Fiche 1: Verordening Europese Verstrekkings- en Bewaringsbevelen voor e-evidence

1. Algemene gegevens

a) Titel voorstel
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

b) Datum ontvangst Commissiedocument
18 april 2018

c) Nr. Commissiedocument
COM (2018) 225

d) EUR-Lex
http://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing
SWD (2018) 118, SWD (2018) 119

f) Behandelingstraject Raad
Raad Justitie en Binnenlandse Zaken

g) Eerstverantwoordelijk ministerie
Ministerie van Justitie en Veiligheid

h) Rechtsbasis
Artikel 82, eerste lid, van het Verdrag betreffende de werking van de Europese Unie (VWEU)

i) Besluitvormingsprocedure Raad
Gekwalificeerde meerderheid

j) Rol Europees Parlement
Medebeslissingsprocedure

2. Essentie voorstel

a) Inhoud voorstel
Op 17 april 2018 is door de Europese Commissie, samen met de publicatie van het 14e voortgangsverslag naar een effectieve Veiligheidsunie, een reeks nieuwe veiligheidsvoorstellen ingediend om resterende lacunes in de veiligheidswetgeving verder te dichten. Hiermee wordt

beoogd om de ruimte waarin terroristen en criminelen opereren verder in te perken door hen de middelen te ontzeggen die nodig zijn om criminaliteit te plannen, te financieren en uit te voeren.
De Commissie betoogt het volgende. Criminaliteit in de Europese Unie kan momenteel niet effectief worden opgespoord en vervolgd vanwege problemen met grensoverschrijdende toegang tot elektronisch bewijs. De samenwerking tussen justitiële autoriteiten van lidstaten, de samenwerking tussen deze autoriteiten en dienstaanbieders en de toegang door justitiële autoriteiten ten aanzien van elektronisch bewijs functioneert niet op een voldoende doeltreffende manier. Als gevolg daarvan moeten strafrechtelijke onderzoeken worden gestopt of komen deze niet van de grond, wordt criminaliteit niet bestraft, worden slachtoffers niet beschermd en voelen EU-burgers zich minder veilig. De voorgestelde juridische maatregelen beogen de mogelijkheden voor grensoverschrijdende toegang tot data binnen strafrechtelijke procedures te vergroten en daarbij de bestaande problemen terug te dringen. Hierbij wordt rekening gehouden met de beginselen van rechtszekerheid, transparantie, toerekenbaarheid en de bescherming van fundamentele rechten.

De probleemdefinitie is overgenomen uit de gemeenschappelijke Mededeling Europese Veiligheidsagenda van 28 april 2015[1] De voorstellen voor een verordening en voor een richtlijn[2]omvatten Europese regels voor het grensoverschrijdend vorderen van gegevens rechtstreeks bij dienstaanbieders ('service providers').

Het voorstel voorziet in de mogelijkheden voor justitiële autoriteiten om een vordering tot verstrekking (European Production Order/Europees Verstrekkingsbevel) of bewaring (European Preservation Order/Europees Bewaringsbevel) van elektronisch bewijsmateriaal, te richten tot dienstaanbieders die hun diensten aanbieden in de Europese Unie, zonder tussenkomst van de justitiële autoriteiten van de lidstaat waar de dienstaanbieder is gevestigd of waar de gegevens zich bevinden. Het voorstel maakt daarbij een onderscheid tussen verschillende soorten gegevens (gebruikersgegevens, toegangsgegevens, verkeersgegevens en gegevens betreffende de inhoud). De gevorderde data kan dus variëren van identificerende gegevens, IP-adressen, meta-data tot sms-berichten, e-mails, foto's of app-berichten. Afhankelijk van de impact op de persoonlijke levenssfeer worden aparte waarborgen voorgesteld.

Europees verstrekkingsbevel
Het voorstel beperkt zich tot opgeslagen data. Voor verkeersgegevens en gegevens betreffende de inhoud gelden zwaardere drempels voordat een Europees verstrekkingsbevel uitgevaardigd kan worden dan voor gebruikers- en toegangsgegevens. Een Europees verstrekkingsbevel kan voor verkeersgegevens en gegevens betreffende de inhoud alleen worden uitgevaardigd door een rechter (in het Nederlandse geval een Rechter-Commissaris) in

[1] BNC-fiche bij kamerbrief van 5 juni 2015, TK-vergaderjaar 2014-2015, 22112, nr. 1972) en de latere aanscherping daarvan in de Raadsconclusies JBZ van 9 juni 2016.

[2] De richtlijn inzake de benoeming van juridische vertegenwoordigers voor het doel van het verzamelen van bewijs in strafprocedures, wordt behandeld in een afzonderlijk BNC-fiche.

gevallen waarin sprake is van misdrijven waarop een gevangenisstraf van drie jaar of meer is gesteld of een misdrijf dat is opgesomd in de conceptverordening (computermisdrijven, terroristische misdrijven en misdrijven met (online) betaalmiddelen), voor zover de nationale wetgeving dat toelaat. In andere gevallen zal een rechtshulpverzoek moeten worden gedaan. Bij gebruikers- en toegangsgegevens kan een Europees verstrekkingsbevel door de officier van justitie worden uitgevaardigd voor alle strafbare feiten. Een verdere toelichting van de type data wordt gegeven in hoofdstuk 3 paragraaf a.
De dienstaanbieder moet binnen tien dagen na het bevel reageren. In geval van nood moet deze binnen zes uur reageren. Dit is aanzienlijk sneller dan bij het bestaande Europees onderzoeksbevel (120 dagen) en bij de procedure voor wederzijdse rechtshulp (tien maanden).

Europees Bewaringsbevel
Een Europees Bewaringsbevel kan vooruitlopend op een Europees verstrekkingsbevel of op een rechtshulpverzoek worden uitgevaardigd, om zo te voorkomen dat de gegevens worden gewist voordat aan het Europees verstrekkingsbevel is voldaan of op het rechtshulpverzoek is beslist. Een justitiële autoriteit in een lidstaat kan met dit bevel een dienstaanbieder die in een andere lidstaat is gevestigd, of daar een juridisch vertegenwoordiger heeft, ertoe verplichten om specifieke gegevens te bewaren. Een voorwaarde is dat deze aanbieder diensten in de Unie aanbiedt. Vervolgens kan de justitiële autoriteit de bewaarde gegevens opvragen via een rechtshulpverzoek, een Europees onderzoeksbevel of een Europees verstrekkingsbevel.

Verzet en naleving
De dienstaanbieder kan op een beperkt aantal formele gronden, opgesomd in het voorstel voor een verordening, zich verzetten tegen de tenuitvoerlegging van een Europees verstrekkingsbevel of Europees bewaringsbevel. Het gaat dan bijvoorbeeld om het geval waarin de dienstaanbieder niet over de gevraagde gegevens beschikt of een bevel niet door de juiste autoriteit is uitgevaardigd. Ook wanneer een bevel manifest in strijd is met het EU-Handvest voor fundamentele rechten of wanneer overduidelijk sprake is van misbruik kan de dienstaanbieder zich verzetten tegen het bevel. Naleving van het bevel kan alleen worden afgedwongen door de lidstaat waar de dienstaanbieder of zijn juridische vertegenwoordiger (legal representative) is gevestigd. Deze bedrijven moeten vertegenwoordigers aanwijzen met het oog op de inontvangstneming, naleving en handhaving van besluiten en bevelen die zijn uitgevaardigd door de bevoegde autoriteiten van de lidstaten met als doel het verzamelen van bewijsmateriaal in strafzaken. De uitvaardigende lidstaat moet zich tot die lidstaat wenden als de dienstaanbieder het bevel niet naleeft. Die lidstaat (van vestiging) kan - als er geen gronden zijn om de naleving van het bevel te weigeren - een boete uitvaardigen als de dienstaanbieder niet aan het bevel voldoet.

Waarborgen en rechtsbescherming
De voorstellen bevatten verscheidene waarborgen. Beide bevelen kunnen alleen worden uitgevaardigd in het kader van een strafrechtelijke procedure en alle waarborgen van het

strafprocesrecht van de uitvaardigende lidstaat zijn van toepassing. De voorgestelde regelingen beogen gedegen waarborgen en bescherming van grondrechten te bieden, onder meer via de rol van justitiële autoriteiten en de extra vereisten die gelden voor het verkrijgen van gegevens die tot bepaalde categorieën behoren. Er zijn ook waarborgen voor het recht op bescherming van persoonsgegevens. De dienstaanbieders en de personen wier gegevens het betreft kunnen een beroep doen op juridische voorzieningen. Zo kan de dienstaanbieder een gemotiveerd bezwaar maken tegen een verstrekkingsbevel als het bevel volgens deze provider in strijd komt met toepasselijke wetgeving van een derde land die verstrekking van de data verbiedt, omdat dit nodig is om of de grondrechten van de betrokken personen of de fundamentele belangen van het derde land in verband met de nationale veiligheid of verdediging te beschermen. De uitvaardigende autoriteit moet dan dit gemotiveerde bezwaar afwegen. Als deze autoriteit het bevel toch wil geven, dan moet zij dit laten toetsen door de bevoegde rechter in de eigen lidstaat. Ook voor het geval er andere conflicterende verplichtingen zijn is voorzien in een bezwaarprocedure die de dienstaanbieder kan toepassen.

Personen en verdachten van wie de gegevens zijn verkregen via een Europees verstrekkingsbevel hebben het recht op een effectieve rechtsgang tegen dit bevel gedurende het strafproces in het kader waarvan het bevel werd gegeven. De rechtsbescherming op grond van de instrumenten voor gegevensbescherming, te weten Richtlijn (EU) 2016/680 en de Verordening (EU) 2016/679, blijft onverlet. Als een persoon over wie de gegevens werden verkregen geen verdachte of beschuldigde is in het strafproces, in het kader waarvan het bevel was gegeven, dan heeft deze persoon het recht op een effectieve rechtsgang tegen een verstrekkingsbevel in de staat die dit bevel heeft uitgevaardigd. Een dergelijk recht op een effectieve rechtsgang wordt uitgeoefend voor een rechter in de uitvaardigende staat overeenkomstig het nationale recht van die staat en zal de mogelijkheid omvatten om de rechtmatigheid van de maatregel aan te vechten, waaronder de noodzaak en proportionaliteit.

b) Impact assessment Commissie

In het impact assessment is een uitgebreide probleemanalyse uitgevoerd.
Na afweging van belangen tussen vier verschillende opties (A-D) concludeert de Commissie in het impact assessment dat de doelstellingen zoals beschreven onder 2a het best bereikt kunnen worden met:

1. Praktische verbeteringen in de grensoverschrijdende samenwerking van politie- en justitiediensten, alsook in samenwerking met private partijen;
2. Internationale afspraken en regels voor het grensoverschrijdend vorderen van gegevens rechtstreeks bij private dienstaanbieders en
3. Regels voor rechtstreekse toegang tot elektronisch bewijs door politie en justitie.

Het impact assessment betreft de richtlijn inzake juridisch vertegenwoordigers[3] en de onderhavige verordening gezamenlijk en becijfert dat er initiële kosten worden gemaakt in de

[3] Richtlijn juridische vertegenwoordigers voor verzameling van bewijs in strafprocedures.

orde van grootte van 3,3 miljoen euro voor EU-lidstaten en 1,7 miljoen euro per lidstaat voor dienstaanbieders. Er worden geen terugkerende jaarlijkse kosten verwacht en zelfs jaarlijks terugkerende besparing in de orde van grootte van 7,1 miljoen euro voor EU-staten en 4,3 miljoen euro voor dienstaanbieders.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

De toegang tot elektronisch bewijs in alle vier in de verordening onderscheiden categorieën van gegevens is steeds moeilijker te verkrijgen (abonneegegevens, toegangsgegevens, transactiegegevens en inhoudelijke gegevens). In de praktijk blijkt het gebruik van de in het internationaal verkeer gangbare vormen van samenwerking, instrumenten van wederzijdse samenwerking in strafzaken, te langzaam en te bewerkelijk voor tijdige toegang tot gegevens door politie en justitie. Verder maken mensen, al dan niet met criminele intenties, gebruik van zogenoemde anonimiseringstechnieken (VPN, TOR) en van versleutelsoftware (encryptie). Veelal is het dan niet mogelijk te bepalen waar (op welke dataservers in welk land) gegevens zijn opgeslagen en daardoor is niet bekend aan welk land samenwerking kan worden gevraagd. Door deze factoren komen onderzoeken niet van de grond of lopen ze in een vroeg stadium vast, ook al is er sprake van Nederlandse verdachten en slachtoffers. Daadwerkelijke rechtshandhaving op het internet staat daardoor onder druk. De tijdens het Nederlands voorzitterschap van de JBZ-raad met zeer brede steun van andere lidstaten op 9 juni 2016 aangenomen Raadsconclusies ("improving criminal justice in cyberspace") worden door het kabinet als uitgangspunt genomen voor actieve steun aan de initiatieven die tot de onderhavige voorstellen voor e-evidence hebben geleid. Naast het voorstel voor de EU-verordening zijn er andere internationale ontwikkelingen op het gebied van elektronisch bewijs. Er wordt onderhandeld over wijziging van het cybercrimeverdrag 2001 van de Raad van Europa.

Verder wijst het kabinet erop dat op 23 maart jl. in de VS de Cloud Act werd aangenomen (*Cloud = Clarifying lawful overseas use of data*). Deze wet geeft een nieuw kader voor toegang door VS-autoriteiten tot data die beheerd worden door in de VS gevestigde technologiebedrijven wereldwijd. Deze regeling omvat daarnaast een raamwerk voor nieuwe bilaterale overeenkomsten tussen de VS en regeringen van andere landen voor grensoverschrijdende dataverzoeken. De VS beogen dat op grond van de bilaterale overeenkomsten de verdragspartijen juridische beperkingen, die technologieleveranciers verbieden om te voldoen aan de vordering van data door autoriteiten van het andere land, zullen opheffen.

b) Beoordeling en inzet ten aanzien van dit voorstel

Digitale opsporing in cyberspace vereist een eigen aanpak, die inspeelt op factoren die opsporing en vervolging in het digitale domein in toenemende mate bemoeilijken.

Vanwege de inherente grenzeloosheid van het internet is internationale samenwerking tussen landen in de opsporing en vervolging van cybercrime zeer belangrijk, alsmede optimalisering

van de huidige vormen van samenwerking en waar nodig ontwikkeling van aanvullende of nieuwe Europese of internationale juridische kaders. Vooral een snelle toegang tot elektronisch bewijs dat zich vaak op servers buiten de landsgrenzen bevindt, is onontbeerlijk geworden. Niet alleen bij cybercrimes zoals hacking en Ddos-aanvallen, bij cybergerelateerde criminaliteit (zoals seksueel misbruik van kinderen en de verkoop van drugs online), maar ook steeds meer bij allerhande vormen van traditionele criminaliteit. Dagelijkse handelingen en communicatie tussen mensen over al hun gedragingen gebeuren immers steeds meer online. Het gaat dan om gegevens, zoals de identiteit van de persoon die gebruik maakt van een via een IP-adres op het internet aangesloten geautomatiseerd werk (abonnee- en toegangsgegevens), maar ook over wie met wie geautomatiseerd communiceert, op welke manier en hoe lang (transactiegegevens). In verdere fases van het opsporingsonderzoek kan ook toegang tot de inhoud van de verwerkte gegevens (e-mails, documenten, afbeeldingen, enz.) nodig zijn. Bij het gebruik van internet doen grenzen er nog maar heel beperkt toe.

Daarom is het kabinet verheugd dat de Commissie het pakket e-evidence heeft gepresenteerd. Nederland ziet deze voorstellen als een belangrijke stap voorwaarts. De voorstellen bieden een oplossing voor een significant probleem in de rechtshandhaving. Daarnaast is het kabinet tevreden dat directe samenwerking als uitgangspunt is gekozen. Het Nederlandse standpunt is dat het voorstel evenwichtig moet zijn: het instrumentarium voor de rechtshandhaving moet worden verbeterd, er dienen goede waarborgen te worden opgenomen voor de rechten van personen en dienstenaanbieders en de uitvoering van de bevelen dient goed werkbaar te zijn ten behoeve van de dienstaanbieder.
De persoonsgegevens waarop dit voorstel betrekking heeft, zijn beschermd en mogen alleen worden verwerkt in overeenstemming met de algemene verordening gegevensbescherming en de richtlijn inzake gegevensbescherming voor politiële en strafrechtelijke autoriteiten. Dit is belangrijk met het oog op de positie van burgers.

Op een aantal belangrijke onderdelen van de verordening dient Nederland zijn positie nog te bepalen met het oog op het doen van voorstellen in de onderhandelingen over het voorstel. Deze onderdelen worden verder bestudeerd en onder meer zal een nationale impactanalyse worden uitgevoerd (zie 5.c en d.). Dit betreffen de volgende onderdelen:

a. de reikwijdte van het voorstel:
    - In het bijzonder wanneer en voor welke feiten een vordering kan worden uitgevaardigd en daarmee de mogelijke toename van de administratieve lasten voor dienstaanbieders.
    - Welke relatie of aanknopingspunt er moet zijn tussen de uitvaardigende lidstaat, de gevorderde gegevens en een dienstaanbieder; en
    - In het bijzonder de in het voorstel gebruikte zeer ruime definitie van elektronische dienstaanbieders in relatie tot de Nederlandse Telecommunicatiewet, de diversiteit aan bedrijven die op internetdiensten aan bieden, en in relatie tot het aantal te verwachten verzoeken en daarmee de mogelijke toename van de administratieve lasten ten nadele van het bedrijfsleven. Hierbij wordt ook nader gekeken naar de

kenbaarheid voor dienstaanbieders van de authenticiteit en integriteit van uit andere landen afkomstige verzoeken. Verder behoeven de gevolgen van de in het voorstel verwerkte mogelijke vergoedingsregeling aandacht.

b. De waarborgen en rechtsmiddelen in het voorstel. Het is positief dat de waarborgen die zijn opgenomen in de EU-regelgeving inzake gegevensbescherming van toepassing zijn. Bezien moet worden of de verwijzing naar de rechtsmiddelen die betrokkenen kunnen aanwenden in de lidstaat waar het strafproces plaatsheeft voldoende is, vanuit het perspectief van de persoon van wie data zijn verkregen alsmede vanuit het perspectief van de dienstaanbieder op grond van een Europees verstrekkingsbevel;
c. De relatie met het Europees Onderzoeksbevel (EOB) Richtlijn 2014/41/EU;
d. De regeling voor rechtsconflicten met derde landen;
e. De vraag of er een rol is voor de autoriteiten van de lidstaat waar de gegevens zijn opgeslagen of van de lidstaat waar de persoon, wiens gegevens het betreft, verblijft;
f. De aansprakelijkheid van bedrijven;
g. De rol van dienstaanbieders, onder meer bij de beoordeling of een bewaringsbevel of verstrekkingsbevel ten uitvoer kan worden gelegd.
h. De positie van het midden- en kleinbedrijf.

Een aantal van deze punten wordt in het onderstaande toegelicht.

Gelet op het voorgaande, onder a), ondersteunt Nederland de essentie van dit voorstel, dat voorziet in een mogelijkheid voor directe samenwerking tussen justitiële autoriteiten van lidstaten en dienstaanbieders. Overeenkomstig de eerdere Nederlandse inzet wordt daarbij de locatie waar de gegevens zijn opgeslagen niet meer als belangrijkste criterium gezien. Een vooral locatie gebonden aanpak past niet bij de realiteit dat dienstaanbieders de data in verschillende landen opslaan en bij het misbruik dat internationale criminele netwerken maken van de grenzeloosheid van het internet. In sommige gevallen worden gegevens verspreid om bedrijfseconomische redenen over verschillende datacentra in verschillende landen en geregeld verplaatst. De locatie waar de gegevens zich bevinden hebben geen tot nauwelijks verband met het land waar de gebruiker zich bevindt. Afhankelijk van het beleid van de aanbieder heeft de gebruiker hier ook geen tot nauwelijks zeggenschap over.

De locatie waar de gegevens zijn opgeslagen wordt losgelaten als criterium dat bepaalt bij welke autoriteit verzoeken om gegevens te verstrekken moeten worden ingediend. Daarom moet worden gezocht naar alternatieve aanknopingspunten die grensoverschrijdende gegevensverkrijging zonder tussenkomst van de autoriteiten van een andere lidstaat rechtvaardigen en begrenzen. Bij deze gegevensverkrijging moet de hoogste mate van transparantie worden nagestreefd. In de verordening is ervoor gekozen te kijken of dienstaanbieders in de Unie gevestigd zijn of daar hun diensten aanbieden. Dit is in lijn met de Algemene Verordening Gegevensbescherming.

Het voorstel in zijn huidige vorm raakt op rechtstatelijk vlak aan het legaliteitsbeginsel en heeft op internationaalrechtelijk vlak consequenties voor de soevereiniteit.
Opsporingsdiensten in de EU kunnen vorderingen versturen op basis van de feiten die in hun lidstaat strafbaar zijn en deze feiten hoeven dus niet naar Nederlands recht strafbaar te zijn. Opsporingsinstanties uit andere lidstaten kunnen dit ook doen voor Nederlanders wanneer de andere lidstaat rechtsmacht heeft, bijvoorbeeld doordat een Nederlander een misdrijf heeft begaan in het buitenland of (mogelijk in Nederland) een onderdaan van een andere lidstaat tot slachtoffer heeft gemaakt.

Het soevereiniteitsbeginsel houdt in dat iedere staat op zijn grondgebied bij uitsluiting bevoegd is te handelen overeenkomstig zijn eigen rechtsorde[4]. In EU-verband is wetgeving tot stand gekomen op grond waarvan beslissingen van een justitiële autoriteit van de ene lidstaat, worden erkend door de autoriteiten in de andere lidstaat (bijvoorbeeld het Europees Aanhoudingsbevel). In de voorgestelde verordening is er geen sprake van expliciete erkenning door autoriteiten van de betreffende lidstaat. De erkenning is eerder impliciet. De justitiële autoriteit van een lidstaat die bewijs vergaart kan een bevel tot verstrekking of bewaring rechtstreeks naar de vertegenwoordiger van de dienstaanbieder sturen.

De internationale aard van het internet en dataopslag en de vluchtigheid waarmee data kunnen worden verplaatst vormen een uitdaging voor een absolute opvatting aangaande het soevereiniteitsbeginsel.
In de maatschappelijke en economische praktijk worden data over landsgrenzen verplaatst. Het is daarom van belang om gezamenlijk afspraken te maken onder welke procedurele en inhoudelijke voorwaarden opsporingsdiensten toegang krijgen tot deze data. Nederland bestudeert of er een grotere rol zou moeten zijn voor de autoriteiten van het land of de lidstaat waar de gegevens zijn opgeslagen of van de lidstaat waar de persoon, wiens gegevens het betreft, verblijft.

Nederland is positief over de aandacht voor rechtsbescherming en fundamentele rechten. De aandachtspunten die Nederland benoemt, genoemd in punten a. tot en met f., staan niet op zichzelf, maar moeten in samenhang worden gezien. Zo wordt bij de bestudering van de vraag of het niveau van de voorgestelde waarborgen van de grondrechten voldoende is niet alleen gekeken naar de waarborgen en rechtsmiddelen in het voorstel, maar bijvoorbeeld ook naar de reikwijdte onder punt a.
Het kabinet zal bezien of de voorgestelde rol van bedrijven op zijn plaats is, onder meer waar dienstaanbieders gronden hebben om niet te voldoen aan een verstrekkingsbevel. Hierbij krijgt ook de aansprakelijkheid van bedrijven aandacht. Ook moet misbruik worden voorkomen, hiervoor is het belangrijk dat duidelijk is dat het verzoek van een opsporingsautoriteit komt. Verdere mogelijke financiële implicaties, gevolgen voor regeldruk en administratieve lasten voor bedrijven zal worden benoemd in hoofdstuk 5 paragraaf d.

[4] Aanwijzing inzake de informatie-uitwisseling in het kader van de wederzijdse rechtshulp in strafzaken.

Een belangrijk aandachtspunt is de samenhang met andere Europese (rechtshulp)instrumenten – waaronder het Europees onderzoeksbevel.

c) *Eerste inschatting van krachtenveld*

Hoewel veel lidstaten tijdens een eerste bespreking van het voorstel benadrukten het voorstel nog te bestuderen, lijken de lidstaten in algemene zin een positieve grondhouding aan te nemen ten opzichte van de hoofdlijnen van het voorstel. Een aantal lidstaten zou de reikwijdte van de verordening willen uitbreiden met rechtstreekse toegang tot gegevens en/of met Europese bevelen voor het onderscheppen van "real time" communicatiegegevens, die nog niet zijn opgeslagen. Verschillende lidstaten gaven aan de effectiviteit van het voorstel als belangrijk aandachtpunt te hebben, anderen wezen ook op de rechtsbescherming. In de JBZ-Raad van juni 2018 heeft het voorzitterschap geconcludeerd dat, rekening houdend met de onderhandelingen in de Raad over de Verordening e-evidence, uitbreiding van de reikwijdte van de verordening met real time interceptie en directe toegang op technisch niveau (expertgroep CIE) nader moet worden onderzocht. Slechts een zeer beperkt aantal lidstaten toont openheid ten aanzien van directe toegang. Voor opname van real time interceptie is meer steun, maar ook op dat punt is een groep lidstaten terughoudend. De Commissie is geen voorstander van uitbreiding van de reikwijdte op zowel inhoudelijke als politieke gronden. Zij wil een politiek akkoord bereiken tijdens huidige zittingsperiode.

Het krachtenveld in het Europees Parlement is op dit moment nog niet bekend. Wel kan worden gewezen op de resolutie die Europese Parlement heeft op 3 oktober 2017 heeft aangenomen over de aanpak van cybercrime. De resolutie erkent de problemen van politie en justitie bij het verkrijgen van grensoverschrijdende toegang tot elektronisch bewijs en benadrukt de noodzaak voor een gemeenschappelijke EU aanpak van strafrechtelijke handhaving in cyberspace, hetgeen met prioriteit moet worden opgepakt.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) *Bevoegdheid*

Het gaat hier om een gedeelde bevoegdheid tussen de EU en de LS (art. 4, lid 2, sub j, VWEU). Als rechtsgrondslag van de verordening wordt genoemd artikel 82, eerste lid van het Verdrag inzake de werking van de Europese Unie. Op grond van deze bepaling kan de Uniewetgever maatregelen vaststellen die ertoe strekken regels en procedures vast te leggen waarmee alle soorten vonnissen en 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. Nederland is het in beginsel eens met deze grondslag, maar wil wel dat nader wordt bekeken of de ontwerpverordening uitvoering geeft aan het beginsel van wederzijdse erkenning, aangezien van erkenning door een autoriteit in de ene lidstaat van een besluit van een autoriteit in een andere lidstaat niet per definitie sprake lijkt te zijn in het voorstel. Nederland zal hiervoor aandacht vragen.

b) *Subsidiariteit*

Nederland beoordeelt de subsidiariteit als positief. De grensoverschrijdende verkrijging van digitaal bewijs kan niet goed op landelijk, provinciaal of gemeentelijk niveau gebeuren. De voorstellen beogen regels te stellen over grensoverschrijdende toegang tot gegevens voor alle EU-lidstaten en hebben ook impact op internet dienstaanbieders die hun (hoofd)vestiging buiten de EU hebben. Opsporing en vervolging in cyberspace is verder nagenoeg per definitie grensoverschrijdend. De met het voorstel beoogde doelen kunnen niet worden bereikt als individuele lidstaten afwijkende regels invoeren.

c) *Proportionaliteit*

De voorgestelde maatregelen dragen bij aan een unierechtelijke aanpak. In beginsel staat de inhoud in verhouding tot het beoogde doel, te weten verbetering van de samenwerking met het oog op de verkrijging van elektronisch bewijs. Echter, Nederland is nog bezig met een nadere standpuntbepaling op de onder 3b genoemde punten. Dit betreft onder meer de reikwijdte van de verordening, de waarborgen en rechtsmiddelen, de regeling voor rechtsconflicten met derde landen, de rol van de lidstaten (bijvoorbeeld van de lidstaat waar de betrokken persoon verblijft) en de positie van bedrijven. Deze standpuntbepaling gebeurt tegen de achtergrond van een positieve grondhouding ten opzichte van dit voorstel.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) *Consequenties EU-begroting*

In het impact assessment uitgevoerd door de Europese Commissie is aangegeven dat geen directe budgettaire implicaties voor de EU-begroting worden voorzien.

b) *Financiële consequenties (incl. personele) voor rijksoverheid en/ of decentrale overheden*

Volgens het impact assessment zijn er voor lidstaten eenmalige kosten ("one-off costs") als gevolg van de implementatie van de voorgestelde regelingen. Het gaat om invoering van processen en eventueel de omzetting van elementen van de richtlijn en het waarborgen van de mogelijkheden van handhaving van een door justitiële autoriteiten uit een andere lidstaat tegen in Nederland gevestigde bedrijven uitgevaardigd verstrekkingsbevel en/of bewaringsbevel. De kosten zijn begroot op 3,3 miljoen Euro voor een EU-lidstaat. Dit betreft de richtlijn inzake juridisch vertegenwoordigers[5] en de onderhavige verordening gezamenlijk. De impactanalyse van de Commissie geeft aan dat er geen jaarlijks terugkerende kosten worden verwacht. Wel wordt ingeschat dat er mogelijk inverdieneffecten zijn als gevolg van – op termijn - meer gestroomlijnde en efficiëntere processen die druk van de rechtshulp kanalen afnemen en mogelijk het volume van criminaliteit doen verminderen.
Artikel 12 van de voorgestelde verordening geeft ruimte voor een vergoeding van kosten die een aanbieder maakt als gevolg van een tegen hem afgeven verstrekkingsbevel in het geval

[5] Richtlijn juridische vertegenwoordigers voor verzameling van bewijs in strafprocedures.

de uitvaardigende lidstaten in vergelijkbare nationale vorderingen bij providers een vergoedingsregeling heeft. Met de "Regeling kosten aftappen en gegevensverstrekking", van 30 maart 2005, nr. WJZ 5017828 (enkele keren herzien) kent Nederland zo een vergoedingsregel. Het betreft een beperkte vergoeding van door bedrijven te maken administratiekosten en personeelskosten die rechtstreeks voortvloeien uit informatieverstrekkingsactiviteiten. Een nationale impactanalyse zal inzicht moeten geven in de daadwerkelijke consequenties als gevolg van het onderhavige voorstel.

Er zijn geen financiële consequenties voor decentrale overheden.

Eventuele) budgettaire gevolgen worden ingepast op de begroting van het/de beleidsverantwoordelijk(e)) departement(en), conform de regels van de budgetdiscipline.

c) *Financiële consequenties (incl. personele) voor bedrijfsleven en burger*

Volgens het Impact assessment zijn er voor het bedrijfsleven (aanbieders) eenmalige kosten ("one-off costs") als gevolg van de implementatie van de voorgestelde regelingen. De kosten zijn begroot op 1,7 miljoen Euro voor het bedrijfsleven in een EU-lidstaat. De kosten worden gemaakt voor de invoering van nieuwe procedures en het opleiden van personeel. Daarnaast is sprake van terugkerende kosten. Per verstrekking zullen aanbieders administratiekosten en personeelskosten maken die rechtstreeks voortvloeien uit concrete informatieverstrekkingsactiviteiten. Volgens de impactanalyse zouden voor providers ook jaarlijkse besparingen mogelijk zijn doordat zij bij de verstrekking nu kunnen werken met een geharmoniseerd kader en niet meer hoeven te reageren op mogelijk tussen staten verschillende rechtsregels.
Het ministerie van Justitie en Veiligheid neemt het initiatief tot de uitvoering van een impactanalyse die meer inzicht moet geven in de consequenties van het voorstel voor Nederland. Worden geen structurele financiële consequenties voor burgers verwacht. De financiële compensatie voor medewerking hangt af van de regelgeving in het uitvoerende land. In Nederland krijgen momenteel grotere dienstaanbieders een lumpsum vergoeding en de kleinere 'aanbieders een beperkte vergoeding op basis van het aantal bevragingen.
Nederland heeft in vergelijking met andere landen een grote elektronische dienstverlenersbranche die zich op de internationale markt richt. Naast grotere bedrijven zijn ook veel MKB-bedrijven actief, waarbij de gevolgen van het voorstel voor deze groepen verschillend zijn.
De eerste inschatting van het kabinet is dat de kosten in de praktijk hoger kunnen zijn, dan in het impact assessment van de Europese Commissie is berekend; zeker als bepaalde bewarings- en verstrekkingsbevelen kunnen worden uitgevaardigd bij onderzoek naar elk denkbaar strafbaar feit.

d) *Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger*

Een nationale impactanalyse zal inzicht moeten geven in de consequenties van het voorstel voor Nederland, hierin wordt het bedrijfsleven meegenomen. Het kabinet bestudeert het voorstel nog op de punten genoemd in hoofdstuk 3 b), omdat er geen onredelijk verhoging van de administratieve lasten mag plaatsvinden en het voor de effectiviteit van het voorstel nodig is dat de regels ook werkbaar zijn voor dienstaanbieders. Het kabinet is van mening dat de verstrekking van bewijs na het voldoen van een vordering geen aansprakelijkheid voor deze bedrijven kan opleveren.

e) *Gevolgen voor concurrentiekracht*

Regels omtrent de omgang met data, onder meer op het gebied van strafrechtelijk onderzoek (gegevensverstrekking), zijn een belangrijke factor die de concurrentiekracht voor digitale dienstverleners kunnen beïnvloeden. Omdat de voorgestelde verordening directe werking heeft en daardoor in elke lidstaat op eenzelfde wijze doorwerkt, beïnvloedt het de Nederlandse concurrentiekracht vis-à-vis andere Europese lidstaten niet. Mogelijk wordt wel de concurrentiekracht ten opzichte van derde landen waarin deze regels niet gelden beïnvloed, maar de mate waarin is nu nog niet bekend. Verder biedt de EU een grote markt, zodat de regelgeving op dit terrein voor aanbieders wellicht geen belemmering zal vormen om zich in de EU te vestigen.

6. Implicaties juridisch

a) *Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)*

Het betreft een verordening in de zin van artikel 288 WVEU. Deze is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat. Op een aantal onderdelen is niettemin Nederlandse besluitvorming en wetgeving nodig, bijvoorbeeld om financiële sancties op te kunnen leggen bij inbreuken op de verplichtingen van dienstenaanbieders om verstrekkingsbevelen of bewaringsbevelen ten uitvoer te leggen en bij een inbreuk op de verplichting om zich te onthouden van het informeren van de persoon van wie data worden achterhaald. Verder moeten de autoriteiten worden aangewezen die bevoegd zijn om Europese verstrekkingsbevelen en bewaringsbevelen uit te vaardigen. Dit geldt ook voor de handhavende autoriteiten die bevoegd zijn om de genoemde bevelen te handhaven namens een andere lidstaat. Ook moeten de gerechten worden aangewezen die bevoegd zijn om gemotiveerde bezwaren van aanbieders te behandelen, overeenkomstig de artikelen 15 en 16.

b) *Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan*

Artikel 21 voorziet in de uitoefening van delegatie aan de Commissie. Dit betreft de bevoegdheid tot wijziging van de certificaten en formulieren die bij de verordening horen, zoals bepaald in artikel 20. Het Europees Parlement of de Raad kunnen deze bevoegdheid herroepen. Voordat een gedelegeerde regeling wordt vastgesteld moet de Commissie experts consulteren die worden aangewezen door elke lidstaat. Een gedelegeerde regeling treedt

alleen in werking als er geen bezwaren zijn geuit door het Europees Parlement of de Raad binnen een periode van twee maanden na notificatie van die regeling (te verlengen met evt. nog twee maanden).
De keuze voor gedelegeerde handelingen ligt juridisch gezien voor de hand aangezien het gaat om een bevoegdheid tot wijziging van bijlagen. Het kabinet vindt het belangrijk dat toekomstige signalen uit de praktijk waar nodig leiden tot aanpassing van de certificaten en formulieren. Als er voorstellen worden gedaan om de formulieren aan te passen, dan dienen daarom het OM en het bedrijfsleven hierbij te worden betrokken. Het kabinet zal dit onder de aandacht brengen van de Commissie.

c) *Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid.*
Voorgesteld wordt dat de verordening in werking treedt op de twintigste dag na haar publicatie. Zes maanden nadien zal de verordening worden toegepast.
Het kabinet vindt dat, nadat de verordening is vastgesteld, voldoende tijd beschikbaar moet zijn voor de betrokken dienstenaanbieders en overheidsdiensten om zich voor te bereiden op de toepassing van de verordening. Bij de invoering van de nieuwe systematiek is zorgvuldigheid vereist, omdat het persoonsgegevens betreft, een groot aantal bedrijven betrokken is en "schijnbare details" essentieel kunnen zijn voor het goed functioneren van de nieuwe aanpak. De termijn van zes maanden is daartoe niet voldoende.

d) Wenselijkheid evaluatie-/horizonbepaling
Artikel 24 voorziet in een evaluatiebepaling. Het kabinet ondersteunt het voorstel om de regeling te evalueren.

7. Implicaties voor uitvoering en/of handhaving
Aan het opstellen van de voorstellen is een intensief proces voorafgegaan van expertmeetings met deskundigen uit de lidstaten, ook uit de uitvoering, en overleg met belanghebbenden, zoals dienstaanbieders en uit het maatschappelijk middenveld (civil society).

De opsporingsdiensten krijgen de bevoegdheid om direct grensoverschrijdend bewijs te vorderen. De noodzakelijke toegang tot elektronisch bewijs wordt hierdoor verbeterd. Gegeven het feit dat elektronisch bewijs steeds belangrijker wordt en de nationale autoriteit in principe niet meer betrokken is bij een buitenlands verzoek zal dit ook een positief effect hebben op de druk op het verwerken van rechtshulpverzoeken in de toekomst. Daarnaast is de informatie in een rechtshulpverzoek een gewaarde informatiebron, bijvoorbeeld voor nationale onderzoeken. In de huidige vorm van het voorstel is de nationale autoriteit waar de dienstverlener is gevestigd in eerste instantie niet betrokken dus draagt het Europese verstrekkingsbevel en het – bewaringsbevel niet bij aan deze informatiebron. Bij niet-nakoming (dat wil zeggen het niet bewaren of verstrekken van gegevens) wordt het uitvoeren van de vordering overgedragen aan de lidstaat waar de dienstaanbieder is gevestigd. Deze lidstaat zal dan moeten optreden ten opzichte van de aanbieder.

8. Implicaties voor ontwikkelingslanden

Er worden geen bijzondere implicaties voor ontwikkelingslanden voorzien.