend voor onbepaalde tijd.

3. Het Europees Parlement of de Raad kan de in artikel 20 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[50].

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

6. Een overeenkomstig artikel 20 vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 22
Kennisgevingen

1. Uiterlijk op *[datum waarop deze verordening van toepassing wordt]* verstrekt elke lidstaat de Commissie de volgende gegevens:

   (a) de autoriteiten die, overeenkomstig hun nationale recht, krachtens artikel 4 bevoegd zijn om een Europees verstrekkingsbevel en een Europees bewaringsbevel uit te vaardigen en/of te bekrachtigen;

   (b) de tenuitvoerleggingsautoriteit of -autoriteiten die bevoegd zijn om Europese verstrekkingsbevelen en Europese bewaringsbevelen namens een andere lidstaat ten uitvoer te leggen;

   (c) de rechtbanken die bevoegd zijn om gemotiveerde bezwaren van adressaten te behandelen overeenkomstig de artikelen 15 en 16.

2. De Commissie maakt de op grond van dit artikel ontvangen informatie publiek beschikbaar, hetzij op een speciale website, hetzij op de website van het Europees justitieel netwerk als bedoeld in artikel 9 van Besluit 2008/976/JHA van de Raad[51].

Artikel 23
Relatie met Europese onderzoeksbevelen

De autoriteiten van de lidstaten kunnen doorgaan met het uitvaardigen van Europese onderzoeksbevelen overeenkomstig Richtlijn 2014/41/EU voor de bewijsgaring die ook binnen het toepassingsgebied van deze verordening zou vallen.

[50] PB L 123 van 12.5.2016, blz. 13.

[51] Besluit 2008/976/JBZ van de Raad van 16 december 2008 betreffende het Europees justitieel netwerk (PB L 348 van 24.12.2008, blz. 130).

Artikel 24
Evaluatie

Uiterlijk *[vijf jaar na de datum waarop deze verordening van toepassing wordt]*, voert de Commissie een evaluatie uit van deze verordening en dient zij een verslag in bij het Europees Parlement en de Raad over de werking van deze verordening, met inbegrip van een beoordeling van de noodzaak om het toepassingsgebied ervan uit te breiden. Indien nodig worden bij het verslag wetgevingsvoorstellen gevoegd. De evaluatie wordt verricht aan de hand van de richtsnoeren voor betere regelgeving van de Commissie. De lidstaten verstrekken de Commissie de informatie die nodig is voor de opstelling van dit verslag.

Artikel 25
Inwerkingtreding

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

Zij is van toepassing met ingang van *[6 maanden na de inwerkingtreding]*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in de lidstaten overeenkomstig de Verdragen.

Gedaan te Straatsburg,

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