



Brussel, 10.1.2017
COM(2017) 7 final

**MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE
RAAD**

Uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld

1. INLEIDING

De bescherming van persoonsgegevens behoort tot Europa's constitutionele structuur en is verankerd in artikel 8 van het Handvest van de grondrechten van de EU. Gegevensbescherming maakt al meer dan twintig jaar deel uit van het EU-recht, vanaf de gegevensbeschermingsrichtlijn van 1995¹ (hierna de "richtlijn van 1995" genoemd) tot de vaststelling van de algemene verordening gegevensbescherming² en de politieke richtlijn in 2016³.

Zoals voorzitter Juncker op 14 september 2016 heeft benadrukt in zijn rede over de toestand van de Europese Unie: *"Europeaan zijn betekent dat u recht heeft op de bescherming van uw persoonsgegevens door middel van krachtige Europese wetten. [...] Want privacy doet ertoe in Europa. Het is een kwestie van menselijke waardigheid."*

De behoefte aan bescherming van persoonsgegevens bestaat echter niet alleen in Europa. Wereldwijd hechten consumenten steeds sterker aan hun privacy. Bedrijven merken dan ook dat goede privacybescherming een concurrentievoordeel oplevert, aangezien het vertrouwen in hun dienstverlening erdoor groeit. Veel bedrijven, en met name bedrijven met een mondiaal bereik, brengen hun privacybeleid in overeenstemming met de algemene verordening gegevensbescherming, aangezien zij zaken in de EU willen doen en de richtlijn als een navolgenswaardig voorbeeld beschouwen.

Verscheidene landen en regionale organisaties buiten de EU, in onze nabuurschap, Azië, Latijns-Amerika en Afrika, stellen nieuwe gegevensbeschermingswetgeving vast of passen de bestaande wetgeving aan, om de kansen van de mondiale digitale economie te benutten en in te spelen op de groeiende vraag naar betere gegevensbeveiliging en privacybescherming. Hoewel er tussen landen verschillen bestaan wat betreft de wijze waarop en de mate waarin de wetgeving is ontwikkeld, zijn er – zeker in bepaalde delen van de wereld – aanwijzingen voor opwaartse convergentie in de richting van belangrijke gegevensbeschermingsbeginselen⁴. Grotere verenigbaarheid van verschillende gegevensbeschermingssystemen zou het internationale persoonsgegevensverkeer vergemakkelijken, zowel voor commerciële doeleinden als voor samenwerking tussen overheden (bv. met het oog op rechtshandhaving).

¹ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PB L 281 van 23.11.1995.

² Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), PB L 119 van 4.5.2016, blz. 1. Deze verordening is op 24 mei 2016 in werking getreden en wordt met ingang van 25 mei 2018 van toepassing.

³ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, PB L 119 van 4.5.2016, blz. 89. Deze richtlijn is op 5 mei 2016 in werking getreden en moet uiterlijk op 6 mei 2018 door de EU-lidstaten in nationale wetgeving worden omgezet.

⁴ Zie "Data protection regulations and international data flows: Implications for trade and development", UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

De EU zou deze mogelijkheid moeten benutten om haar gegevensbeschermingsbeginselen uit te dragen en gegevensstromen te vergemakkelijken door aan te sturen op convergentie van wettelijke systemen. Zoals is aangekondigd in het werkprogramma van de Commissie⁵, bevat de onderhavige mededeling derhalve het strategische kader van de Commissie voor adequaatheidsbesluiten en andere instrumenten voor gegevensdoorgiften en internationale gegevensbeschermingsinstrumenten.

2. HET EU-HERVORMINGSPAKKET VOOR GEGEVENSBECHERMING – EEN MODERN WETGEVINGSKADER DAT INTERNATIONALE GEGEVENSSTROMEN ONDERSTEUNT MET EEN HOOG BESCHERMINGSNIVEAU

De hervorming van de in april 2016 vastgestelde EU-gegevensbeschermingswetgeving omvat een systeem dat zowel een hoog beschermingsniveau waarborgt als openstaat voor de mogelijkheden van de mondiale informatiemaatschappij. Door de hervorming krijgen burgers meer controle over hun persoonsgegevens en neemt het consumentenvertrouwen in de digitale economie toe. Dankzij de harmonisering en vereenvoudiging van het rechtskader wordt het voor zowel binnenlandse als buitenlandse bedrijven gemakkelijker en minder belastend om – onder meer door middel van internationaal gegevensverkeer – zaken te doen in de EU. De EU combineert vandaag de dag openheid voor internationale gegevensstromen en het hoogste niveau van bescherming voor natuurlijke personen. De Unie heeft de potentie om uit te groeien tot een knooppunt voor gegevensdiensten waarvoor vrij gegevensverkeer en vertrouwen vereist zijn.

2.1 Een breed, uniform en vereenvoudigd EU-gegevensbeschermingskader

De EU-hervorming voorziet in een breed kader voor de verwerking van persoonsgegevens in zowel de particuliere als de publieke sector en in zowel de commerciële als de rechtshandavingssector (de algemene verordening gegevensbescherming respectievelijk de politieke richtlijn).

Krachtens de algemene verordening gegevensbescherming geldt er vanaf mei 2018 één pan-Europees pakket regels, dat in de plaats komt van de 28 nationale wetgevingen die nu van toepassing zijn. Dankzij het nieuwe één-loketmechanisme zal er één gegevensbeschermingsautoriteit verantwoordelijk zijn voor het toezicht op grensoverschrijdende gegevensverwerking door een onderneming in de EU. Er wordt gewaarborgd dat de nieuwe regels op coherente wijze worden uitgelegd. Met name in grensoverschrijdende gevallen waarbij meerdere nationale gegevensbeschermingsautoriteiten betrokken zijn, zal er één besluit worden genomen om te waarborgen dat gemeenschappelijke problemen op dezelfde manier worden opgelost. Bovendien creëert de algemene verordening gegevensbescherming een gelijk speelveld voor ondernemingen uit de EU en ondernemingen uit derde landen die in de EU goederen en diensten aanbieden of het gedrag van natuurlijke personen monitoren. Groter consumentenvertrouwen komt marktdeelnemers van binnen en buiten de EU ten goede.

⁵ Werkprogramma van de Commissie voor 2017, Naar een Europa dat ons beschermt, sterker maakt en verdedigt, COM(2016) 710 final, 25.10.2016, blz.12 en bijlage 1.

De politieke richtlijn voorziet in gemeenschappelijke regels voor de verwerking van persoonsgegevens van personen die betrokken zijn bij een strafrechtelijke procedure, ongeacht of zij beschuldigde, getuige of slachtoffer zijn, met inachtneming van de specifieke aard van de politieke en strafrechtelijke sectoren. De harmonisering van gegevensbeschermingsregels in de rechtshandavingssector, met inbegrip van regels inzake internationale doorgiften, zal grensoverschrijdende samenwerking tussen politieke en justitiële autoriteiten vergemakkelijken, zowel binnen de EU als met internationale partners, en zo de voorwaarden voor een doeltreffender bestrijding van criminaliteit scheppen. Dit is een belangrijke bijdrage aan de Europese veiligheidsagenda⁶.

2.2 Een vernieuwd en ruimer instrumentarium voor internationale doorgiften

De EU-wetgeving inzake gegevensbescherming voorziet van oudsher in verschillende mechanismen voor gegevensdoorgifte. Het primaire doel van deze regels is te waarborgen dat de persoonsgegevens van Europeanen ook bij doorgifte naar het buitenland beschermd blijven. Door de jaren heen zijn deze regels in vele jurisdicties normatief geworden voor internationale gegevensstromen. Hoewel de architectuur wezenlijk dezelfde blijft als die op grond van de richtlijn van 1995, verheldert en vereenvoudigt de hervorming van de regels inzake internationale doorgiften de toepassing van die regels en voorziet ze in nieuwe instrumenten voor doorgiften.

Volgens het EU-recht is doorgifte van persoonsgegevens naar het buitenland onder meer mogelijk op grond van een adequaatheidsbesluit van de Commissie, waarbij wordt vastgesteld dat een niet-EU-land een gegevensbeschermingsniveau biedt dat "in wezen overeenkomt"⁷ met dat in de Unie. Een dergelijk besluit maakt vrij verkeer van persoonsgegevens naar dat derde land mogelijk zonder dat degene die de gegevens naar het buitenland doorgeeft, verdere waarborgen hoeft te verschaffen of toestemming hoeft te verkrijgen. Een precies en uitvoerig overzicht van de elementen waarmee de Commissie bij het beoordelen van het door een buitenlands systeem geboden bescherming rekening moet houden, is beschikbaar voor belanghebbende landen of internationale organisaties⁸. De Commissie kan nu ook adequaatheidsbesluiten nemen voor de rechtshandavingssector⁹. Voortbouwend op een op de

⁶ Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, "De Europese veiligheidsagenda", COM(2015) 185 final van 28.4.2015.

⁷ Arrest van het Hof van Justitie van de EU van 6 oktober 2015 in zaak C-362/14, *Maximilian Schrems tegen Data Protection Commissioner*, punten 73, 74 en 96. Zie ook overweging 104 van de algemene verordening gegevensbescherming en overweging 67 van de politieke richtlijn, waarin wordt verwezen naar de norm van wezenlijke overeenkomst.

⁸ Zie artikel 45 van de algemene verordening gegevensbescherming. Volgens artikel 45, lid 2, moet de Commissie bij haar beoordeling onder meer rekening houden met de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden en de toepasselijke wetgeving, onder meer inzake gegevensbescherming, openbare veiligheid, defensie, nationale veiligheid en strafrecht en de toegang van overheidsinstanties tot persoonsgegevens. Deze aspecten moeten worden ondersteund door doeltreffende en afdwingbare rechten, waaronder administratief beroep of beroep in rechte voor natuurlijke personen, en een doeltreffende onafhankelijke toezichthoudende autoriteit, teneinde naleving van de gegevensbeschermingsregels te waarborgen en te handhaven. Ook zal er rekening worden gehouden met de naleving van juridisch bindende overeenkomsten, met name Verdrag 108 van de Raad van Europa, en medewerking aan multilaterale of regionale regelingen voor gegevensbescherming.

⁹ Zie artikel 36, lid 2, van de politieke richtlijn voor de specifieke aspecten van een adequaatheidsbeoordeling.

richtlijn van 1995 gebaseerde praktijk voorziet de hervorming uitdrukkelijk in de mogelijkheid om de adequaatheid te bepalen inzake een bepaald grondgebied van een derde land of inzake een specifieke sector of bedrijfstak van een derde land (zogenoeten "gedeeltelijke" adequaatheid)¹⁰.

Als er geen adequaatheidsbesluit voorhanden is, kunnen internationale doorgiften plaatsvinden op basis van een aantal alternatieve doorgifte-instrumenten die passende gegevensbeschermingswaarborgen bieden¹¹. Bij de hervorming wordt de mogelijkheid om gebruik te maken van bestaande instrumenten als modelcontractbepalingen¹² en bindende bedrijfsvoorschriften¹³, geformaliseerd en verruimd. Zo kunnen modelcontractbepalingen nu worden opgenomen in een overeenkomst tussen in de EU gevestigde verwerkers en in een niet-EU-land gevestigde verwerkers¹⁴. Bindende bedrijfsvoorschriften, die vooralsnog beperkt waren tot regelingen tussen entiteiten van dezelfde vennootschapsgroep, kunnen nu ook worden gebruikt door een groep ondernemingen die wel betrokken zijn bij een gezamenlijke economische activiteit, maar niet noodzakelijkerwijs deel uitmaken van dezelfde vennootschap¹⁵. De hervorming vermindert ook de administratieve rompslomp door algemene voorschriften af te schaffen inzake voorafgaande melding aan en toestemming van gegevensbeschermingsautoriteiten met betrekking tot doorgiften naar een derde land op basis van modelcontractbepalingen en bindende bedrijfsvoorschriften¹⁶. Het betreft een belangrijke vereenvoudiging van het EU-systeem van internationale gegevensdoorgifte, aangezien het bestaan van dergelijke voorschriften, die momenteel van lidstaat tot lidstaat verschillen, dikwijls als een fors obstakel voor gegevensstromen wordt beschouwd, met name voor kleinere ondernemingen¹⁷.

Daarnaast worden bij de hervorming nieuwe instrumenten voor internationale doorgiften ingevoerd¹⁸. Verwerkingsverantwoordelijken en verwerkers zullen, onder bepaalde voorwaarden¹⁹, gebruik kunnen maken van goedgekeurde gedragscodes of

¹⁰ Zie artikel 45, lid 1, van de algemene verordening gegevensbescherming en artikel 36, lid 1, van de politieke richtlijn.

¹¹ Zie bv. Mededeling van de Commissie aan het Europees Parlement en de Raad over de doorgifte van persoonsgegevens van de EU naar de Verenigde Staten van Amerika krachtens Richtlijn 95/46/EG naar aanleiding van het arrest van het Hof van Justitie in zaak C-362/14 (*Schrems*), COM(2015) 566 final, 6.11.2015.

¹² Modelcontractbepalingen bevatten de respectieve gegevensbeschermingsverplichtingen tussen de EU-exporteur en de importeur in een derde land.

¹³ Bindende bedrijfsvoorschriften zijn interne regels die zijn vastgesteld door een multinationale groep ondernemingen voor de doorgifte van gegevens binnen dezelfde vennootschapsgroep naar entiteiten die gevestigd zijn in landen waar geen passend beschermingsniveau is. Hoewel bindende bedrijfsvoorschriften al in gebruik zijn op grond van de richtlijn van 1995, wordt de rol ervan als instrument voor doorgiften bij de algemene verordening gegevensbescherming gecodificeerd en geformaliseerd.

¹⁴ Zie artikel 46, lid 2, onder c) en d), en overweging 168 van de algemene verordening gegevensbescherming.

¹⁵ Zie artikel 46, lid 2, onder b), artikel 47 en overweging 110 van de algemene verordening gegevensbescherming.

¹⁶ Zie artikel 46, lid 2, van de algemene verordening gegevensbescherming.

¹⁷ Dat vergunningsvereisten voor menige onderneming, en met name voor kmo's, een handelsbarrière vormen, is onder meer benadrukt in het UNCTAD-verslag, blz. 34.

¹⁸ Zie artikel 46, lid 2, onder e) en f), van de algemene verordening gegevensbescherming.

¹⁹ Verwerkingsverantwoordelijken buiten de EU zullen zich kunnen houden aan een EU-gedragscode of -certificeringsmechanisme door via contractuele of andere juridisch bindende instrumenten bindende en afdwingbare toezeggingen te doen om de in die instrumenten vervatte waarborgen inzake

certificeringsmechanismen (zoals privacyzegels of -keurmerken) om in "passende waarborgen" te voorzien. Dit zou het mogelijk moeten maken om meer maatoplossingen voor internationale doorgifte te ontwikkelen en bijvoorbeeld rekening te houden met de specifieke kenmerken en behoeften van een bepaalde sector of bedrijfstak, of specifieke gegevensstromen. Ook biedt het de mogelijkheid om voor passende waarborgen te zorgen voor gegevensdoorgiften tussen overheidsinstanties of openbare organen op basis van internationale overeenkomsten of administratieve regelingen²⁰. Ten slotte wordt in de algemene verordening gegevensbescherming het gebruik verduidelijkt van zogeheten afwijkingen²¹ (zoals toestemming, uitvoering van een overeenkomst of gewichtige redenen van algemeen belang) waarop entiteiten in specifieke situaties hun gegevensdoorgifte kunnen baseren bij ontstentenis van een adequaatheidsbesluit en ongeacht het gebruik van een van de voornoemde instrumenten. Met name bevat deze verordening, zij het in omschreven vorm, een nieuwe afwijking voor doorgiften die in het gerechtvaardigde belang²² van een onderneming kunnen plaatsvinden.

Ten slotte houdt de hervorming in dat de Commissie de bevoegdheid krijgt internationale samenwerkingsmechanismen te ontwikkelen om de handhaving van gegevensbeschermingsregels te vergemakkelijken, onder meer door middel van regelingen voor wederzijdse bijstand²³. Nauwere vormen van internationale samenwerking tussen toezichthoudende autoriteiten zouden namelijk kunnen bijdragen tot een doeltreffender bescherming van afzonderlijke rechten en tot meer rechtszekerheid voor bedrijven.

3. INTERNATIONALE GEGEVENSDOORGIFTE IN DE COMMERCIËLE SECTOR: HANDEL BEVORDEREN DOOR PRIVACY TE BESCHERMEN

Eerbiediging van privacy is een voorwaarde voor stabiele, veilige en concurrerende wereldwijde handelsstromen. Privacy is geen handelswaar²⁴. Internet en digitalisering van goederen en diensten hebben de wereldeconomie ingrijpend veranderd en grensoverschrijdende doorgifte van gegevens, waaronder persoonsgegevens, maakt deel uit van de dagelijkse activiteiten van Europese ondernemingen, groot en klein en in alle sectoren. Aangezien handelsverkeer in toenemende mate afhankelijk is van het verkeer van persoonsgegevens, zijn de privacy en de beveiliging van dergelijke gegevens van cruciaal belang geworden voor consumentenvertrouwen. Zo baart het twee derde van de bevroegde Europeanen zorgen dat zij geen controle hebben over de informatie die zij online verstrekken, en is de helft van de respondenten beducht voor fraude²⁵. Tegelijkertijd krijgen Europese ondernemingen die in bepaalde derde landen actief zijn, steeds vaker te maken met

gegevensbescherming toe te passen. Zie artikel 42, lid 2, van de algemene verordening gegevensbescherming.

²⁰ Zie artikel 46, lid 2, onder a), en artikel 46, lid 3, onder b), van de algemene verordening gegevensbescherming.

²¹ Zie artikel 49 van de algemene verordening gegevensbescherming.

²² Artikel 49, lid 1, tweede alinea.

²³ Zie artikel 50 van de algemene verordening gegevensbescherming.

²⁴ Zie bv. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, "Handel voor iedereen – Naar een meer verantwoord handels- en investeringsbeleid", COM(2015) 497 final van 14.10.2015, blz. 7.

²⁵ Speciale Eurobarometer 431 – Gegevensbescherming, juni 2015.

protectionistische maatregelen die niet worden gewettigd door gerechtvaardigde privacyoverwegingen.

In het digitale tijdperk moeten het bevorderen van hoge gegevensbeschermingsnormen en het stimuleren van internationale handel hand in hand gaan. Over de bescherming van persoonsgegevens kan bij handelsovereenkomsten niet worden onderhandeld²⁶, maar de reeds beschreven EU-regels inzake internationale gegevensdoorgifte voorzien in een ruim instrumentarium dat zowel gegevensverkeer in verschillende situaties mogelijk maakt als een hoge mate van bescherming waarborgt.

3.1 Adequaateitsbesluiten

Een adequaateitsbesluit maakt de weg vrij voor vrij verkeer van persoonsgegevens vanuit de EU, zonder dat de EU-gegevensexporteur voor aanvullende waarborgen hoeft te zorgen of aan nadere voorwaarden hoeft te voldoen. De constatering dat de betrokken rechtsorde een passend beschermingsniveau waarborgt, houdt in dat het stelsel van het land sterk lijkt op dat van de EU-lidstaten. Doorgifte naar het land in kwestie wordt dan ook gelijkgesteld aan doorgifte van gegevens binnen de EU, hetgeen bevoorrechte toegang tot de interne markt van de EU meebrengt en handelsmogelijkheden ontsluit voor EU-marktdeelnemers. Zoals reeds is uitgelegd, is voor deze erkenning een beschermingsniveau vereist dat vergelijkbaar is (of "in wezen overeenkomt")²⁷ met het niveau dat in de Unie wordt gewaarborgd. Het veronderstelt een brede beoordeling van het systeem van het derde land, met inbegrip van de regels inzake toegang tot persoonsgegevens door de overheidsinstanties met het oog op rechtshandhaving, de nationale veiligheid en andere doelstellingen van openbaar belang.

Er kan echter ook sprake zijn van adequaateit zonder dat de EU-regels integraal worden overgenomen, zoals het Hof van Justitie in 2015 in zijn *Schrems*-arrest heeft vastgesteld²⁸. Het gaat er veeleer om of het betreffende buitenlandse systeem als geheel het vereiste hoge beschermingsniveau biedt, door de invulling van het recht op privacy, de doeltreffende toepassing en afdwingbaarheid daarvan en het toezicht dat wordt uitgeoefend. Zoals blijkt uit de adequaateitsbesluiten die tot dusver zijn vastgesteld, kan de Commissie zeer diverse privacysystemen, die verschillende rechtstradities weerspiegelen, als adequaat aanmerken. Deze besluiten betreffen landen die een nauwe band hebben met de Europese Unie en haar lidstaten (Zwitserland, Andorra, Faeröer, Guernsey, Jersey, Isle of Man), belangrijke handelspartners (Argentinië, Canada, Israël, Verenigde Staten) en landen die in hun regio vooroplopen bij het ontwikkelen van gegevensbeschermingswetgeving (Nieuw-Zeeland, Uruguay).

Bij de besluiten inzake Canada en de Verenigde Staten gaat het om "gedeeltelijke" adequaateit. Het besluit inzake Canada is alleen van toepassing op particuliere entiteiten die onder de Canadese *Personal Information Protection and Electronic Documents Act* vallen.

²⁶ Politieke beleidslijnen van voorzitter Juncker: *Een nieuwe start voor Europa: mijn agenda voor banen, groei, billijkheid en democratische verandering*.

²⁷ Zie voetnoot 7.

²⁸ Vgl. punt 74 van het *Schrems*-arrest.

Het onlangs vastgestelde besluit met betrekking tot het EU-VS-privacyschild²⁹ is een specifiek geval, dat – bij ontstentenis van algemene gegevensbeschermingswetgeving in de VS³⁰ – berust op toezeggingen van deelnemende ondernemingen om de hoge gegevensbeschermingsnormen te zullen toepassen die in deze regeling zijn vervat en die afdwingbaar zijn op grond van het recht van de VS. Voorts is het privacyschild gebaseerd op de specifieke verklaringen en garanties van de overheid van de VS met betrekking tot de toegang ten behoeve van de nationale veiligheid³¹, die ten grondslag liggen aan de vaststelling van adequaatheid. De Commissie zal er nauwlettend op toezien dat deze toezeggingen worden nagekomen, onder meer bij de jaarlijkse beoordeling van de werking van het kader.

Wereldwijd hebben de laatste jaren steeds meer landen nieuwe wetgeving op het gebied van gegevensbescherming en privacy vastgesteld of voorbereid. In 2015 hadden 109 landen gegevensbeschermingswetgeving vastgesteld; beduidend meer dan de 76 die medio 2011 over dit soort wetgeving beschikten³². Daarnaast zijn circa 35 landen momenteel gegevensbeschermingswetgeving aan het opstellen³³. Deze nieuwe of gemoderniseerde wetten zijn in de regel gebaseerd op een aantal centrale gemeenschappelijke beginselen, zoals de erkenning van gegevensbescherming als een grondrecht, de vaststelling van overkoepelende wetgeving op dit terrein, het bestaan van afdwingbare individuele privacyrechten, en de instelling van een onafhankelijke toezichthoudende autoriteit. Dit biedt nieuwe mogelijkheden om, met name door middel van adequaatheidsvaststellingen, het gegevensverkeer verder te bevorderen en tegelijkertijd te waarborgen dat de bescherming van persoonsgegevens op een hoog niveau blijft.

Volgens het EU-recht is voor een adequaatheidsvaststelling het bestaan vereist van gegevensbeschermingsregels die vergelijkbaar zijn met die in de EU³⁴. Het gaat zowel om materiële beschermingsvoorschriften voor persoonsgegevens als om de relevante toezichts- en verhaalsmechanismen die in het derde land beschikbaar zijn.

²⁹ Uitvoeringsbesluit (EU) 2016/1250 van de Commissie of 12 juli 2016.

³⁰ De Commissie moedigt de VS aan om inspanningen te blijven leveren om tot een breed systeem voor privacy- en gegevensbescherming te komen, zodat de twee systemen op de langere termijn kunnen convergeren. Zie Mededeling van de Commissie aan het Europees Parlement en de Raad "Trans-Atlantische gegevensstromen: herstel van vertrouwen door solide waarborgen", COM(2016) 117 final van 29.2.2016.

³¹ Dit omvat met name de toepassing van *Presidential Policy Directive 28* (PPD-28), waarbij een aantal beperkingen en waarborgen voor operaties betreffende signaalinlichtingen worden ingesteld, en de aanstelling van een specifieke ombudsman voor klachten hieromtrent van EU-burgers.

³² G. Greenleaf, "Global data privacy laws 2015: 109 countries, with European laws now in a minority", (2015) 133 *Privacy Laws & Business International Report*, 14-17.

³³ UNCTAD-studie, blz. 8 en 42 (voetnoot 4 hierboven).

³⁴ In dit opzicht houdt de Commissie bij het beoordelen van de adequaatheid ook rekening met de verplichtingen van het derde land die voortvloeien uit juridisch bindende verdragen, met name de toetreding tot Verdrag 108 en het bijbehorende Aanvullend Protocol. Zie artikel 45, lid 2, onder c), en overweging 105 van de algemene verordening gegevensbescherming.

Op grond van haar kader voor adequaatheidsvaststellingen is de Commissie van oordeel dat de volgende criteria in aanmerking moeten worden genomen bij de afweging met welke derde landen een dialoog over adequaatheid dient te worden gevoerd³⁵:

- (i) het belang van de (huidige of potentiële) handelsbetrekkingen van de EU met een bepaald derde land, met inbegrip van de vraag of er een vrijhandelsovereenkomst is dan wel onderhandelingen gaande zijn;
- (ii) de omvang van het persoonsgegevensverkeer vanuit de EU, als gevolg van de geografische ligging en/of culturele banden;
- (iii) de baanbrekende rol die het derde land op het gebied van privacy- en gegevensbescherming speelt en die andere landen in dezelfde regio tot voorbeeld zou kunnen strekken³⁶; en
- (iv) de algehele politieke verhouding met het betrokken derde land, met name wat betreft de bevordering van gemeenschappelijke waarden en gedeelde doelstellingen op internationaal niveau.

Op basis van deze overwegingen zal de Commissie actief overleggen met belangrijke handelspartners in Oost- en Zuidoost-Azië; eerst met Japan en Korea in 2017³⁷ en vervolgens, afhankelijk van de voortgang bij de modernisering van de gegevensbeschermingswetgeving, met India, maar ook met landen in Latijns-Amerika, met name Mercosur, en de Europese nabuurschap, die belangstelling hebben getoond voor een adequaatheidsvaststelling. Daarnaast kijkt de Commissie ook uit naar blijken van belangstelling van andere derde landen die bereid zijn om te overleggen over deze kwesties. Besprekingen over een mogelijke adequaatheidsvaststelling zijn een dialoog waarbij de EU-gegevensbeschermingsvoorschriften zo nodig worden verduidelijkt en wordt onderzocht hoe de convergentie van de wetgeving en praktijk van het derde land kan worden versterkt.

In bepaalde situaties kan het passender zijn om geen nationale benadering te volgen, maar andere opties te benutten, zoals gedeeltelijke adequaatheid of sectorspecifieke adequaatheid (bv. voor financiële dienstverlening of IT), voor geografische gebieden of bedrijfstakken die een belangrijk deel uitmaken van de economie van een derde land. Daarbij moet onder meer rekening worden gehouden met elementen als de aard en stand van de ontwikkeling van de privacyregelgeving (op zichzelf staande wetgeving, meerdere of sectorale wetten enz.), de constitutionele structuur van het derde land en de vraag of het gegevensverkeer vanuit de EU geconcentreerd is in bepaalde economische sectoren.

³⁵ Voor landen die van belang zijn voor samenwerking op het gebied van interne veiligheid en rechtshandhaving, zal de Commissie onderzoeken of specifieke adequaatheidsvaststellingen mogelijk zijn op grond van de politieke richtlijn (zie deel 4).

³⁶ Dit kan met name relevant zijn voor ontwikkelings- en overgangslanden, aangezien de bescherming van persoonsgegevens zowel een essentieel element van de rechtsstaat is als een belangrijke factor voor economisch concurrentievermogen.

³⁷ Japan en Korea hebben onlangs hun wetgeving vastgesteld of gemoderniseerd en daarbij brede gegevensbeschermingsregelingen ingevoerd.

Voor de vaststelling van een adequaathheidsbesluit zijn een specifieke dialoog en nauwe samenwerking met het betrokken derde land nodig. Adequaathheidsbesluiten zijn "levende" documenten, waarop de Commissie scherp toezicht moet houden en die moeten worden aangepast als zich ontwikkelingen voordoen met gevolgen voor het beschermingsniveau dat het betrokken derde land waarborgt³⁸. Daartoe zullen periodieke toetsingen worden verricht, minstens om de vier jaar, om in te spelen op nieuwe kwesties en om in het kader van een hecht partnerschap goede praktijken uit te wisselen³⁹. Deze dynamische aanpak is ook van toepassing op de bestaande, op grond van de richtlijn van 1995 vastgestelde adequaathheidsbesluiten, die zullen moeten worden herzien ingeval zij niet meer aan de toepasselijke norm voldoen⁴⁰. De betrokken derde landen wordt derhalve verzocht om de Commissie in kennis te stellen van elke relevante verandering in wetgeving en praktijk die heeft plaatsgevonden sinds de vaststelling van het adequaathheidsbesluit dat op hen ziet. Dit is van belang voor het waarborgen van de continuïteit van deze besluiten wanneer de nieuwe regels van de hervorming van toepassing zijn⁴¹.

Over de EU-gegevensbeschermingsregels kan niet worden onderhandeld met het oog op een vrijhandelsovereenkomst⁴². Hoewel het overleg over gegevensbescherming los moet staan van handelsbesprekingen met derde landen, is een adequaathheidsbesluit – ook in zijn gedeeltelijke of sectorspecifieke variant – het beste middel om wederzijds vertrouwen op te bouwen. Door vrij verkeer van persoonsgegevens te waarborgen, bevordert een dergelijk besluit het handelsverkeer waarbij doorgifte van persoonsgegevens naar het betrokken derde land plaatsvindt. Dergelijke besluiten kunnen handelsbesprekingen dan ook vergemakkelijken of bestaande handelsovereenkomsten aanvullen, waardoor de voordelen daarvan nog kunnen toenemen. Door de convergentie van het niveau van bescherming in de EU en het derde land te bevorderen, beperkt een adequaathheidsvaststelling tegelijkertijd het risico dat het land in kwestie de bescherming van persoonsgegevens aanvoert om ongerechtvaardigde vereisten inzake gegevenslokalisatie of -opslag op te leggen. Zoals is uiteengezet in de mededeling "Handel voor iedereen", zal de Commissie bovendien trachten gebruik te maken van EU-vrijhandelsovereenkomsten om regels op te stellen voor e-handel en grensoverschrijdende gegevensstromen en om nieuwe vormen van digitaal protectionisme te bestrijden, volledig in

³⁸ Krachtens artikel 45, leden 4 en 5, van de algemene verordening gegevensbescherming dient de Commissie doorlopend toezicht op ontwikkelingen in derde landen te houden en is zij bevoegd tot intrekking, wijziging of schorsing van een adequaathheidsbesluit over te gaan als zij vaststelt dat het betrokken land niet langer een passend beschermingsniveau waarborgt.

³⁹ Artikel 45, lid 3, van de algemene verordening gegevensbescherming.

⁴⁰ Artikel 97, lid 2, onder a), van de algemene verordening gegevensbescherming bepaalt ook dat de Commissie een evaluatieverslag uiterlijk in 2020 moet indienen bij het Europees Parlement en de Raad.

⁴¹ Om consequenties te verbinden aan het *Schrems*-arrest, waarbij werd vastgesteld dat de Commissie haar bevoegdheden had overschreden door in het veiligheidsbesluit de bevoegdheden van de gegevensbeschermingsautoriteiten om gegevensstromen op te schorten of te verbieden, te beperken, stelde de Commissie op 16 december 2016 een corrigerend "omnibus"-besluit vast, waarbij soortgelijke bepalingen in bestaande adequaathheidsbesluiten worden geschrapt en vervangen door bepalingen die louter voorzien in informatievoorschriften tussen de lidstaten en de Commissie ingeval een gegevensbeschermingsautoriteit doorgiften naar een derde land opschort of verbiedt. Verder wordt de Commissie bij het omnibusbesluit verplicht om de relevante ontwikkelingen in het derde land te volgen. Zie PB L 344 van 17.12.2016, blz. 83.

⁴² Een adequaathheidsvaststelling is met name een unilateraal uitvoeringsbesluit dat de Commissie neemt overeenkomstig het EU-recht inzake gegevensbescherming, op basis van de daarin vervatte criteria.

overeenstemming met en onverminderd de EU-wetgeving op het gebied van gegevensbescherming⁴³.

De Commissie zal:

- voorrang geven aan besprekingen over mogelijke adequaatheidsbesluiten met belangrijke handelspartners in Oost- en Zuidoost-Azië, eerst met Japan en Korea in 2017, maar ook andere strategische partners, zoals India, in aanmerking nemen, evenals landen in Latijns-Amerika, met name Mercosur, en de Europese nabuurschap.
- de werking van de bestaande adequaatheidsbesluiten nauwlettend volgen. Daarbij gaat het in het bijzonder om de tenuitvoerlegging van het EU-VS-privacyschild, die met name wordt gecontroleerd via het mechanisme voor jaarlijkse gezamenlijke toetsing.
- samenwerken met en bijstand verlenen aan landen die belangstelling hebben voor strenge gegevensbeschermingswetgeving en de convergentie daarvan met de EU-beginselen inzake gegevensbescherming ondersteunen.

3.2 Alternatieve mechanismen voor gegevensdoorgifte

In de EU-wetgeving inzake gegevensbeschermingsregels is altijd onderkend dat er niet één uniforme aanpak is die geschikt is voor alle vormen van internationale gegevensdoorgifte. Dit geldt nog sterker voor de regels die voortvloeien uit de hervorming. Hoewel adequaatheidsvaststellingen enkel beschikbaar zullen zijn voor de derde landen die voldoen aan de relevante criteria, voorziet de algemene verordening gegevensbescherming in diverse mechanismen die flexibel genoeg zijn om in te spelen op zeer uiteenlopende vormen van doorgifte. Er kunnen instrumenten worden ontwikkeld om de bijzondere behoeften of voorwaarden van specifieke bedrijfstakken, bedrijfsmodellen en/of marktdeelnemers in aanmerking te nemen. Daarbij kan het bijvoorbeeld gaan om modelcontractbepalingen die gericht zijn op de behoeften van een bepaalde sector, zoals specifieke waarborgen voor de verwerking van gevoelige gegevens in de zorgsector, of om een specifieke verwerkingsactiviteit die vooral gangbaar is in bepaalde derde landen, zoals uitbestede diensten die worden verricht voor Europese ondernemingen. Dit zou kunnen worden gedaan door ofwel nieuwe modelbepalingen vast te stellen of de bestaande bepalingen aan te vullen met extra waarborgen in de vorm van bv. technische dan wel organisatorische maatregelen of oplossingen die verband houden met het bedrijfsmodel⁴⁴. In bepaalde specifieke sectorale behoeften kan ook worden voorzien door middel van bindende bedrijfsvoorschriften voor groepen ondernemingen die gezamenlijk een economische activiteit uitoefenen, bv. in de reissector. De ontwikkeling van verwerker-naar-verwerker-modelbepalingen en/of bindende bedrijfsvoorschriften voor verwerkers zou ten goede kunnen komen aan de internationale doorgiften tussen verwerkers. Ten slotte bieden nieuwe doorgiftemechanismen zoals

⁴³ Zie mededeling "Handel voor iedereen", blz. 12 (voetnoot 24 hierboven).

⁴⁴ Zie artikel 46, lid 2, onder c) en d), en overweging 109 van de algemene verordening gegevensbescherming, waarin wordt uitgelegd dat aanpassingen van goedgekeurde standaardbepalingen mogelijk zijn, mits deze niet direct of indirect in tegenspraak zijn met die standaardbepalingen en geen afbreuk doen aan de grondrechten of fundamentele vrijheden van de betrokkenen.

goedgekeurde gedragscodes en geaccrediteerde certificeringen van derden het bedrijfsleven de mogelijkheid om met maatplossingen te komen voor internationale doorgiften en te profiteren van de concurrentievoordelen die daarmee gepaard gaan, zoals een privacyzegel of -keurmerk. Een aantal van deze instrumenten kan worden ontwikkeld als specifiek voor doorgifte bedoelde mechanismen of als deel van algemenere instrumenten voor het aantonen van conformiteit met alle voorschriften van de algemene verordening gegevensbescherming, zoals in het geval van een goedgekeurde gedragscode.

De Commissie zal samenwerken met het bedrijfsleven, de civiele samenleving en de gegevensbeschermingsautoriteiten om volledig gebruik te maken van het potentieel van het instrumentarium voor internationale doorgiften waarin de algemene verordening gegevensbescherming voorziet. Het lopende overleg met belanghebbenden in het kader van de tenuitvoerlegging van de hervorming zal helpen prioritaire actiegebieden vast te stellen. Zo zouden reeds begonnen werkzaamheden kunnen worden afgerond, zoals het opstellen, in samenwerking met de Groep artikel 29 (die in 2018 zal worden vervangen door het Europees Comité voor gegevensbescherming), van verwerker-naar-verwerker-modelbepalingen⁴⁵. Ook kunnen nieuwe componenten van de EU-conformiteitsstructuur worden ontwikkeld, bijvoorbeeld doordat de Commissie vereisten en technische normen formuleert voor het invoeren en gebruiken van certificeringsmechanismen, onder meer voor aspecten die betrekking hebben op internationale doorgiften⁴⁶. Een aantal van deze maatregelen kan worden aangevuld door samenwerking op internationaal niveau, met name met organisaties die soortgelijke doorgiftemechanismen hebben ontwikkeld. Zo zouden manieren kunnen worden onderzocht om convergentie te versterken tussen enerzijds de bindende bedrijfsvoorschriften krachtens het EU-recht en anderzijds de grensoverschrijdende privacyregels van de economische samenwerking Azië-Stille Oceaan (APEC)⁴⁷, wat betreft zowel de toepasselijke normen als het toepassingsproces van de respectieve systemen. Dit zou wereldwijd hoge gegevensbeschermingsnormen moeten helpen bevorderen door de verschillen in de benadering van privacy- en gegevensbescherming te overbruggen, marktdeelnemers te helpen omgaan met verschillende systemen, en beleidsmaatregelen te bedenken die met voornoemde normen in overeenstemming zijn.

De Commissie zal:

- samen met belanghebbenden alternatieve mechanismen voor de doorgifte van persoonsgegevens ontwikkelen die aansluiten bij de specifieke behoeften of voorwaarden van specifieke bedrijfstakken, bedrijfsmodellen en/of marktdeelnemers.

⁴⁵ Momenteel zijn er geen modelbepalingen van toepassing op doorgifte tussen in de EU gevestigde verwerkers en in een niet-EU-land gevestigde verwerkers.

⁴⁶ Artikel 43, leden 8 en 9, van de algemene verordening gegevensbescherming.

⁴⁷ Zie de APEC/EU Common Referential for the Structure of the EU Binding Corporate Rules (2014) en het APEC Cross Border Privacy Rules System (CBPR), ter vergelijking van de conformiteits- en certificeringsvoorschriften van beide systemen: http://www.apec.org/~media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

3.3 Internationale samenwerking voor de bescherming van persoonsgegevens

3.3.1. Gegevensbeschermingsnormen bevorderen via multilaterale instrumenten en fora

Het EU-wetgevingskader voor gegevensbescherming fungeert vaak als een referentiepunt voor derde landen die wetgeving op dit gebied ontwikkelen. De EU zal actief blijven overleggen met haar internationale partners, zowel op bilateraal als multilateraal vlak, teneinde convergentie te bevorderen door wereldwijd hoge en compatibele normen voor de bescherming van persoonsgegevens te ontwikkelen. Dit draagt bij tot een doeltreffender bescherming van de rechten van natuurlijke personen en beperkt tegelijkertijd de belemmeringen voor grensoverschrijdend gegevensverkeer – een belangrijk element van vrijhandel.

De Commissie stimuleert met name de toetreding van derde landen tot Verdrag 108 van de Raad van Europa en het bijbehorende Aanvullend Protocol⁴⁸. Het Verdrag, dat openstaat voor niet-leden van de Raad van Europa en al door vijftig landen is bekrachtigd, waaronder Afrikaanse en Zuid-Amerikaanse landen⁴⁹, is het enige bindende multilaterale instrument op het gebied van gegevensbescherming. Momenteel wordt het herzien en de Commissie zal erop aandringen dat de gemoderniseerde tekst snel wordt vastgesteld, met het oog op toetreding van de EU. Het Verdrag zal uitgaan van dezelfde beginselen als die welke zijn verankerd in de nieuwe EU-gegevensbeschermingsregels en aldus bijdragen tot convergentie in de richting van hoge gegevensbeschermingsnormen.

De G20-top in 2017 biedt de EU opnieuw gelegenheid om aan te sturen op convergentie vanuit het beginsel dat hoge gegevensbeschermingsnormen van wezenlijk belang zijn voor de verdere ontwikkeling van een wereldwijde informatiemaatschappij die in staat is innovatie, groei en sociale welvaart te stimuleren⁵⁰.

Ook ziet de Commissie ernaar uit samen te werken met belangrijke nieuwe actoren, zoals de speciale VN-rapporteur voor het recht op privacy in het digitale tijdperk⁵¹, en haar werkrelatie met regionale organisaties, zoals de APEC, verder te ontwikkelen, ter bevordering van een mondiale cultuur van respect ten aanzien van het recht op privacy en persoonsgegevensbescherming.

Als onderdeel van haar bredere inspanningen om privacy onder de aandacht te brengen en gegevensbeschermingsnormen internationaal aan te kaarten, heeft de Europese Commissie op 15 november 2016 een project in het kader van het partnerschapsinstrument goedgekeurd,

⁴⁸ Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (ETS nr. 108) en Aanvullend Protocol bij het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens inzake toezichthoudende autoriteiten en grensoverschrijdend verkeer van gegevens (ETS nr. 181) (2001).

⁴⁹ Mauritius, Senegal en Uruguay hebben het Verdrag bekrachtigd. Daarnaast zijn Kaapverdië, Marokko en Tunesië verzocht om toe te treden.

⁵⁰ Zie ook de "Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity" van de OESO van 23 juni 2016 ("de verklaring van Cancun").

⁵¹ Zie: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

zulks ter versterking van de samenwerking met partnerlanden op dit gebied⁵². Het gaat onder meer om de financiering van activiteiten als opleiding en voorlichting. Bij de tenuitvoerlegging van de hervorming kan de EU op haar beurt profiteren van de uitwisseling van beste praktijken en de ervaring die in het kader van andere systemen is opgedaan met nieuwe uitdagingen voor de bescherming van privacy en nieuwe juridische of technische oplossingen, bv. ten aanzien van handhaving, conformiteitsinstrumenten (zoals certificeringsmechanismen en privacyeffectbeoordelingen) en de bescherming van specifieke categorieën gegevens (bv. gegevens over kinderen).

3.3.2. Samenwerking op het gebied van handhaving

De noodzaak samen te werken met toezichhoudende en handhavingsautoriteiten op het gebied van privacy neemt toe, gezien het wereldwijde bereik van multinationale ondernemingen die in een groot aantal landen enorme hoeveelheden persoonsgegevens verwerken. Problemen van niet-naleving van gegevensbeschermingsvoorschriften of inbreuken in verband met persoonsgegevens hebben vaak gevolgen voor mensen in meer dan één rechtsgebied. In dergelijke gevallen zouden de betrokkenen doeltreffender kunnen worden beschermd door middel van gezamenlijk optreden. Tegelijkertijd zouden marktdeelnemers profiteren van een duidelijker rechtskader, waarbij interpretatiehulpmiddelen en handhavingspraktijken op mondiaal niveau worden ontwikkeld.

Nu in de verbonden wereld van het gegevensverkeer grenzen geen rol meer spelen, is het zaak dat handhavingsautoriteiten nauwer gaan samenwerken⁵³. De EU staat klaar. Zoals reeds is uiteengezet, stelt de algemene verordening gegevensverwerking de Commissie in staat om internationale samenwerkingsmechanismen te ontwikkelen om de doeltreffende handhaving van gegevensbeschermingsregels mogelijk te maken, onder meer door middel van regelingen voor wederzijdse bijstand. In dit verband zou de mogelijkheid moeten worden onderzocht om een kaderovereenkomst voor samenwerking tussen EU-gegevensbeschermingsautoriteiten en handhavingsautoriteiten in bepaalde derde landen te ontwikkelen, op basis van onder meer de ervaring die de Commissie op andere handhavingsgebieden heeft opgedaan, zoals mededinging en consumentenbescherming.

⁵² Uitvoeringsbesluit C(2016)7198 van de Commissie, ter goedkeuring van de tweede fase van het jaarlijks actieprogramma 2016 van het partnerschapsinstrument.

⁵³ Tot de bestaande netwerken behoort ook het Global Privacy Enforcement Network (GPEN), dat in 2010 in OESO-verband is opgezet. Het betreft een informeel netwerk van privacyhandhavingsautoriteiten, waarbij gegevensbeschermingsautoriteiten zijn aangesloten en dat onder meer belast is met samenwerking op het gebied van rechtshandhaving, uitwisseling van beste praktijken op het gebied van grensoverschrijdende uitdagingen en ondersteuning van gezamenlijke handhavingsinitiatieven en voorlichtingscampagnes. Het GPEN brengt geen nieuwe juridisch bindende verplichtingen mee voor de deelnemers en beoogt in de eerste plaats de samenwerking bij de handhaving van privacywetgeving voor de particuliere sector te bevorderen. Zie <https://privacyenforcement.net/>.

De Commissie zal:

- de snelle vaststelling van de gemoderniseerde tekst van Verdrag 108 van de Raad van Europa bevorderen met het oog op de toetreding van de EU, en toetreding door derde landen stimuleren.
- multilaterale fora zoals de Verenigde Naties, G20 en APEC benutten om een mondiale cultuur van respect voor gegevensbeschermingsrechten te bevorderen.
- Internationale samenwerkingsmechanismen ontwikkelen met belangrijke internationale partners ter bevordering van doeltreffende handhaving.

4. DOELTREFFENDER SAMENWERKING BIJ RECHTSHANDHAVING MET KRACHTIGE GEGEVENSBECHERMINGSWAARBORGEN

De uitwisseling van persoonsgegevens maakt integrerend deel uit van het voorkomen, onderzoeken en vervolgen van strafbare feiten. In een wereld vol onderlinge verbindingen houdt criminaliteit zelden op bij nationale grenzen en de snelle uitwisseling van persoonsgegevens is dan ook van wezenlijk belang voor succesvolle samenwerking bij rechtshandhaving en een doeltreffende aanpak van criminaliteit. Dergelijke uitwisselingen moeten berusten op krachtige gegevensbeschermingswaarborgen. Een en ander draagt tevens bij tot het opbouwen van vertrouwen tussen rechtshandhavingsautoriteiten en het versterken van de rechtszekerheid wanneer informatie wordt verzameld en/of uitgewisseld.

De in de politieke richtlijn vervatte regels inzake internationale doorgiften zien op de uitwisseling tussen rechtshandhavingsautoriteiten van binnen en buiten de EU, alsmede – in specifieke situaties – op doorgiften van rechtshandhavingsautoriteiten naar andere entiteiten. De richtlijn voorziet in de mogelijkheid om adequaatheidsvaststellingen te doen op strafrechtelijk gebied. De Commissie zal de mogelijkheid van dergelijke adequaatheidsvaststellingen onder de aandacht brengen van de derde landen die daarvoor in aanmerking komen, met name die landen waarmee nauw en snel moet worden samengewerkt bij de bestrijding van criminaliteit en terrorisme en waarmee reeds op aanzienlijke schaal persoonsgegevens worden uitgewisseld. Op deze basis zal de Commissie prioriteit geven aan besprekingen over adequaatheidsbesluiten met derde landen die belangrijke partners zijn bij dit streven.

Ook de in december 2016 gesloten raamovereenkomst betreffende gegevensbescherming⁵⁴ is een geslaagd voorbeeld van hoe samenwerking bij rechtshandhaving met een belangrijke internationale partner kan worden verbeterd door overeenstemming te bereiken over krachtige gegevensbeschermingswaarborgen. De raamovereenkomst vult bestaande rechtsinstrumenten

⁵⁴ Overeenkomst tussen de EU en de VS over de bescherming van persoonsgegevens die worden doorgegeven en verwerkt met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, waaronder terrorisme, in het kader van politieke en justitiële samenwerking in strafzaken: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (de "raamovereenkomst")

waarop gegevensuitwisselingen zijn gebaseerd (met name bilaterale overeenkomsten op zowel lidstatelijk als EU-niveau), automatisch aan; dit brengt onmiddellijke en directe voordelen mee voor de betrokkenen en versterkt de samenwerking op het gebied van rechtshandhaving door informatie-uitwisseling te vergemakkelijken. De raamovereenkomst dient ook als uitgangspunt voor toekomstige regelingen inzake gegevensdoorgifte met de Verenigde Staten, zodat er ook niet steeds opnieuw hoeft te worden onderhandeld over dezelfde waarborgen. De raamovereenkomst is de eerste bilaterale internationale overeenkomst met een brede catalogus van rechten en verplichtingen inzake gegevensbescherming die in overeenstemming zijn met het EU-acquis. Daarom kan de kaderovereenkomst dienen als basis voor soortgelijke overeenkomsten met derde landen, niet alleen op het gebied van justitiële en politieke samenwerking, maar ook bij openbare handhaving (bv. mededingingsbeleid, consumentenbescherming). Daarbij zou het zowel gaan om uitwisseling tussen overheden als om gegevensdoorgifte tussen particuliere ondernemingen en rechtshandhavingsautoriteiten. De kaderovereenkomst zou het ook gemakkelijker maken voor de Unie om overeenkomsten te sluiten over gegevensuitwisseling tussen relevante EU-agentschappen (met name Europol en Eurojust) en derde landen⁵⁵. De Commissie zal derhalve de mogelijkheid onderzoeken om soortgelijke kaderovereenkomsten te sluiten met haar belangrijkste rechtshandhavingpartners.

Bovendien voorziet de politieke richtlijn in de mogelijkheid dat, met inachtneming van strenge waarborgen en onder specifieke omstandigheden, rechtshandhavingsautoriteiten in de EU rechtstreeks om informatie verzoeken bij een particuliere onderneming in een derde land en in het betreffende verzoek persoonsgegevens opnemen (gewoonlijk een naam of een IP-adres)⁵⁶. De algemene verordening gegevensbescherming heeft daarentegen betrekking op gevallen waarin particuliere entiteiten in de EU op verzoek persoonsgegevens aan de rechtshandhavingsautoriteiten van een derde land doorgeven: dergelijke doorgiften vanuit de EU zijn uitsluitend toegestaan onder bepaalde voorwaarden; zo moeten zij berusten op een internationale overeenkomst of moet verstrekking nodig zijn om gewichtige redenen van algemeen belang als erkend in het recht van de Unie of een lidstaat⁵⁷.

Deze samenwerking, die van cruciaal belang is voor succes bij onderzoek en vervolging van criminaliteit en terrorisme, wordt extra onder de aandacht gebracht in de conclusies van de Raad over het verbeteren van de strafrechtpleging in de cyberruimte. De Raad heeft de Commissie verzocht om concrete maatregelen te nemen, op basis van een gemeenschappelijke EU-aanpak, om de samenwerking met dienstverleners te verbeteren, wederzijdse rechtsbijstand doeltreffender te maken en oplossingen voor te stellen voor de problemen bij het vaststellen en handhaven van de rechtsbevoegdheid in de cyberruimte⁵⁸. Deze maatregelen omvatten zowel uitwisselingen tussen rechtshandhavingsautoriteiten en

⁵⁵ Het sluiten van operationele overeenkomsten met Europol en Eurojust is ook een benchmark bij de dialogen over visumliberalisering met bepaalde derde landen, bv. in het kader van de lopende dialoog met Turkije.

⁵⁶ Zie artikel 39 en overweging 73 van de politieke richtlijn.

⁵⁷ Zie artikel 48 en overweging 115 van de algemene verordening gegevensbescherming.

⁵⁸ Conclusies van de Raad van de Europese Unie over het verbeteren van de strafrechtpleging in de cyberruimte, 9 juni 2016: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. Nadat de Commissie in december 2016 een voortgangsverslag bij de Raad had ingediend, heeft zij opdracht gekregen om de Raad in juni 2017 concrete resultaten voor te leggen.

dienstverleners binnen de EU als uitwisselingen met autoriteiten en ondernemingen buiten de EU. De Commissie zal in juni 2017 opties schetsen voor toegang tot elektronisch bewijs, gelet op de behoefte aan snelle en betrouwbare samenwerking op basis van de strenge normen inzake gegevensbescherming van de politieke richtlijn en de algemene verordening gegevensbescherming, zowel binnen de EU als bij internationale doorgiften.

Ten slotte zal de Commissie overeenkomstig de nieuwe rechtsgrondslag van Europol de voorschriften beoordelen die zijn opgenomen in de krachtens Besluit 2009/371/JBZ gesloten operationele samenwerkingsovereenkomst tussen Europol en derden, met inbegrip van de gegevensbeschermingsvoorschriften daarin⁵⁹. Zoals is uiteengezet in de Europese veiligheidsagenda 2015, zal de Unie er bij haar toekomstige aanpak van de uitwisseling van persoonsgegevens van passagiers (PNR-gegevens) met niet-EU-landen rekening mee houden dat er consistente normen en specifieke beschermende bepalingen op het gebied van de grondrechten moeten worden toegepast. De Commissie zal werken aan juridisch deugdelijke en duurzame oplossingen voor de uitwisseling van PNR-gegevens met derde landen; zo zal zij onder meer de mogelijkheid overwegen van een modelovereenkomst over PNR-gegevens met vereisten waaraan derde landen moeten voldoen om PNR-gegevens vanuit de EU te kunnen ontvangen. Beleidsoptreden op dit gebied zal echter afhangen van met name het geplande advies van het Hof van Justitie van de Europese Unie over de voorgenomen PNR-overeenkomst tussen de EU en Canada⁶⁰.

DOELTREFFENDER SAMENWERKING BIJ RECHTSHANDHAVING MET KRACHTIGE GEGEVENSBESCHERMINGSWAARBORGEN

De Commissie zal:

- de mogelijkheid om adequaatheidsbesluiten vast te stellen op grond van de politieke richtlijn onder de aandacht brengen van landen die ervoor in aanmerking komen.
- aansturen op onderhandelingen over overeenkomsten op het gebied van rechtshandhaving met belangrijke internationale partners, volgens het model waarin de raamovereenkomst met de VS voorziet.
- gevolg geven aan de conclusies van de Raad over het verbeteren van de strafrechtpleging in de cyberruimte, ter bevordering van de grensoverschrijdende uitwisseling van elektronisch bewijs conform de gegevensbeschermingsregels.

⁵⁹ Zie artikel 25, lid 4, van Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad, PB L 135 van 24.5.2016, blz. 53. De Commissie dient uiterlijk op 14 juni 2021 een beoordelingsverslag in te dienen over de samenwerkingsovereenkomsten van Europol die vóór 1 mei 2017 zijn gesloten.

⁶⁰ Advies van het Hof van Justitie over de ontwerpovereenkomst tussen de EU en Canada inzake PNR van 2014 (Advies 1/15). Het Hof was verzocht om de verenigbaarheid van de ontwerpovereenkomst te toetsen aan het EU-Handvest van de grondrechten.

5. CONCLUSIE

Persoonsgegevens beschermen en uitwisselen sluiten elkaar niet uit. Een krachtig gegevensbeschermingssysteem bevordert het gegevensverkeer door het consumentenvertrouwen te vergroten in ondernemingen die de persoonsgegevens van hun klanten zorgvuldig behandelen. Hoge gegevensbeschermingsnormen worden zo een voordeel in de digitale wereldeconomie. Hetzelfde geldt voor samenwerking bij rechtshandhaving: privacywaarborgen zijn een integrerend onderdeel van de doeltreffende en snelle uitwisseling van informatie bij de bestrijding van criminaliteit, gebaseerd op wederzijds vertrouwen en rechtszekerheid.

Wanneer de hervorming van de gegevensbeschermingsregels eenmaal is afgerond, dient de EU hierover proactief te overleggen met derde landen. Zij moet internationaal, zowel op bilateraal als multilateraal vlak, streven naar meer opwaartse convergentie van gegevensbeschermingsbeginselen. Dit is in het belang van zowel burgers als bedrijven. Het nieuwe wetgevingskader inzake gegevensbescherming biedt de EU de nodige en passende instrumenten om deze doelstellingen te verwezenlijken. Op basis van de in deze mededeling geschetste strategische aanpak zal de Commissie actief overleggen met belangrijke derde landen om na te gaan of er adequaatheidsvaststellingen kunnen worden gedaan, teneinde op convergentie van de regelgeving in de richting van de EU-normen aan te sturen en de handelsbetrekkingen te bevorderen, om te beginnen met Japan en Korea in 2017. Tegelijkertijd zal de EU de diverse alternatieve instrumenten voor doorgifte ten volle benutten om gegevensbeschermingsrechten te beschermen en marktdeelnemers te ondersteunen wanneer gegevens worden doorgegeven aan landen waarvan het binnenlands recht geen adequaat niveau van gegevensbescherming waarborgt. Dergelijke instrumenten zouden ook moeten worden gebruikt om de samenwerking tussen toezichhoudende en rechtshandavingsautoriteiten van de EU en hun internationale partners verder te bevorderen. De Commissie zal de samenhang tussen de interne en externe dimensie van het EU-gegevensbeschermingsbeleid waarborgen en krachtige gegevensbescherming op internationaal niveau stimuleren, teneinde de samenwerking bij rechtshandhaving te verbeteren, bij te dragen tot vrijhandel en wereldwijd hoge normen voor de bescherming van persoonsgegevens te ontwikkelen.