



EUROPESE
COMMISSIE

Brussel, 25.11.2021
COM(2021) 719 final

2021/0383 (NLE)

Voorstel voor een

BESLUIT VAN DE RAAD

houdende machtiging van de lidstaten om, in het belang van de Europese Unie, het tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, inzake nauwere samenwerking en verstrekking van elektronisch bewijsmateriaal te ratificeren

TOELICHTING

1. ONDERWERP VAN HET VOORSTEL

Dit voorstel betreft het besluit waarbij de lidstaten worden gemachtigd om in het belang van de Europese Unie over te gaan tot ratificatie van het tweede Aanvullend Protocol betreffende nauwere samenwerking en verstrekking van elektronisch bewijsmateriaal bij het Verdrag van Boedapest inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken van de Raad van Europa (hierna “het protocol” genoemd)¹. Doel van het protocol is te voorzien in gemeenschappelijke voorschriften op internationaal niveau ter versterking van de samenwerking inzake cybercriminaliteit en de vergaring van bewijs in elektronische vorm ten behoeve van strafrechtelijke onderzoeken en procedures.

Dit voorstel vormt een aanvulling op een afzonderlijk voorstel van de Commissie voor een besluit van de Raad van de Europese Unie (hierna “de Raad”) waarbij de lidstaten worden gemachtigd het protocol in het belang van de Europese Unie te ondertekenen.

Cybercriminaliteit blijft een grote uitdaging voor onze samenleving. Ondanks de inspanningen van de rechtshandavingsinstanties en de justitiële autoriteiten nemen cyberaanvallen, waaronder aanvallen met ransomware, toe en worden zij complexer². Met name doordat het internet geen grenzen kent, zijn onderzoeken op het gebied van cybercriminaliteit vrijwel altijd grensoverschrijdend van aard en is dan ook nauwe samenwerking tussen instanties in verschillende landen vereist.

Elektronisch bewijsmateriaal wordt voor strafrechtelijke onderzoeken steeds belangrijker. De Commissie schat dat rechtshandavingsinstanties en justitiële autoriteiten thans in 85 % van de strafrechtelijke onderzoeken, met inbegrip van die op het gebied van cybercriminaliteit, toegang moeten hebben tot elektronisch bewijsmateriaal³. Bewijzen van strafbare feiten worden door serviceproviders in buitenlandse rechtsgebieden steeds vaker in elektronische vorm bewaard, zodat een doeltreffende strafrechtelijke reactie passende maatregelen vereist om dergelijk bewijsmateriaal te verkrijgen teneinde de rechtsstaat te handhaven.

Wereldwijd wordt gewerkt aan verbetering van de grensoverschrijdende toegang tot elektronisch bewijsmateriaal voor strafrechtelijke onderzoeken, zowel op nationaal niveau als op EU-niveau⁴ en op internationaal niveau, onder meer door middel van het protocol. Het is belangrijk dat er op internationaal niveau compatibele voorschriften komen om wetsconflicten te vermijden wanneer om grensoverschrijdende toegang tot elektronisch bewijsmateriaal wordt gevraagd.

2. CONTEXT VAN HET VOORSTEL

2.1. Achtergrond

Het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (CETS nr. 185), ook wel het verdrag inzake cybercriminaliteit of het cybercrimeverdrag genoemd en hierna aangeduid als “het verdrag”, moet bijdragen aan de strijd tegen strafbare feiten waarbij van computernetwerken gebruik wordt gemaakt. Het verdrag 1) bevat bepalingen voor de harmonisatie van nationale bepalingen van materieel

¹ De tekst van het protocol is in een bijlage bij dit voorstel opgenomen.

² Dreigingsevaluatie van de Europese Unie voor zware en georganiseerde criminaliteit 2021 (EU SOCTA 2021).

³ SWD(2018) 118 final.

⁴ COM(2018) 225 en 226 final.

strafrecht betreffende strafbare feiten en daarmee samenhangende bepalingen op het gebied van cybercriminaliteit, 2) voorziet in de nodige bevoegdheden in het nationale strafprocesrecht voor het onderzoeken en vervolgen van dergelijke feiten en andere strafbare feiten die door middel van een computersysteem zijn gepleegd of waarvoor bewijzen in elektronische vorm bestaan, en 3) is gericht op een snelle en doeltreffende regeling voor internationale samenwerking.

Het verdrag staat open voor de lidstaten van de Raad van Europa en op uitnodiging voor staten die geen lid zijn. Momenteel zijn 66 landen partij bij het Verdrag, waaronder 26 lidstaten van de Europese Unie⁵. Het verdrag voorziet er niet in dat de Europese Unie tot het verdrag kan toetreden. De Europese Unie wordt evenwel erkend als een organisatie met de status van waarnemer bij de commissie Cybercrimeverdrag (T-CY)⁶.

Ondanks de inspanningen om op het niveau van de Verenigde Naties te onderhandelen over een nieuw verdrag inzake cybercriminaliteit⁷ blijft het Verdrag van Boedapest het belangrijkste multilaterale verdrag voor de bestrijding van cybercriminaliteit. De Unie steunt het verdrag consequent⁸, ook in het kader van de financiering van programma's voor capaciteitsopbouw⁹.

Naar aanleiding van voorstellen van de Cloud Evidence Group¹⁰ heeft de commissie Cybercrimeverdrag verscheidene aanbevelingen aangenomen om, onder meer via onderhandelingen over een tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken betreffende nauwere internationale samenwerking, het probleem aan te pakken dat elektronisch bewijsmateriaal in verband met cybercriminaliteit en andere strafbare feiten steeds vaker in handen is van serviceproviders in buitenlandse rechtsgebieden, terwijl de bevoegdheden van de rechtshandhavinginstanties beperkt blijven door territoriale grenzen. In juni 2017 heeft de commissie Cybercrimeverdrag de Terms of Reference vastgesteld voor de voorbereiding van het tweede aanvullend protocol in de periode tussen september 2017 en december 2019¹¹. Omdat er meer tijd nodig bleek om de besprekingen af te ronden en gezien de beperkingen waartoe de COVID-19-pandemie in 2020 en 2021 leidde, heeft de commissie Cybercrimeverdrag het mandaat tweemaal verlengd, eerst tot december 2020 en vervolgens tot mei 2021.

Naar aanleiding van de oproep van de Europese Raad in zijn conclusies van 18 oktober 2018¹² heeft de Commissie op 5 februari 2019 een aanbeveling aangenomen voor een besluit van de Raad houdende machtiging van de Commissie tot deelname, namens de Europese Unie, aan de onderhandelingen over een tweede aanvullend protocol bij het Verdrag van de Raad van

⁵ Alle lidstaten, met uitzondering van Ierland, dat het verdrag heeft ondertekend zonder het te ratificeren, maar wel heeft toegezegd toetreding tot het verdrag na te streven.

⁶ Reglement van orde van de commissie Cybercrimeverdrag (T-CY (2013) 25 rev), beschikbaar op www.coe.int/cybercrime.

⁷ Resolutie 74/247 van de Algemene Vergadering van de Verenigde Naties van december 2019 over de bestrijding van het gebruik van informatie- en communicatietechnologieën voor criminele doeleinden. JOIN(2020) 81 final.

⁹ Zie bijvoorbeeld de Global Action on Cybercrime Extended (GLACY)+ op <https://www.coe.int/en/web/cybercrime/glacyplus>

¹⁰ Eindverslag van de Cloud Evidence Group van de commissie Cybercrimeverdrag "Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY" van 16 september 2016.

¹¹ <https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690>

¹² <https://www.consilium.europa.eu/nl/press/press-releases/2018/10/18/20181018-european-council-conclusions/>

Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken¹³. De Europese Toezichthouder voor gegevensbescherming heeft op 2 april 2019 advies uitgebracht over de aanbeveling¹⁴. Bij besluit van 6 juni 2019 heeft de Raad van de Europese Unie de Commissie gemachtigd om namens de Europese Unie deel te nemen aan de onderhandelingen over het tweede aanvullend protocol¹⁵.

Zoals verwoord in de EU-strategie voor de veiligheidsunie van 2020¹⁶, de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk van 2020¹⁷ en de EU-strategie voor de aanpak van georganiseerde criminaliteit van 2021¹⁸ heeft de Commissie zich ertoe verbonden de onderhandelingen over het protocol snel en met succes af te ronden. Ook het Europees Parlement stelde in zijn resolutie van 2021 over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk¹⁹ dat de werkzaamheden aan het protocol moesten worden afgerond.

Overeenkomstig het besluit van de Raad van de Europese Unie heeft de Commissie namens de Europese Unie deelgenomen aan de onderhandelingen over het protocol. De Commissie heeft over het standpunt van de Unie consequent overleg gepleegd met het speciaal comité van de Raad voor de onderhandelingen.

Overeenkomstig het Kaderakkoord over de betrekkingen tussen het Europees Parlement en de Europese Commissie²⁰ heeft de Commissie het Europees Parlement ook door middel van schriftelijke verslagen en mondelinge presentaties op de hoogte gehouden van de voortgang van de onderhandelingen.

Op de plenaire vergadering van de commissie Cybercrimeverdrag van 28 mei 2021 heeft de commissie het ontwerpprotocol op haar niveau goedgekeurd en het ontwerp ter aanneming voorgelegd aan het Comité van Ministers van de Raad van Europa²¹. Op 17 november 2021 heeft het Comité van Ministers van de Raad van Europa het protocol aangenomen.

2.2. Tweede aanvullend protocol

Het protocol moet zorgen voor verbetering van de samenwerking op het gebied van cybercriminaliteit en de vergaring van bewijs in elektronische vorm van enig strafbaar feit met het oog op specifieke strafrechtelijke onderzoeken of procedures. In het protocol wordt erkend dat er behoefte is aan meer en efficiëntere samenwerking tussen staten en met de particuliere sector, en aan meer duidelijkheid en rechtszekerheid voor serviceproviders en andere entiteiten met betrekking tot de omstandigheden waarin zij kunnen reageren op verzoeken van strafrechtelijke autoriteiten in andere partijen om verstrekking van elektronisch bewijsmateriaal.

In het protocol wordt ook erkend dat doeltreffende grensoverschrijdende samenwerking voor strafrechtelijke doeleinden, onder meer tussen overheidsinstanties en entiteiten van de particuliere sector, doeltreffende voorwaarden en krachtige waarborgen voor de bescherming van de grondrechten vereist. Daartoe wordt in het protocol uitgegaan van een op rechten

¹³ COM(2019) 71 final.

¹⁴ Advies van de EDPS over deelname aan de onderhandelingen over een tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit (advies 3/2019 van 2 april 2019).

¹⁵ Besluit van de Raad met documentnummer 9116/19.

¹⁶ COM(2020) 605 final.

¹⁷ JOIN(2020) 81 final.

¹⁸ COM(2021) 170 final.

¹⁹ Resolutie van het Europees Parlement van 10 juni 2021 over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk.

²⁰ PB L 304 van 20.11.2010, blz. 47.

²¹ <https://rm.coe.int/0900001680a2aa42>

gebaseerde benadering en wordt voorzien in voorwaarden en waarborgen die in overeenstemming zijn met de internationale mensenrechteninstrumenten, waaronder het Verdrag van de Raad van Europa tot bescherming van de rechten van de mens en de fundamentele vrijheden van 1950. Aangezien elektronisch bewijsmateriaal vaak persoonsgegevens betreft, zijn in het protocol ook krachtige waarborgen voor de bescherming van de persoonlijke levenssfeer en persoonsgegevens opgenomen.

De in de volgende alinea's bedoelde bepalingen zijn van bijzonder belang voor het protocol. Het protocol gaat vergezeld van een uitvoerige toelichting. Hoewel de toelichting geen instrument is dat een gezaghebbende interpretatie van het protocol biedt, is het bedoeld om de partijen te begeleiden en bij te staan bij de toepassing van het protocol²².

2.2.1. Gemeenschappelijke bepalingen

In hoofdstuk I van het protocol zijn gemeenschappelijke bepalingen opgenomen. In artikel 2 wordt het toepassingsgebied van het protocol vastgesteld, in overeenstemming met het toepassingsgebied van het verdrag: het is van toepassing op specifieke strafrechtelijke onderzoeken en procedures die betrekking hebben op strafbare feiten die verband houden met computersystemen en -gegevens, en op de vergaring van bewijs in elektronische vorm van enig strafbaar feit.

In artikel 3 zijn definities opgenomen van “centrale autoriteiten”, “bevoegde autoriteiten”, “noodsituaties”, “persoonsgegevens” en “doorgevende partij”. Deze definities zijn van toepassing op het protocol, samen met de definities die in het verdrag zijn opgenomen.

In artikel 4 wordt bepaald welke talen de partijen in het kader van het protocol moeten gebruiken voor het indienen van bevelen, verzoeken of kennisgevingen.

2.2.2. Samenwerkingsmaatregelen

In hoofdstuk II van het protocol zijn maatregelen ter verbetering van de samenwerking opgenomen. In lid 1 van artikel 5 wordt allereerst bepaald dat de partijen op basis van het protocol zoveel mogelijk moeten samenwerken. In de leden 2 tot en met 5 van artikel 5 wordt bepaald hoe de maatregelen van het protocol moeten worden toegepast met betrekking tot bestaande verdragen of regelingen inzake wederzijdse bijstand. In lid 7 van artikel 5 wordt bepaald dat de maatregelen van hoofdstuk II niet mogen leiden tot beperking van de samenwerking tussen de partijen, of de samenwerking met serviceproviders of entiteiten, op grond van andere toepasselijke overeenkomsten, regelingen, praktijken of het nationale recht.

Artikel 6 biedt met betrekking tot de verstrekking van domeinnaamregistratiegegevens een basis voor rechtstreekse samenwerking tussen bevoegde autoriteiten in de ene partij en entiteiten die in een andere partij domeinnaamregistratiediensten aanbieden.

Artikel 7 biedt met betrekking tot de verstrekking van abonneegegevens een basis voor rechtstreekse samenwerking tussen de bevoegde autoriteiten van de ene partij en serviceproviders in een andere partij.

Artikel 8 biedt met betrekking tot de verstrekking van computergegevens een basis voor nauwere samenwerking tussen autoriteiten.

Artikel 9 biedt met betrekking tot de verstrekking van computergegevens in een noodsituatie een basis voor samenwerking tussen autoriteiten.

Artikel 10 biedt een basis voor wederzijdse rechtshulp in noodsituaties.

²² Zie punt 2 van de toelichting bij het protocol.

Artikel 11 biedt een basis voor samenwerking via videoconferentie.

Artikel 12 biedt een basis voor gezamenlijke onderzoeken en gemeenschappelijke onderzoeksteams.

2.2.3. Waarborgen

Het protocol gaat uit van een op rechten gebaseerde benadering met specifieke voorwaarden en waarborgen, waarvan er enkele zijn opgenomen in de specifieke samenwerkingsmaatregelen en in hoofdstuk III van het protocol. Artikel 13 van het protocol bepaalt dat de partijen erop moeten toezien dat de bevoegdheden en procedures onderworpen zijn aan een passend niveau van bescherming van de grondrechten, dat in overeenstemming met artikel 15 van het verdrag de toepassing van het evenredigheidsbeginsel waarborgt.

Artikel 14 van het protocol voorziet in de bescherming van persoonsgegevens zoals gedefinieerd in artikel 3 van het protocol, in overeenstemming met het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (CETS 223) (Verdrag 108+) en het Unierecht.

In artikel 14, leden 2 tot en met 15, zijn op die basis de fundamentele gegevensbeschermingsbeginselen opgenomen, waaronder doelbinding, de rechtsgrondslag, bepalingen inzake gegevenskwaliteit en de regels die van toepassing zijn op de verwerking van bijzondere categorieën gegevens, de verplichtingen die voor verwerkingsverantwoordelijken gelden, onder meer inzake bewaring, het bijhouden van registers, beveiliging en verdere doorgifte, afdwingbare individuele rechten, onder meer inzake kennisgeving, toegang, rectificatie en geautomatiseerde besluitvorming, onafhankelijk en doeltreffend toezicht door een of meer autoriteiten en administratief beroep en beroep in rechte. De waarborgen hebben betrekking op alle vormen van samenwerking waarin het protocol voorziet, waar nodig aangepast om rekening te houden met de specifieke kenmerken van rechtstreekse samenwerking (bv. bij kennisgeving van inbreuken). De uitoefening van bepaalde individuele rechten kan worden uitgesteld, beperkt of geweigerd indien dat noodzakelijk is voor het nastreven van belangrijke doelstellingen van algemeen belang en evenredig is met dat doel, met name om risico's voor lopende rechtshandavingsonderzoeken te voorkomen, hetgeen ook in overeenstemming is met het recht van de Unie.

Artikel 14 van het protocol moet bovendien worden gelezen in samenhang met artikel 23 van het protocol. Artikel 23 maakt de door het protocol geboden waarborgen doeltreffender, door te bepalen dat de commissie Cybercrimeverdrag een beoordeling zal verrichten van de uitvoering en toepassing van de maatregelen van de nationale wetgeving om uitvoering te geven aan de bepalingen van het protocol. Met name wordt in artikel 23, lid 3, uitdrukkelijk erkend dat de tenuitvoerlegging van artikel 14 door de partijen zal worden geëvalueerd zodra tien partijen bij het verdrag hebben verklaard ermee in te stemmen door het protocol gebonden te zijn.

Op grond van artikel 14, lid 15, geldt verder de waarborg dat een partij die over substantieel bewijs beschikt dat een andere partij de in het protocol vervatte waarborgen stelselmatig of wezenlijk schendt, de doorgifte van persoonsgegevens aan die partij mag opschorten na overleg (hetgeen in dringende gevallen niet vereist is). Persoonsgegevens die vóór de opschorting zijn doorgegeven, worden ook na de opschorting overeenkomstig het protocol behandeld.

Tot slot wordt in artikel 14, lid 1, punten b) en c), van het protocol, gezien het multilaterale karakter van het protocol, de partijen de mogelijkheid geboden om in hun bilaterale betrekkingen onder bepaalde voorwaarden afspraken te maken over alternatieve manieren om de bescherming van uit hoofde van het protocol doorgegeven persoonsgegevens te

waarborgen. Hoewel de waarborgen van artikel 14, leden 2 tot en met 15, standaard van toepassing zijn op partijen die persoonsgegevens ontvangen, kunnen de partijen die onderling gebonden zijn door een internationale overeenkomst tot vaststelling van een alomvattend kader voor de bescherming van persoonsgegevens overeenkomstig de toepasselijke voorschriften van de wetgeving van de betrokken partijen, op grond van artikel 14, lid 1, punt b), ook overeenkomstig dat kader handelen. Dit betreft bijvoorbeeld Verdrag 108+ (voor de partijen die gegevensdoorgiften naar andere partijen in het kader van dat verdrag toestaan) of de raamovereenkomst tussen de EU en de VS (binnen het toepassingsgebied ervan, d.w.z. waar het gaat om de doorgifte van persoonsgegevens tussen autoriteiten of, in combinatie met een specifieke doorgifteregeling tussen de VS en de EU, om rechtstreekse samenwerking tussen autoriteiten en serviceproviders). Voorts kunnen de partijen op grond van artikel 14, lid 1, punt c), onderling bepalen dat de doorgifte van persoonsgegevens plaatsvindt op basis van andere overeenkomsten of regelingen tussen de betrokken partijen. Voor de EU-lidstaten kan voor gegevensdoorgiften in het kader van het protocol slechts gebruik worden gemaakt van een dergelijke alternatieve overeenkomst of regeling als de doorgifte voldoet aan de vereisten van het Unierecht inzake gegevensbescherming, namelijk hoofdstuk V van Richtlijn (EU) 2016/680 (richtlijn gegevensbescherming bij rechtshandhaving), alsmede (voor rechtstreekse samenwerking tussen autoriteiten en serviceproviders uit hoofde van de artikelen 6 en 7 van het protocol) hoofdstuk V van Verordening (EU) 2016/679 (algemene verordening gegevensbescherming).

2.2.4. Slotbepalingen

In hoofdstuk IV van het protocol zijn slotbepalingen opgenomen. Artikel 15, lid 1, punt a), waarborgt onder meer dat de partijen hun betrekkingen inzake de in het protocol genoemde aangelegenheden kunnen vaststellen, in overeenstemming met artikel 39, lid 2, van het verdrag. Artikel 15, lid 1, punt b), waarborgt dat EU-lidstaten die partij zijn bij het protocol, het Unierecht in hun onderlinge betrekkingen kunnen blijven toepassen. Artikel 15, lid 2, bepaalt ook dat artikel 39, lid 3, van het verdrag van toepassing is op het protocol.

Artikel 16, lid 3, bepaalt dat het protocol in werking treedt zodra vijf partijen bij het verdrag hebben verklaard ermee in te stemmen door het protocol gebonden te zijn.

Artikel 19, lid 1, bepaalt dat de partijen voorbehouden kunnen maken met betrekking tot artikel 7, lid 9, punten a) en b), artikel 8, lid 13, en artikel 17. Artikel 19, lid 2, bepaalt dat de partijen verklaringen kunnen afleggen met betrekking tot artikel 7, lid 2, punt b), en lid 8, artikel 8, lid 11, artikel 9, lid 1, punt b), en lid 5, artikel 10, lid 9, artikel 12, lid 3, en artikel 18, lid 2. Artikel 19, lid 3, bepaalt dat een partij verklaringen moet afleggen of kennisgevingen of mededelingen moet doen als bedoeld in artikel 7, lid 5, punten a) en e), artikel 8, lid 4, en lid 10, punten a) en b), artikel 14, lid 7, punt c), en lid 10, punt b), en artikel 17, lid 2.

Artikel 23, lid 1, vormt een basis voor overleg tussen de partijen, onder meer via de commissie Cybercrimeverdrag, overeenkomstig artikel 46 van het verdrag. Artikel 23, lid 2, vormt bovendien een basis voor de beoordeling van de toepassing en de uitvoering van de bepalingen van het protocol. Artikel 23, lid 3, strekt ertoe dat met de beoordeling van de toepassing en de uitvoering van artikel 14 inzake gegevensbescherming wordt begonnen zodra tien partijen hebben verklaard ermee in te stemmen door het protocol gebonden te zijn.

2.3. Unierecht en Uniebeleid op dit gebied

Het gebied waarop het protocol van toepassing is, valt grotendeels onder gemeenschappelijke voorschriften die op basis van artikel 82, lid 1, en artikel 16 VWEU zijn vastgesteld. Het huidige rechtskader van de Europese Unie omvat in het bijzonder instrumenten op het gebied

van rechtshandhaving en justitiële samenwerking in strafzaken, zoals Richtlijn 2014/41/EU betreffende het Europees onderzoeksbevel in strafzaken, de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie en Kaderbesluit 2002/465/JBZ van de Raad inzake gemeenschappelijke onderzoeksteams. Wat de externe betrekkingen betreft, heeft de Europese Unie een aantal bilaterale overeenkomsten gesloten met derde landen, zoals de overeenkomsten betreffende wederzijdse rechtshulp in strafzaken met de Verenigde Staten van Amerika, met Japan en met Noorwegen en IJsland. Het huidige rechtskader van de Europese Unie omvat ook Verordening (EU) 2017/1939 van de Raad betreffende nauwere samenwerking bij de instelling van het Europees Openbaar Ministerie (“EOM”). De lidstaten die aan de nauwere samenwerking deelnemen, moeten ervoor zorgen dat het EOM bij de uitoefening van zijn bevoegdheden, als bedoeld in de artikelen 22, 23 en 25 van Verordening (EU) 2017/1939, in het kader van het protocol op dezelfde wijze om medewerking kan verzoeken als de nationale aanklagers van die lidstaten. Deze instrumenten en overeenkomsten hebben met name betrekking op de artikelen 8, 9, 10, 11 en 12 van het protocol.

Daarnaast heeft de Unie diverse richtlijnen vastgesteld die de procedurele rechten van verdachten en beklaagden versterken²³. Deze instrumenten hebben met name betrekking op de artikelen 6, 7, 8, 9, 10, 11, 12 en 13 van het protocol. Een aantal bijzondere waarborgen betreft de bescherming van persoonsgegevens, een grondrecht dat is verankerd in de EU-Verdragen en in het Handvest van de grondrechten van de Europese Unie. Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met Verordening (EU) 2016/679 (algemene verordening gegevensbescherming) en Richtlijn (EU) 2016/680 (richtlijn gegevensbescherming bij rechtshandhaving). De privacy van de communicatie is een essentieel onderdeel van het grondrecht van eenieder op eerbiediging van het privéleven en het familie- en gezinsleven, de woning en de communicatie. Elektronischecommunicatiegegevens mogen alleen worden verwerkt in overeenstemming met Richtlijn 2002/58/EG (e-privacyrichtlijn). Deze instrumenten hebben met name betrekking op artikel 14 van het protocol.

In artikel 14, leden 2 tot en met 15, van het protocol wordt voorzien in passende waarborgen op het gebied van gegevensbescherming in de zin van de gegevensbeschermingsvoorschriften van de Unie, en met name artikel 46 van de algemene verordening gegevensbescherming en artikel 37 van de richtlijn gegevensbescherming bij rechtshandhaving, en de desbetreffende

²³ 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); 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); 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); Richtlijn (EU) 2016/1919 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); 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); Richtlijn (EU) 2016/343 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); Richtlijn 2012/13/EU van het Europees Parlement en de Raad van 22 mei 2012 betreffende het recht op informatie in strafprocedures.

rechtspraak van het Europees Hof van Justitie. Zoals vereist overeenkomstig het Unierecht²⁴ en om de doeltreffendheid van de waarborgen van artikel 14 van het protocol te waarborgen, moeten de lidstaten ervoor zorgen dat personen van wie gegevens zijn doorgegeven, daarvan in kennis worden gesteld, met inachtneming van bepaalde beperkingen om bijvoorbeeld te voorkomen dat lopende onderzoeken in gevaar worden gebracht. Artikel 14, lid 11, punt c), van het protocol biedt de lidstaten de basis om aan deze eis te voldoen.

Voor de verenigbaarheid van artikel 14, lid 1, van het protocol met de gegevensbeschermingsvoorschriften van de Unie is het tevens noodzakelijk dat de lidstaten, met betrekking tot mogelijke alternatieve manieren om de passende bescherming van uit hoofde van het protocol doorgegeven persoonsgegevens te waarborgen, de volgende overwegingen maken. Waar het gaat om andere internationale overeenkomsten die een alomvattend kader voor de bescherming van persoonsgegevens tussen de partijen tot stand brengen overeenkomstig hun toepasselijke rechtsvoorschriften, moeten de lidstaten er overeenkomstig artikel 14, lid 1, punt b), rekening mee houden dat, wat rechtstreekse samenwerking betreft, de raamovereenkomst tussen de EU en de VS moet worden aangevuld met extra waarborgen (in het kader van een specifieke doorgiftheregeling tussen de VS en de EU en haar lidstaten) die rekening houden met de bijzondere vereisten voor de rechtstreekse doorgifte van elektronisch bewijs door serviceproviders ten opzichte van de doorgifte door overheidsinstanties²⁵.

Voorts moeten de lidstaten overeenkomstig artikel 14, lid 1, punt b), van het protocol tevens in overweging nemen dat, voor EU-lidstaten die partij zijn bij Verdrag 108+, die overeenkomst op zich geen passende basis vormt voor grensoverschrijdende doorgifte van gegevens uit hoofde van het protocol naar andere partijen bij dat verdrag. In dit verband moeten zij rekening houden met de laatste zin van artikel 14, lid 1, van Verdrag 108+²⁶.

Tot slot moeten de lidstaten, wat andere overeenkomsten of regelingen uit hoofde van artikel 14, lid 1, punt c), betreft, in overweging nemen dat zij van dergelijke andere overeenkomsten of regelingen slechts gebruik mogen maken indien de Europese Commissie overeenkomstig artikel 45 van Verordening (EU) 2016/679 (algemene verordening gegevensbescherming) of artikel 36 van Richtlijn (EU) 2016/680 (gegevensbescherming bij

²⁴ Zie advies 1/15 van het Hof van Justitie (Grote kamer), ECLI:EU:C:2017:592, punt 220. Zie ook de bijdrage van de EDPB aan de raadpleging over een ontwerp van tweede aanvullend protocol bij het Verdrag van de Raad van Europa inzake cybercriminaliteit (Verdrag van Boedapest), 13 november 2019, blz. 6 (*De bevoegde nationale autoriteiten aan wie toegang tot de gegevens is verleend, moeten de betrokken personen volgens de toepasselijke nationale procedures daarvan in kennis stellen zodra die kennisgeving de door die autoriteiten verrichte onderzoeken niet langer in gevaar kan brengen. [...] Kennisgeving is noodzakelijk om de betrokken personen in staat te stellen onder meer hun recht op een voorziening in rechte en hun rechten inzake gegevensbescherming in verband met de verwerking van hun gegevens uit te oefenen*).

²⁵ Om deze reden is een aantal aanvullende waarborgen inzake gegevensbescherming opgenomen in de onderhandelingsrichtsnoeren die deel uitmaken van het besluit van de Raad van 21 mei 2019 houdende machtiging tot het openen van onderhandelingen met het oog op de sluiting van een overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika over grensoverschrijdende toegang tot elektronisch bewijsmateriaal voor justitiële samenwerking in strafzaken (document 9114/19). In de onderhandelingsrichtsnoeren wordt met name gesteld dat de overeenkomst de raamovereenkomst moet aanvullen met extra waarborgen die rekening houden met de gevoeligheidsgraad van de betrokken gegevenscategorieën en met de specifieke vereisten inzake de rechtstreekse doorgifte van elektronisch bewijsmateriaal door serviceproviders ten opzichte van de doorgifte door overheidsinstanties, en de rechtstreekse doorgifte door bevoegde autoriteiten aan serviceproviders.

²⁶ Zie ook de toelichting bij het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, 10 oktober 2018, punten 106-107.

rechtshandhaving) ten aanzien van het betreffende derde land een adequaatheidsbesluit heeft vastgesteld dat van toepassing is op de respectieve gegevensdoorgiften, of indien in die andere overeenkomst of regeling zelf passende gegevensbeschermingswaarborgen worden geboden overeenkomstig artikel 46 van de algemene verordening gegevensbescherming of artikel 37, lid 1, punt a), van de richtlijn gegevensbescherming bij rechtshandhaving.

Er moet niet alleen rekening worden gehouden met de huidige stand van het Unierecht op het betrokken gebied, maar ook met de ontwikkeling daarvan wanneer die ten tijde van de beoordeling voorspelbaar is. Het door het tweede aanvullend protocol bestreken gebied is rechtstreeks relevant voor de voorzienbare toekomstige ontwikkelingen van het Unierecht. In dit verband wordt gewezen op de voorstellen van de Commissie inzake grensoverschrijdende toegang tot elektronisch bewijsmateriaal van april 2018²⁷. Deze instrumenten hebben met name betrekking op de artikelen 6 en 7 van het protocol.

Bij de deelname aan de onderhandelingen namens de Unie heeft de Commissie erop toegezien dat het protocol volledig verenigbaar is met het Unierecht en de verplichtingen van de lidstaten uit hoofde daarvan. Meer bepaald heeft de Commissie erop toegezien dat de bepalingen van het protocol het mogelijk maken dat de lidstaten de grondrechten, de vrijheden en algemene beginselen van het Unierecht zoals die in de EU-Verdragen en het Handvest van de grondrechten zijn neergelegd, eerbiedigen, waaronder evenredigheid, procedurele rechten, het vermoeden van onschuld, en het recht op verdediging van personen tegen wie een strafprocedure loopt, alsmede het recht op eerbiediging van het privéleven, de bescherming van persoonsgegevens en elektronischecommunicatiegegevens wanneer dergelijke gegevens worden verwerkt, met inbegrip van de doorgifte daarvan aan rechtshandavingsinstanties in landen buiten de Europese Unie, en alle verplichtingen die in dat verband op rechtshandavingsinstanties en justitiële autoriteiten rusten. De Commissie heeft ook rekening gehouden met het advies van de Europese Toezichthouder voor gegevensbeschermingen²⁸ en het advies van het Europees Comité voor gegevensbescherming²⁹.

Voorts heeft de Commissie erop toegezien dat de bepalingen van het protocol en de voorstellen van de Commissie inzake elektronisch bewijsmateriaal met elkaar verenigbaar zijn – mede aangezien de ontwerpwetgeving tijdens de besprekingen met de medewetgevers is geëvolueerd – en dat het protocol geen aanleiding geeft tot wetsconflicten. De Commissie heeft er met name voor gezorgd dat in het protocol passende waarborgen inzake gegevensbescherming en privacy zijn opgenomen, waardoor serviceproviders uit de EU kunnen voldoen aan hun verplichtingen uit hoofde van de gegevensbeschermings- en privacywetgeving van de EU, voor zover het protocol een rechtsgrondslag biedt voor gegevensdoorgiften die plaatsvinden naar aanleiding van bevelen of verzoeken van een instantie van een niet-EU-partij bij het protocol aan een verwerkingsverantwoordelijke of een verwerker in de EU om persoonsgegevens of elektronischecommunicatiegegevens te verstrekken.

²⁷ COM(2018) 225 en 226 final.

²⁸ Advies van de EDPS over deelname aan de onderhandelingen inzake een tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit (advies 3/2019 van 2 april 2019).

²⁹ Met inbegrip van de bijdrage van de EDPB aan de raadpleging over een tweede aanvullend protocol bij het Verdrag van Boedapest van de Raad van Europa inzake cybercriminaliteit van 13 november 2019; Verklaring 02/201 inzake nieuwe ontwerpbepalingen van het tweede aanvullende protocol bij het Verdrag van de Raad van Europa inzake cybercriminaliteit (Verdrag van Boedapest), aangenomen op 2 februari 2021; Bijdrage van de EDPB aan de zesde overlegronde over het ontwerp van tweede aanvullend protocol bij het Verdrag van Boedapest van de Raad van Europa inzake cybercriminaliteit van 4 mei 2021.

2.4. Voorbehouden, verklaringen, kennisgevingen en mededelingen, en andere overwegingen

Het protocol biedt de partijen de mogelijkheid om met betrekking tot bepaalde artikelen voorbehouden te maken en verklaringen, kennisgevingen of mededelingen af te leggen. De lidstaten moeten een uniforme aanpak hanteren ten aanzien van bepaalde voorbehouden en verklaringen, kennisgevingen en mededelingen, zoals in de bijlage bij dit besluit aangegeven. Om te waarborgen dat de uitvoering van het protocol verenigbaar is met het Unierecht moeten de EU-lidstaten met betrekking tot die voorbehouden en verklaringen het hierna uiteengezette standpunt innemen. Wanneer het protocol een mogelijkheid biedt voor andere voorbehouden, verklaringen, kennisgevingen of mededelingen, machtigt dit voorstel de lidstaten om te overwegen hun eigen voorbehouden te maken en verklaringen, kennisgevingen of mededelingen af te leggen.

Teneinde de verenigbaarheid van de bepalingen van het protocol met het toepasselijke Unierecht en -beleid te waarborgen, mogen de lidstaten geen voorbehouden maken als bedoeld in artikel 7, lid 9, punt a)³⁰ of punt b)³¹. Bovendien moeten de lidstaten de verklaring bedoeld in artikel 7, lid 2, punt b)³², en de kennisgeving overeenkomstig artikel 7, lid 5, punt a)³³, doen uitgaan. Het achterwege laten van deze voorbehouden en het doen uitgaan van de bedoelde verklaring en kennisgeving is bovendien van belang om te waarborgen dat het protocol verenigbaar is met de wetgevingsvoorstellen van de Commissie inzake elektronisch bewijsmateriaal, onder meer in verband met de ontwikkeling van de besprekingen over de ontwerpwetgeving met de medewetgevers.

Om te zorgen voor een uniforme toepassing van het protocol door de EU-lidstaten in het kader van hun samenwerking met partijen die geen EU-lidstaat zijn, worden de lidstaten bovendien aangemoedigd geen voorbehoud te maken als bedoeld in artikel 8, lid 13³⁴, ook omdat een dergelijk voorbehoud wederkerige werking zou hebben³⁵. De lidstaten zouden de in artikel 8, lid 4, bedoelde verklaring moeten afleggen om ervoor te zorgen dat aan bevelen gevolg kan worden gegeven indien aanvullende ondersteunende informatie nodig is, bijvoorbeeld over de omstandigheden van de zaak in kwestie, teneinde de evenredigheid en noodzakelijkheid te kunnen beoordelen³⁶.

³⁰ Staat de partijen toe zich het recht voor te behouden om artikel 7 (Verstreking van abonnee-informatie) niet toe te passen.

³¹ Staat de partijen toe zich het recht voor te behouden om artikel 7 (Verstreking van abonnee-informatie) niet toe te passen op bepaalde soorten toegangsnummers indien dat onverenigbaar zou zijn met de grondbeginselen van hun nationale rechtstelsel.

³² Staat de partijen toe te verklaren dat het bevel uit hoofde van artikel 7 (Verstreking van abonnee-informatie), lid 1, moet worden uitgevaardigd door of onder toezicht van een aanklager of een andere justitiële instantie, of anderszins onder onafhankelijk toezicht moet worden uitgevaardigd.

³³ Staat een partij toe de secretaris-generaal van de Raad van Europa ervan in kennis te stellen dat wanneer uit hoofde van artikel 7 (Verstreking van abonnee-informatie), lid 1, een bevel wordt uitgevaardigd aan een serviceprovider op haar grondgebied, die partij in alle gevallen dan wel in bepaalde omstandigheden gelijktijdige kennisgeving verlangt van het bevel, de aanvullende informatie en een samenvatting van de feiten in verband met het onderzoek of de procedure.

³⁴ Staat partijen toe zich het recht voor te behouden om artikel 8 (Uitvoering geven aan bevelen van een andere partij) niet toe te passen op verkeersgegevens.

³⁵ Zie punt 147 van de toelichting bij het protocol, waarin wordt bepaald dat een partij die een voorbehoud maakt ten aanzien van dit artikel, andere partijen geen bevel mag geven tot verstrekking van verkeersgegevens overeenkomstig artikel 8, lid 1.

³⁶ Staat partijen toe te verklaren dat aanvullende ondersteunende informatie vereist is om gevolg te geven aan bevelen uit hoofde van artikel 8 (Uitvoering geven aan bevelen van een andere partij), lid 1.

De lidstaten worden ook aangemoedigd af te zien van het afleggen van de verklaring uit hoofde van artikel 9, lid 1, punt b)³⁷, teneinde de efficiënte toepassing van het protocol te waarborgen.

De lidstaten zouden de mededelingen bedoeld in artikel 7, lid 5, punt e)³⁸, artikel 8, lid 10, punten a) en b)³⁹, artikel 14, lid 7, punt c), en lid 10, punt b), moeten doen, teneinde een algeheel doeltreffende toepassing van het protocol te waarborgen⁴⁰.

Tot slot moeten de lidstaten ook de nodige maatregelen nemen overeenkomstig artikel 14, lid 11, punt c), om ervoor te zorgen dat de ontvangende partij bij de doorgifte in kennis wordt gesteld van de verplichting uit hoofde van het Unierecht om kennisgeving te doen aan de persoon op wie de gegevens betrekking hebben⁴¹, en passende contactgegevens verstrekken zodat de ontvangende partij de bevoegde autoriteit in de EU-lidstaat in kennis kan stellen zodra de vertrouwelijkheidsbeperkingen niet langer van kracht zijn en kennisgeving kan worden gedaan.

2.5. Motivering van het voorstel

Het protocol treedt in werking zodra vijf partijen hebben verklaard ermee in te stemmen door het protocol gebonden te zijn overeenkomstig artikel 16, leden 1 en 2. De ceremonie voor de ondertekening van het protocol zal naar verwachting in maart 2022 plaatsvinden.

De lidstaten van de EU moeten de nodige maatregelen nemen voor een snelle inwerkingtreding en ratificatie van het protocol, hetgeen om een aantal redenen van belang is.

Ten eerste zal het protocol ervoor zorgen dat de rechtshandhavingsinstanties en de justitiële autoriteiten beter zijn toegerust om elektronisch bewijsmateriaal te verkrijgen dat nodig is voor strafrechtelijke onderzoeken. Gezien het toenemende belang van elektronisch bewijsmateriaal voor strafrechtelijke onderzoeken is het dringend noodzakelijk dat de rechtshandhavingsinstanties en justitiële autoriteiten over de juiste instrumenten beschikken om op doeltreffende wijze toegang te krijgen tot elektronisch bewijsmateriaal, zodat zij onlinecriminaliteit doeltreffend kunnen bestrijden.

Ten tweede zal het protocol ervoor zorgen dat dergelijke maatregelen voor de toegang tot elektronisch bewijsmateriaal door de lidstaten zodanig worden toegepast dat de grondrechten kunnen worden geëerbiedigd, met inbegrip van procedurele rechten in strafzaken, het recht op privacy en het recht op bescherming van persoonsgegevens. Door het ontbreken van duidelijke regels op internationaal niveau kunnen bestaande praktische problemen opleveren

³⁷ Staat partijen toe te verklaren dat zij geen gevolg zullen geven aan verzoeken uit hoofde van artikel 9 (Spoedverstrekking van computergegevens in noodgevallen), lid 1, punt a), wanneer daarbij uitsluitend om verstrekking van abonneegegevens wordt verzocht.

³⁸ Staat een partij toe de contactgegevens mee te delen van de autoriteit die zij aanwijst voor het ontvangen van kennisgevingen uit hoofde van artikel 7, lid 5, punt a), en het verrichten van de in artikel 7 (Verstrekking van abonnee-informatie), lid 5, punten b), c) en d), beschreven handelingen.

³⁹ Staat partijen toe de contactgegevens mee te delen van de autoriteiten die zijn aangewezen voor het uitvaardigen en ontvangen van bevelen uit hoofde van artikel 8 (Uitvoering geven aan bevelen van een andere partij). Overeenkomstig de vereisten van Verordening (EU) 2017/1939 nemen de lidstaten die aan de nauwere samenwerking bij de instelling van het Europees Openbaar Ministerie (EOM) deelnemen, de contactgegevens van het EOM op in de mededeling.

⁴⁰ Staat partijen toe om informatie te verstrekken over de instantie of instanties die in kennis moet(en) worden gesteld bij een beveiligingsincident, of waarmee contact moet worden opgenomen om voorafgaande toestemming te vragen voor verdere doorgifte aan een andere staat of een internationale organisatie.

⁴¹ Zie voetnoot 24.

in verband met rechtszekerheid, transparantie, verantwoordingsplicht en eerbiediging van de grondrechten en procedurele waarborgen van verdachten in strafrechtelijke onderzoeken.

Door op internationaal vlak compatibele regels vast te stellen voor de grensoverschrijdende toegang tot elektronisch bewijsmateriaal zal het protocol ten derde een oplossing bieden voor wetsconflicten die gevolgen hebben voor overheden, serviceproviders uit de particuliere sector en andere entiteiten, en dergelijke conflicten voorkomen.

Ten vierde zal het protocol aantonen dat het verdrag nog steeds van belang is als het belangrijkste multilaterale kader voor de bestrijding van cybercriminaliteit. Dit zal van cruciaal belang zijn in het kader van het proces dat het gevolg is van resolutie 74/247 van de Algemene Vergadering van de Verenigde Naties van december 2019 over de bestrijding van het gebruik van informatie- en communicatietechnologieën voor criminele doeleinden, waarbij een open intergouvernementele ad-hoccommissie van deskundigen werd opgericht, met als opdracht een breed internationaal verdrag op te stellen ter bestrijding van het gebruik van informatie- en communicatietechnologieën voor criminele doeleinden.

3. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

- *Rechtsgrondslag*

De bevoegdheid van de Unie om wetgeving vast te stellen ter vergemakkelijking van de samenwerking tussen justitiële autoriteiten en gelijkwaardige instanties in verband met strafprocedures en de tenuitvoerlegging van beslissingen, is gebaseerd op artikel 82, lid 1, VWEU. De bevoegdheid van de Unie op het gebied van de bescherming van persoonsgegevens is gebaseerd op artikel 16 VWEU.

Op grond van artikel 3, lid 2, VWEU is de Unie exclusief bevoegd een internationale overeenkomst te sluiten wanneer die sluiting gemeenschappelijke regels van de EU kan aantasten of de strekking daarvan kan wijzigen. De bepalingen van het protocol behoren tot een gebied dat grotendeels onder de eerder in punt 2.3 uiteengezette gemeenschappelijke regels valt.

Het protocol valt derhalve onder de exclusieve externe bevoegdheid van de Unie. De ratificatie van het protocol door de lidstaten in het belang van de Unie kan derhalve plaatsvinden op basis van artikel 16, artikel 82, lid 1, en artikel 218, lid 6, VWEU.

- *Subsidiariteit (bij niet-exclusieve bevoegdheid)*

Niet van toepassing.

- *Evenredigheid*

De doelstellingen van de Unie met betrekking tot dit voorstel zijn uiteengezet in punt 2.5. Zij kunnen alleen worden verwezenlijkt door sluiting van een bindende internationale overeenkomst die voorziet in de nodige samenwerkingsmaatregelen en tegelijkertijd een passende bescherming van de grondrechten waarborgt. Met het protocol wordt dit doel bereikt. De bepalingen van het protocol zijn beperkt tot hetgeen nodig is om de belangrijkste doelstellingen ervan te verwezenlijken. Eenzijdige maatregelen zijn geen alternatief, aangezien die geen toereikende basis zouden vormen voor de samenwerking met niet-EU-landen en niet de noodzakelijke bescherming van de grondrechten zouden kunnen bieden. Ook is het sluiten van een multilaterale overeenkomst, zoals het protocol, die de Unie heeft kunnen uitonderhandelen, efficiënter dan het aangaan van onderhandelingen met afzonderlijke niet-EU-landen op bilateraal niveau. Ervan uitgaande dat alle 66 partijen, alsmede toekomstige nieuwe partijen bij het verdrag, het protocol zullen ratificeren, zal het

protocol een gemeenschappelijk rechtskader bieden voor de samenwerking van de EU-lidstaten met hun belangrijkste internationale partners in de strijd tegen criminaliteit.

- *Keuze van het instrument*

Niet van toepassing.

4. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- *Evaluatie van bestaande wetgeving en controle van de resultaatgerichtheid ervan*

Niet van toepassing.

- *Raadpleging van belanghebbenden*

De Raad van Europa heeft zes openbare raadplegingsronden over de onderhandelingen over het protocol georganiseerd, die plaats hebben gevonden in juli en november 2018, februari en november 2019, december 2020 en mei 2021⁴². De partijen hebben de daarbij ontvangen input in overweging genomen.

In haar rol van onderhandelaar namens de Unie heeft de Commissie ook van gedachten gewisseld met gegevensbeschermingsautoriteiten en heeft zij in 2019 en 2021 gerichte raadplegingsbijeenkomsten georganiseerd met maatschappelijke organisaties, serviceproviders en brancheverenigingen. De Commissie heeft rekening gehouden met de input die zij daarbij heeft gekregen.

- *Bijeenbrengen en gebruik van expertise*

Tijdens het onderhandelingsproces heeft de Commissie consequent het speciaal comité van de Raad voor de onderhandelingen geraadpleegd, overeenkomstig het besluit van de Raad van de Europese Unie van 6 juni 2019 houdende machtiging van de Commissie tot deelname, namens de Unie, aan de onderhandelingen, waarbij deskundigen uit de lidstaten de gelegenheid kregen om een bijdrage te leveren aan de formulering van het standpunt van de Unie. Een aantal deskundigen uit de lidstaten is ook aan de onderhandelingen blijven deelnemen, samen met de onderhandelaars van de Commissie namens de Unie. Ook zijn belanghebbenden geraadpleegd, zoals eerder vermeld.

- *Effectbeoordeling*

In 2017–2018 is een effectbeoordeling uitgevoerd in het kader van de voorstellen van de Commissie betreffende elektronisch bewijsmateriaal⁴³. In dit verband maakten de onderhandelingen over een tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit deel uit van de voorkeursoptie. De relevante effecten komen ook in deze toelichting aan de orde.

- *Resultaatgerichtheid en vereenvoudiging*

Het protocol kan implicaties hebben voor bepaalde categorieën serviceproviders, zoals kleine en middelgrote ondernemingen (kmo's), aangezien het protocol ertoe kan leiden dat zij verzoeken of bevelen krijgen om elektronisch bewijsmateriaal te verstrekken. Momenteel zullen deze aanbieders dergelijke verzoeken vaak al krijgen via de bestaande kanalen, soms

⁴² <https://www.coe.int/en/web/cybercrime/protocol-consultations>

⁴³ SWD(2018) 118 final.

via verschillende autoriteiten, onder meer op grond van het verdrag⁴⁴, op grond van andere verdragen inzake wederzijdse rechtshulp of in andere verbanden, zoals in het kader van het multistakeholderbeleid voor internetgovernance⁴⁵. Serviceproviders, met inbegrip van kleine en middelgrote ondernemingen, zullen baat hebben bij een duidelijk rechtskader op internationaal niveau en een gemeenschappelijke aanpak door alle partijen bij het protocol.

- *Grondrechten*

De samenwerkingsinstrumenten in het kader van het protocol zullen waarschijnlijk gevolgen hebben voor de grondrechten, waaronder het recht op een onpartijdig gerecht, het recht op privacy en het recht op bescherming van persoonsgegevens, namelijk wanneer in het kader van een strafprocedure mogelijk persoonsgegevens zijn verkregen. Het protocol gaat uit van een op rechten gebaseerde benadering en voorziet in voorwaarden en waarborgen die in overeenstemming zijn met de internationale mensenrechteninstrumenten, waaronder het Verdrag van de Raad van Europa tot bescherming van de rechten van de mens en de fundamentele vrijheden van 1950. Het protocol voorziet met name in specifieke waarborgen op het gebied van gegevensbescherming. Waar nodig biedt het protocol de partijen ook een basis om bepaalde voorbehouden te maken en verklaringen of kennisgevingen af te leggen, en bevat het gronden waarop medewerking aan een verzoek in specifieke situaties kan worden geweigerd. Dit waarborgt de verenigbaarheid van het protocol met het Handvest van de grondrechten van de EU.

5. GEVOLGEN VOOR DE BEGROTING

Het voorstel heeft geen gevolgen voor de begroting van de Unie. Het kan zijn dat lidstaten eenmalig kosten moeten maken voor de uitvoering van het protocol en mogelijk moeten de autoriteiten van de lidstaten hogere kosten maken als gevolg van de verwachte toename van het aantal zaken.

6. OVERIGE ELEMENTEN

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

Er is geen uitvoeringsplan vastgesteld, aangezien de lidstaten na de ondertekening en ratificatie verplicht zullen zijn het protocol ten uitvoer te leggen.

Wat monitoring betreft, zal de Commissie deelnemen aan de vergaderingen van de commissie Cybercrimeverdrag, waar de Europese Unie is erkend als waarnemende organisatie.

⁴⁴ Zie bijvoorbeeld Guidance Note 10 van de commissie Cybercrimeverdrag van 1 maart 2017 inzake verstrekkingen met betrekking tot abonnee-informatie (artikel 18 van het Verdrag van Boedapest).

⁴⁵ Zie bijvoorbeeld de resolutie van de raad van bestuur van de Internet Corporation for Assigned Names and Numbers (ICANN) van 15 mei 2019 over de aanbevelingen inzake de tijdelijke specificatie voor gTLD-registratiegegevens, beschikbaar op www.icann.org.

Voorstel voor een

BESLUIT VAN DE RAAD

houdende machtiging van de lidstaten om, in het belang van de Europese Unie, het tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, inzake nauwere samenwerking en verstrekking van elektronisch bewijsmateriaal te ratificeren

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 16, artikel 82, lid 1, en artikel 218, lid 6,

Gezien het voorstel van de Europese Commissie,

Gezien het advies van het Europees Parlement,

Overwegende hetgeen volgt:

- (1) De Raad heeft de Commissie op 9 juni 2019 gemachtigd om namens de Unie deel te nemen aan de onderhandelingen over een tweede aanvullend protocol bij het Verdrag van Boedapest van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken.
- (2) De tekst van het tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, inzake nauwere samenwerking en verstrekking van elektronisch bewijsmateriaal (hierna “het protocol” genoemd) is op 17 november 2021 door het Comité van Ministers van de Raad van Europa aangenomen en het protocol zal naar verwachting in maart 2022 voor ondertekening worden opengesteld.
- (3) De bepalingen van het protocol zijn van toepassing op een gebied dat voor een groot deel onder de gemeenschappelijke regels in de zin van artikel 3, lid 2, VWEU valt, met inbegrip van instrumenten ter vergemakkelijking van de justitiële samenwerking in strafzaken, die minimumnormen voor procedurele rechten waarborgen, alsmede gegevensbescherming en privacywaarborgen.
- (4) De Commissie heeft ook wetgevingsvoorstellen ingediend voor een verordening betreffende het Europees bevel tot verstrekking en het Europees bevel tot bewaring van elektronisch bewijsmateriaal in strafzaken (COM(2018) 225 final) en voor een richtlijn tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures (COM(2018) 226 final), waarmee bindende grensoverschrijdende Europese verstrekking- en bewaringsbevelen worden geïntroduceerd die rechtstreeks tot een vertegenwoordiger van een dienstverlener in een andere lidstaat zijn gericht.
- (5) Door namens de Unie aan de onderhandelingen deel te nemen, heeft de Commissie ervoor gezorgd dat het tweede aanvullend protocol verenigbaar is met de desbetreffende gemeenschappelijke regels van de Europese Unie.

- (6) Enkele voorbehouden, verklaringen, kennisgevingen en mededelingen zijn van belang voor de verenigbaarheid van het protocol met het recht en het beleid van de Unie, voor de eenvormige toepassing van het protocol door de EU-lidstaten in hun betrekkingen met partijen die geen lid zijn van de EU, en voor een doeltreffende toepassing van het protocol.
- (7) Doordat het protocol voorziet in snelle procedures ter verbetering van de grensoverschrijdende toegang tot elektronisch bewijsmateriaal en in krachtige waarborgen, zal de inwerkingtreding ervan bijdragen tot de strijd tegen cybercriminaliteit en andere vormen van criminaliteit op mondiaal niveau door facilitering van de samenwerking tussen de partijen bij het protocol die EU-lidstaat zijn en de partijen bij het protocol die geen EU-lidstaat zijn, een hoog niveau van bescherming van personen waarborgen en een oplossing bieden voor wetsconflicten.
- (8) Doordat het protocol voorziet in passende waarborgen die in overeenstemming zijn met de vereisten inzake internationale doorgifte van persoonsgegevens uit hoofde van Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680, zal de inwerkingtreding ervan bijdragen tot bevordering van de gegevensbeschermingsnormen van de Unie op mondiaal niveau, de gegevensstromen tussen de partijen bij het protocol die EU-lidstaat zijn en de partijen bij het protocol die geen EU-lidstaat zijn, vergemakkelijken en ervoor zorgen dat de EU-lidstaten hun verplichtingen uit hoofde van de gegevensbeschermingsvoorschriften van de Unie nakomen.
- (9) De positie van het Verdrag van Boedapest van de Raad van Europa als het belangrijkste multilaterale kader voor de bestrijding van cybercriminaliteit zal bovendien door een snelle inwerkingtreding worden bevestigd.
- (10) De Europese Unie kan geen partij worden bij het protocol, aangezien zowel het protocol als het Verdrag van de Raad van Europa inzake cybercriminaliteit alleen openstaat voor staten.
- (11) De lidstaten moeten daarom worden gemachtigd om, gezamenlijk handelend in het belang van de Europese Unie, het protocol te ratificeren.
- (12) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad en heeft op [...] advies uitgebracht.
- (13) [Overeenkomstig de artikelen 1 en 2 van Protocol nr. 21 betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, gehecht aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, en onverminderd artikel 4 van dat protocol, neemt Ierland niet deel aan de vaststelling van dit besluit en is dit niet bindend voor, noch van toepassing op deze lidstaat.]

[OF]

[Overeenkomstig de artikelen 1 en 2 van Protocol nr. 21 betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, gehecht aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, en onverminderd artikel 4 van dat protocol, heeft Ierland [, bij brief van ...] kennisgegeven van zijn wens om deel te nemen aan de vaststelling en toepassing van dit besluit.]

- (14) 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 dit besluit en is dit niet bindend voor, noch van toepassing op deze lidstaat,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

De lidstaten worden gemachtigd om, in het belang van de Europese Unie, het tweede aanvullend protocol bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, inzake nauwere samenwerking en verstrekking van elektronisch bewijsmateriaal (hierna “het protocol” genoemd) te ratificeren.

Artikel 2

De voorbehouden, verklaringen, kennisgevingen en mededelingen van de lidstaten bij de ratificatie van het protocol zijn in de bijlage opgenomen.

Artikel 3

Dit besluit treedt in werking op de datum waarop het wordt vastgesteld.

Artikel 4

Dit besluit wordt bekendgemaakt in het *Publicatieblad van de Europese Unie*.

Artikel 5

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel,

Voor de Raad
De voorzitter