

Vergaderjaar 2012–2013

**33 169**

**EU-voorstel: Richtlijn bescherming  
persoonsgegevens bij gebruik door politie en  
justitiële autoriteiten (COM(2012) 10) en  
EU-voorstel Verordening algemeen kader  
bescherming persoonsgegevens (COM(2012)11)<sup>1</sup>**

**F**

**BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN  
JUSTITIE**

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 11 februari 2013

Bijgaand treft u een afschrift aan van mijn brief van heden aan de Voorzitter van de Tweede Kamer der Staten-Generaal over de stand van zaken van de onderhandelingen over de EU-verordening gegevensbescherming en de richtlijn gegevensbescherming opsporing en vervolging.

De staatssecretaris van Veiligheid en Justitie,  
F. Teeven

<sup>1</sup> Zie dossiers E120003 en E120004 op [www.europapoort.nl](http://www.europapoort.nl)

## **BRIEF AAN DE VOORZITTER VAN DE TWEDE KAMER DER STATEN-GENERAAL**

Den Haag, 11 februari 2013

In het algemeen overleg van 7 maart 2012 (Kamerstukken II 2011/12, 32 761, nr. 27) heb ik u toegezegd u periodiek op de hoogte te houden van de stand van zaken over de onderhandelingen in Brussel over de Algemene verordening gegevensbescherming en de richtlijn gegevensbescherming opsporing en vervolging. Eerdere rapportages zond ik u bij mijn brieven van 29 juni 2012 (Kamerstukken II 2011/12, 32 761, nr. 34) en van 23 oktober 2012 (Kamerstukken II 2012/13, 32 761, nr. 44).

In deze brief doe ik verslag van de onderhandelingen die in de maanden oktober, november en december 2012 plaatsvonden. In oktober en november 2012 is verder onderhandeld over de verordening. In december 2012 is alleen onderhandeld over de richtlijn.

### *Friends of the Presidency 12 oktober 2012*

Het Cypriotisch voorzitterschap heeft op 12 oktober 2012, ter uitvoering van besluiten van de informele JBZ Raad van 25 juli 2012 in Nicosia, een afzonderlijke vergadering georganiseerd over een vragenlijst die betrekking heeft over de onderwerpen gedelegeerde regelgeving, administratieve lasten en de mate van flexibiliteit voor gegevensverwerking in de publieke sector.

Op deze vergadering is uitsluitend gesproken over gedelegeerde regelgeving. Nederland heeft daarbij tevoren ingezet op schrapping van vrijwel alle grondslagen voor gedelegeerde handelingen en een groot aantal uitvoeringshandelingen. In een gedelegeerde handeling wordt de Commissie bevoegd verklaard tot het stellen van aanvullende regels. In een uitvoeringshandelingen wordt bijvoorbeeld voorzien bij de vaststelling van standaardformulieren of andere handelingen van ondergeschikt belang.

Nederland ziet voor gedelegeerde handelingen alleen toegevoegde waarde bij de uitwerking van artikel 33 (data protectie impact assessment). Nederland is van oordeel dat de schaal waarop gedelegeerde handelingen worden voorgesteld, en de selectie onderwerpen waarop dit gebeurt, vrijwel zeker leidt tot overregulering indien al deze bevoegdheden worden gebruikt. Er zijn alternatieven beschikbaar, in de eerste plaats door meer aan de samenleving over te laten, in de tweede plaats door de European Data Protection Board meer te betrekken bij de invulling van de verordening.

Nederland ziet voor uitvoeringshandelingen toegevoegde waarde bij de uitvoering van de artikelen 12 (wijze uitvoering rechten betrokkene), 14 (informatieverplichting verantwoordelijke), 18 (dataportabiliteit), 30 (beveiligingsplicht), 31 (meldplicht datalekken), 33 (data protectie impact assessment), 38 (gedragscodes) en 41 (bekendmaking niveaus passendheid gegevensbescherming derde landen).

Nederland heeft bovengenoemde standpunten op de vergadering nog eens mondeling naar voren gebracht en toegelicht. Daarbij bleek dat vrijwel alle lidstaten in algemene zin fundamentele bezwaren hebben tegen de manier waarop gedelegeerde en uitvoeringshandelingen als beleidsinstrument worden benut.

Het was verheugend te vernemen dat de Commissie de bereidheid heeft de keuzes in overleg met Raad en Europees Parlement nader te overwegen. De Commissie heeft gewezen op alternatieven als het inhoudelijk inperken van de delegatiegrondslag, het procedureel verzwaren van de delegatie, het schrappen van de delegatiegrondslag, al dan niet in combinatie met het strakker redigeren van de desbetreffende

bepaling, het benutten van de samenwerking tussen de toezichthouders, het overlaten van meer zaken aan de lidstaten, of zwaarder leunen op het accountabilitybeginsel en de verantwoordelijkheid van de sectoren aanpreken. Op de Friends of the Presidency vergadering zijn geen besluiten genomen, noch is op besluitvorming door de Raad voorgesorteerd. De discussie is in de vergadering niet voltooid en voortgezet op de volgende raads werkgroep.

#### *Raads werkgroep 22 en 23 oktober 2012*

Tijdens deze raads werkgroep is eerst de discussie voortgezet die op de Friends of the Presidency van 12 oktober 2012 is gestart met een artikelsgewijze behandeling van alle afzonderlijke delegatiegrondslagen voor gedelegeerde en uitvoeringshandelingen, voor zover het betrefte de artikelen die reeds in een eerder stadium door de raads werkgroep zijn besproken. Delegatiegrondslagen in de artikelen 34 tot en met 91 worden in het vervolg gelijktijdig met de rest van het desbetreffende artikel besproken.

Nederland heeft zich na het algemene debat over de delegatiegrondslagen beperkt tot het herhalen van het reeds bij het algemene debat uitgesproken standpunt. Nederland heeft bij de bespreking van de delegatiegrondslagen in de artikelen 11 tot en met 38 samen met een aantal andere lidstaten gewezen op de samenhang tussen het delegatievraagstuk en het vraagstuk van de administratieve lasten. Minder regels en het geven van meer verantwoordelijkheid aan verantwoordelijken voor de gegevensbescherming en aan onafhankelijke toezichthouders hangen nauw samen.

Principiële bezwaren houdt Nederland tegen de gedelegeerde handelingen op grond van artikel 6 (rechtvaardigingsgronden voor gegevensverwerking). Een bevoegdheid van de Commissie om de rechtvaardigingsgrond «gerechtvaardigd belang van de verantwoordelijke of een derde» in te vullen, komt er in feite op neer dat de Commissie het eindoordeel heeft over het vaststellen van doeleinden voor de verwerking van persoonsgegevens voor alle gevallen die niet onder een andere rechtvaardigingsgrond vallen te scharen. Het is volgens Nederland principieel onmogelijk dat de overheid – Europees of nationaal – ooit op voorhand een dergelijk oordeel zelf kan vellen. Dat zou bovendien aanzienlijke negatieve effecten hebben op het bedrijfsleven en het innoverend vermogen van economische actoren. De rechtvaardiging van een gegevensverwerking kan daarnaast altijd door de toezichthouder worden getoetst.

Zonodig kan het oordeel van de rechter worden ingeroepen. Deze delegatiegrondslag is naar het oordeel van Nederland ook niet in overeenstemming te brengen met artikel 290 VWEU (dat regelt dat gedelegeerde handelingen niet de essentie van de delegerende bepaling mogen betreffen).

Vervolgens is de artikelsgewijze discussie voortgezet met *artikel 34* (voorafgaande toestemming en voorafgaande raadpleging toezichthouder).

Nederland is in grote lijnen akkoord met de gevallen waarin er nog moet worden voorzien in voorafgaande toestemming van de toezichthouder bij enkele met name genoemde verwerkingen van persoonsgegevens of de ten aanzien van die verwerking te verrichten handelingen. Wel is het de vraag of het criterium dat wordt gebruikt bij de bepaling of die toestemming noodzakelijk is voldoende onderscheidend is. In het voorstel wordt gesproken over «specifieke» risico's. Dat geeft weinig houvast. Nederland voelt meer voor een aanscherping.

Nederland heeft meer moeite met het instrument van voorafgaande raadpleging van de toezichthouder. Raadpleging suggereert openheid en gelijkwaardigheid tussen toezichthouder en ondertoezichtgestelde. Dat is

onjuist, vindt Nederland. De verhouding is niet gelijkwaardig. Een toezichthouder beschikt over overheidsbevoegdheden. Raadpleging impliceert ook dat een toezichthouder gedurende de raadpleging tot de conclusie komt dat die bevoegdheden moeten worden gebruikt. Er kan dan geen sprake meer zijn van echte raadpleging. Er is dan sprake van onderzoek, gericht op handhaving. Nederland is voorstander van een scherp onderscheid tussen bestuursrechtelijke instrumenten als toestemming of ontheffing enerzijds, en zuivere onderzoeks- en handhavingsbevoegdheden anderzijds. Raadpleging is een onduidelijke tussenfiguur. Dat leidt tot duidelijkheid in de bevoegdheidsuitoefening door de toezichthouder. Ook de ondertoezichtgestelde heeft daarbij baat. Nederland heeft ernstige bedenkingen bij de voorgestelde bevoegdheid van de toezichthouder tot het vaststellen van een verbod op het verwerken van gegevens, indien dit verbod voorafgaand aan de verwerking wordt vastgesteld. Dat is in strijd met het recht op de vrijheid van meningsuiting, zoals geregeld in artikel 7 van de Grondwet. Uit oogpunt van wetssystematiek acht Nederland regeling van de bevoegdheid van de toezichthouder tot het uitbrengen van advies op voorgestelde wetgeving in artikel 34 niet wenselijk. Artikel 53 is daarvoor de juiste plaats.

De gedelegeerde handelingen, voorzien in art. 34, achtste lid, kunnen wat Nederland betreft worden gemist. Een betere omschrijving van het begrip «specifiek risico» in het eerste lid is een beter alternatief.

In *artikel 35* wordt de aanwijzing van een functionaris voor de gegevensbescherming (FG) geregeld. Nederland is van mening dat de instelling van een FG een belangrijke bepaling van de verordening is. De officiële evaluatie van de Wet bescherming persoonsgegevens in Nederland leert twee zaken. In de eerste plaats blijkt dat wanneer een bedrijf of instelling een FG heeft aangesteld het niveau van zorg voor de gegevensbescherming en het bewustzijn van medewerkers van de organisatie significant hoger is dan bij bedrijven of instellingen die geen FG hebben aangesteld. Dat blijkt dus een belangrijk instrument van zelfregulering te zijn. In de tweede plaats schrikken veel bedrijven in de private sector toch terug voor de aanstelling van een FG, omdat de verplichting deze met formele bevoegdheden uit te rusten wordt afgewezen. Men staat afwijzend tegenover regulering van de interne structuur van bedrijven, en geeft de voorkeur aan zelfregulering. Stimuleren een FG aan te stellen lijkt Nederland daarom verstandig.

De vraag is echter of de verordening dat in voldoende mate doet.

Nederland vraagt of hierover is nagedacht of het noodzakelijk is dat zowel de verantwoordelijke als de verwerker beide een FG aanstellen. De maatstaf van 250 personen per bedrijf of instelling – ditmaal als ondergrens voor de oplegging van de verplichting een FG aan te stellen – is al veelvuldig aan de orde geweest. Bedrijfsomvang staat los van de risico's voor de bescherming van de persoonlijke levenssfeer. Risico en aard van de verwerking is volgens Nederland een betere maatstaf. Er is dan natuurlijk nog wel de vraag hoe dat risico wordt bepaald. Nederland denkt dat een data protectie impact assessment daarbij nuttige diensten kan leveren. Dan staat tenminste op een transparante wijze vast hoe groot dat risico naar redelijke inschatting is, en kan de vraag worden beantwoord of aanstelling van een FG een nuttige maatregel is om het risico te verkleinen.

Wat de positie van de FG binnen een organisatie betreft, is Nederland van oordeel dat een FG aanspraak mag maken op een zekere arbeidsbescherming, maar principieel niet een ander belang dan dat van de verantwoordelijke die hem aanstelt en betaalt kan dienen. Dat moet ook voor betrokkenen duidelijk zijn. De verordening verdient in dit opzicht bijstelling. Ook de benoemingstermijn van twee jaar acht Nederland in dat verband ongewenst. Dit moet aan de verantwoordelijke worden overgelaten.

In de *artikelen 36 en 37* worden de positie en de taken van de FG geregeld. Nederland kan zich in de hoofdlijn van deze bepalingen vinden. Wel verdient het volgens Nederland aanbeveling dat duidelijk wordt geregeld dat de FG twee rechten heeft: het recht om intern in de organisatie waar hij werkt inlichtingen te kunnen inwinnen, en het recht om de verwerkte gegevens te mogen inzien. Die rechten behoren volgens Nederland te worden aangevuld met een geheimhoudingsplicht ter bescherming van de belangen van de organisatie en de belangen van de betrokkenen wier gegevens worden verwerkt.

In *artikel 38* is de regeling over (private) gedragscodes neergelegd. Nederland heeft de inmiddels opgedane ervaringen met gedragscodes ter tafel gebracht. Gedragscodes zijn in elk geval in kwantitatief opzicht achtergebleven bij de verwachtingen die er in 1995 van bestonden. In kwalitatief opzicht zijn niet alle gedragscodes even goed, maar er zijn er die goed lijken te werken. Nederland steunt de bottom up benadering van de Commissie, die uitgaat van stimuleren en niet van verplichten. Nederland vindt dat naast zelfregulering ook andere alternatieven de kans moeten krijgen om verantwoordelijken wat meer vrijheid te bieden. Een dataprotectie impact assessment kan de basis vormen voor een meer gerichte inzet van de ex ante instrumenten die de verordening kent.

Het Voorzitterschap doet tenslotte verslag van het contact met de raads werkgroep inzake statistiek. Laatstgenoemde werkgroep kijkt met belangstelling naar de wijze waarop gegevensverwerking voor statistische doeleinden is geregeld.

#### *Friends of the Presidency 13 november 2012*

Het Voorzitterschap probeert naar aanleiding van de discussies op 12 en 22 oktober 2012 vast te stellen op welke onderdelen van de verordening sprake is van convergenties tussen de lidstaten op het gebied van de gedelegeerde handelingen. Op die manier zou volgens het Voorzitterschap een begin van besluitvorming kunnen worden voorbereid. Het overgrote deel van de lidstaten, Nederland daaronder begrepen, meent dat het nog te vroeg is voor de voorbereiding van besluitvorming. Nog niet alle bepalingen waarin delegatiegrondslagen zijn opgenomen zijn besproken. Die grondslagen moeten worden gezien tegen de achtergrond van de rest van het desbetreffende artikel.

De discussie wordt voortgezet over het tweede onderwerp dat door het Cypriotische voorzitterschap is aangemerkt als horizontaal onderwerp, administratieve lasten.

Nederland heeft in algemene zin gereageerd met het uitgangspunt dat afschaffing van de meldingsplicht een heel belangrijke stap vooruit is. Maar die stap moet niet teniet worden gedaan door het zonder werkbaar en redelijk onderscheid opleggen van lasten aan alle verantwoordelijken en bewerkers. Waar de verordening onderscheid maakt, is dit voornamelijk gericht op bedrijfsgrootte en niet op het risico gemoeid met de verwerking. Een risicoanalyse, procedureel ingeleid door een privacy impact assessment en materieel geassocieerd met risico's als aantal en aard van de gegevens, aantal en hoedanigheid van de betrokken, het risico voor identiteitsdiefstal bij ongecontroleerde toegang en financiële risico's bij verlies of blootstelling is de weg vooruit.

Een hoger risico rechtvaardigt het opleggen van hogere lasten en zwaardere verplichtingen. Dat alles moet nog worden uitgewerkt. Er zijn varianten denkbaar. Het zou een algemene regeling, een aanpassing van de artikelen of een combinatie van deze methoden kunnen zijn.

Uit de discussie komen de volgende vragen naar voren die op een nader te bepalen wijze – mogelijkerwijs in een algemene bepaling – beantwoord moeten worden in de verordening: 1. Welke risico's kunnen worden geïdentificeerd. 2. Op welke wijze wordt dit risico vastgesteld en wie

draagt daarvoor de verantwoordelijkheid. 3. Met welke maatregelen kan het risico worden voorkomen of verkleind. 4. Op wie rust de verantwoordelijkheid voor het voorkomen of verkleinen van het risico.

Het Voorzitterschap beoordeelt de gehouden discussie positief en besluit deze voort te zetten op de raads werkgroep die aansluitend wordt gehouden.

#### *Raads werkgroep 14 en 15 november 2012*

Bij de voortzetting van de discussie over de administratieve lasten laat Nederland weten dat het positief terugkijkt op hetgeen de voorgaande dag naar voren is gebracht. Nederland is ook ingenomen met de mededeling van de Commissie dat zij zich constructief opstelt ten aanzien van de suggestie dat de risicobeoordeling in een horizontale bepaling wordt neergelegd. Er zijn door enkele lidstaten verdere suggesties gedaan over de uitwerking van een dergelijke bepaling. De verwachting is dat deze in een later stadium zullen worden uitgewerkt.

De artikelsgewijze behandeling wordt voortgezet met *artikel 39* (certificering). Nederland kan deze bepaling, die uitgaat van het stimuleren van private initiatieven van harte ondersteunen. Nederland maakt melding van de beperkte ervaring die in eigen land met het systeem van certificering bestaat. Er zijn nog weinig bedrijven en instellingen die over een privacycertificaat beschikken. Het Nederlands Forensisch Instituut, onderdeel van mijn ministerie, is daar overigens één van. Wel blijft het de vraag of de normen aan de hand waarvan het certificaat wordt afgegeven niet geharmoniseerd moeten worden. Daarbij is het vervolgens weer de vraag of die normen inhoudelijk door de Commissie worden vastgesteld in een gedelegeerde handeling – zoals de bedoeling lijkt – of door de Commissie alleen erkend moeten worden in een instrument.

Nederland is voorstander van laatstgenoemde oplossing, omdat die beter past bij een vrijwillige vorm van certificering.

De artikelsgewijze behandeling wordt voortgezet met een nieuw hoofdstuk, te weten *hoofdstuk V*, over de grensoverschrijdende gegevensdoorgiften. Nederland brengt in algemeen zin naar voren over dit hoofdstuk dat het twee gezichten heeft. Enerzijds zijn in dit hoofdstuk echt belangrijke stappen vooruit gezet. Te denken valt aan de bindende bedrijfsvoorschriften. Anderzijds zijn er ook voorstellen gedaan die nog onvoldoende duidelijkheid bieden, of die zelfs beperkend zijn in vergelijking met het huidige recht. Ernstiger is dat uit hoofdstuk V in het geheel niet blijkt hoe de effecten van cloudcomputing in de verordening worden geregeld. Cloudcomputing wint zeer snel aan populariteit en is in feite niets anders dan een permanente grensoverschrijdende verwerking van gegevens.

Zo is het voor Nederland de vraag wat nu eigenlijk de bedoeling is van *artikel 40* (algemene bepaling over grensoverschrijdende gegevensdoorgiften). Nederland vraagt wat de toegevoegde waarde is van een bepaling die in feite niet meer zegt dan dat grensoverschrijdende gegevensdoorgiften zijn onderworpen aan de verordening. Dat is volgens Nederland een overbodige bepaling.

De artikelsgewijze behandeling is onderbroken door een discussie over de keuze van een instrument, een verordening, en de consequenties die dat met zich brengt. Het gaat daarbij met name om de vraag hoeveel ruimte een verordening laat aan het recht van de lidstaten om ten behoeve van de publieke sector. De juridische dienst van de Raad verduidelijkt dat een verordening rechtstreeks geldend recht is in de rechtsordes van de lidstaten, en daarom niet mag worden omgezet in nationaal recht. Wel kan een verordening een zekere mate van flexibiliteit bieden in het overlaten

van onderwerpen aan de regelgevende bevoegdheid van de lidstaten, maar die ruimte wordt door artikel 288 van het Verdrag betreffende de werking van de Europese Unie en vaste jurisprudentie van het Hof van Justitie van de Europese Unie beperkt.

Nederland herhaalt bij deze discussie het ingenomen standpunt dat het voorstander is van een verordening. Wel verwacht Nederland dat deze voor de publieke sector op onderdelen de nodige ruimte biedt voor regelgeving door de lidstaten. De artikelen 5 en 21 bieden daarvoor een goed begin, maar er is vermoedelijk meer nodig. En dat is ook gerechtvaardigd, want de organisatie van de publieke sector verschilt per lidstaat. Dat zal ook door de Commissie moeten worden gerespecteerd. Met de keuze voor een verordening die ruimte laat aan de lidstaten, ligt primair bij de Commissie de verantwoordelijkheid de consequenties daarvan in alle opzichten te doordenken. De Commissie heeft aangegeven te zullen nadenken over de vragen van de lidstaten.

Wat de behandeling van *artikel 40* betreft, is Nederland van oordeel dat het teleurstellend is dat de mededeling van de Commissie inzake cloudcomputing van 27 september 2012, COM (2012) 529 (def), voor de oplossing van vragen van gegevensbescherming verwijst naar de verordening, terwijl de Commissie bij de behandeling van de verordening weer verwijst naar de mededeling. Dit onderwerp zal daarom verder moeten worden besproken.

In *artikel 41* is de nieuwe regeling voor de beoordeling van de passendheid van het niveau van gegevenbescherming in derde landen neergelegd. Nederland noteert dat de Commissie in deze bepaling nu het enige orgaan is dat bevoegd is een dergelijke beoordeling te doen. In de huidige richtlijn is er ruimte voor andere oplossingen. In de bestaande Nederlandse wetgeving is een primaire beoordeling overgelaten aan de verantwoordelijke.

Nederland acht dat passend bij het beeld dat in Nederland bestaat bij het begrip «verantwoordelijkheid». Dat kwam goed van pas omdat het aantal landen dat een beoordeling van de Commissie heeft ontvangen betrekkelijk klein is, en het bij de meeste van die landen gaat om bescheiden economieën. En het kan in veel gevallen ook goed gaan zonder expliciete toestemming van de overheid. Bij het uitwisselen van medische gegevens tussen artsen of het uitwisselen van strafrechtelijke gegevens tussen advocaten, bestaat meestal zekerheid over het bestaan van geheimhoudings- en verschoningsplichten in het betreffende derde land. Als die waarborgen er zijn, dan moeten er ook geen nodeloze drempels voor de doorgifte van gegevens worden opgeworpen. Nederland kan zich voorstellen dat in het kader van de informatie- en documentatieplicht voor verantwoordelijkheden hieraan aandacht kan worden besteed.

Daarnaast vraagt Nederland zich af wat de betekenis van de laatste volzin van art. 41, lid 1, is. Er staat geen «verdere toestemming». De vraag is of er dan sprake van een eerdere of een voorafgaande toestemming. Verder vraagt Nederland of er nog een onderlinge relatieve zwaarte tussen de elementen van art. 41, lid 2, is. Bij sub a vraagt Nederland zich af of de EU derdelanden de maat moet nemen waar het gaat om de wetgeving met betrekking tot de nationale veiligheid van derde landen, terwijl dat geen competentie van de EU is, maar van de lidstaten. Bij sub b vraagt Nederland of er inderdaad altijd sprake kan zijn van onafhankelijk toezicht in de zin van de verordening. Er bestaan ook andere toezichthoudende mechanismen. Nederland verwijst in dit kader naar het PNR-akkoord met de VS. Bij sub c stelt Nederland dat deze bepaling wat minder ruim geformuleerd zou kunnen worden. Nederland stelt zich zo voor dat de internationale verplichtingen van het desbetreffende land specifiek betrekking moet hebben op de gegevensbescherming en het niveau van de grondrechtenbescherming. Verder ziet Nederland hier ook een rol voor de EDPB.

Bij art. 41, lid 5, stelt Nederland dat het niet eenvoudig voorstelbaar is dat de beslissingen van de Commissie op grond van lid 5 spontaan worden genomen. Is het niet beter, zo vraagt Nederland zich af, om een regeling die voorziet in vaststelling dat een derde land expliciet niet beschikt over een passend niveau van gegevensbescherming te vervangen door een regeling waarbij reeds gegeven beslissingen over de passendheid kunnen worden ingetrokken. Daarnaast is Nederland van mening dat overweging 82 suggereert dat na een besluit op grond van art. 41, lid 5, een verbod bestaat tot het exporteren van gegevens. Verboden horen in de tekst van de verordening te staan. Die moeten dan ook worden gesanctioneerd of anders worden weggelaten. Bij art. 41, lid 6, zou volgens Nederland het horen van de belanghebbende door de Commissie niet misstaan.

*Artikel 42* regelt de doorgiften onder passende waarborgen, zoals de bestaande bindende standaardcontractclausules en enkele andere in de artikelen 43 en 44 nader uitgewerkte grondslagen. Nederland kan met dit artikel goed uit de weg. Het sluit goed aan bij het huidige recht. Een enkele redactionele opmerking zal schriftelijk worden nagezonden aan het Raadssecretariaat.

#### *Raadswerkgroep 19 en 20 december 2012*

In deze raadswerkgroep zijn de artikelen 9 tot en met 15 en artikel 17 van de ontwerprichtlijn gegevensbescherming opsporing en vervolging besproken.

Nederland heeft positief gereageerd op de voorgestelde regeling rond de profilering en geautomatiseerde verwerking van persoonsgegevens in artikel 9. De tekst is nauw afgestemd op die van de verordening (art. 20 van de verordening). Wel heeft Nederland gewezen op de resolutie van de Raad van Europa over profilering (CM/REC (2010)13) en aanbevolen om deze resolutie als uitgangspunt te nemen voor een regeling voor profilering op het niveau van de Unie. Daarnaast heeft de Nederlandse delegatie voorgesteld om aan het woord «uitsluitend» toe te voegen de woorden «of in beslissende mate», zodat de reikwijdte van de bepaling wordt verruimd. De Commissie geeft aan open te staan voor een definitie van profileren. Voor de verwerking van gevoelige gegevens, als geregeld in het tweede lid, zou het woord «uitsluitend» vervangen kunnen worden vervangen door de woorden «uitsluitend of hoofdzakelijk», in overeenstemming met het advies van het Agentschap voor de Grondrechten.

Nederland heeft eveneens positief gereageerd op de voorgestelde tekst van artikel 10, inzake de modaliteiten voor de uitoefening van de rechten van de betrokkene. De tekst van het eerste en derde lid kan strakker worden geredigeerd, door de woorden «all reasonable steps» te schrappen. In het vierde lid zou een concrete tijdslimiet ingevoegd moeten worden, naar het voorbeeld van de termijn van vier weken van de verordening (artikel 12, tweede lid, van de verordening). Bij het vijfde lid heeft Nederland voorgesteld het woord «vexatoire» te vervangen door «duidelijk buitensporig», overeenkomstig de tekst van de verordening (art. 12, vierde lid, van de verordening). Voorts heeft Nederland bij dit lid een studievoorbehoud geplaatst, vanwege de mogelijke financiële consequenties van het afschaffen van de verplichting voor de betrokkene om een vergoeding te betalen voor het verstrekken van persoonsgegevens. De Commissie gaat akkoord met de vervanging van het woord «vexatoire» door de woorden «duidelijk buitensporig».

Nederland heeft aangegeven grote aarzelingen te hebben bij het voorstel voor een actieve informatieverstrekking aan de betrokkene, als neergelegd in artikel 11. De aard van het politiewerk staat dikwijls in de weg aan het



verschaffen van informatie aan de betrokkene. De voorgestelde regeling gaat ervan uit dat wanneer de persoonsgegevens bij de betrokkene worden verzameld, de verantwoordelijke de betrokkene inlicht over de gegevensverwerking, op het tijdstip waarop de persoonsgegevens van de betrokkene worden verkregen (art. 11, eerste en derde lid, onderdeel a). Nederland heeft vragen over de wijze waarop een dergelijke verplichting tenuitvoer kan worden gelegd bij het aftappen van telecommunicatie; de gegevens worden dan van de betrokkene verkregen zonder dat deze daar zelf kennis van heeft. Voor gegevens die niet bij de betrokkene worden verzameld, bestaat de mogelijkheid om de betrokkene binnen een redelijke termijn na de gegevensverzameling in te lichten (art. 11, eerste en derde lid, onder b). Dit zal in de praktijk lastig uitvoerbaar zijn, omdat dit veronderstelt dat de politie zich periodiek rekenschap geeft van de vraag of alle betrokkenen, niet alleen de verdachte maar ook aangevers, getuigen en andere personen van wie enig persoonsgegeven wordt verwerkt, in een opsporingsonderzoek adequaat zijn ingelicht. In opsporingsonderzoeken van enige omvang zullen tientallen personen kunnen voorkomen waarmee de politie in aanraking is gekomen, hetgeen een enorme administratieve belasting zal vormen voor de politie of het openbaar ministerie. Nederland is van mening dat een wettelijke regeling aan de betrokkene voldoende duidelijkheid kan bieden om te weten wanneer en in welke omstandigheden op zijn persoon betrekking hebben gegevens verwerkt kunnen worden.

De kenbaarheid van de gegevensverwerking kan daarmee voldoende worden verzekerd. Te dien aanzien zouden ook alternatieven, zoals een facultatieve verplichting tot het informeren van de betrokkene, onderzocht moeten worden. De Commissie wijst erop dat de voorgestelde tekst de lidstaten de nodige ruimte biedt («passende maatregelen» in het eerste lid, en de mogelijkheid om bepaalde categorieën van persoonsgegevens uit te zonderen). Wel is de Commissie bereid de lasten te beperken, de tekst zal nog worden herzien.

#### *Artikel 12 en 13*

Nederland heeft aangegeven zich te kunnen vinden in de artikelen betreffende het recht van toegang van de betrokkene en de bepalingen op dat recht. Deze teksten zijn gebaseerd op die van het bestaande kaderbesluit dataprotectie. Nederland is minder gelukkig met een actieve informatieverstrekking door politie en justitie, als voorzien in artikel 11 van de ontwerprichtlijn, maar is voorstander van een uitgebreid recht op toegang voor de betrokkene.

Voor wat betreft artikel 12 heeft Nederland enige reserve bij de verplichting voor de lidstaten om de betrokkene een kopie te verstrekken van de persoonsgegevens die worden verwerkt. Het is niet duidelijk hoe aan een dergelijke verplichting kan worden voldaan als het gaat om de banden met opgenomen telefoongesprekken of video-opnamen. Dit kunnen omvangrijke gegevensbestanden betreffen, die minder eenvoudig kunnen worden gekopieerd. Hierbij zou politie en justitie ook meer flexibiliteit geboden kunnen worden, bijvoorbeeld met de mogelijkheid van inzage voor de betrokkene. In een reactie zegt de Commissie toe het realiteitsgehalte van het voorgestelde tweede lid van artikel 12 te zullen bezien.

Voor wat betreft artikel 13 meent Nederland dat iedere weigering afzonderlijk moet worden beoordeeld. Dit betekent dat het tweede lid – dat voorziet in de mogelijkheid om categorieën van gegevensverwerking uit te sluiten van het recht van toegang – moet worden geschrapt.

#### *Artikel 14*

In dit artikel zijn de modaliteiten voor de uitoefening van het recht van toegang geregeld. Nederland is positief over dit voorstel maar acht het van belang dat de toezichthoudende autoriteit zelf een afweging kan maken of zij termen aanwezig acht om een onderzoek in te stellen. Dit moet geen verplichting zijn, zoals de voorliggende tekst impliceert. De Commissie geeft aan dat duidelijk moet zijn dat de lidstaten zelf kunnen inrichten op welke wijze de nationale toezichthouder deze toetsing invult.

#### *Artikel 15*

Nederland heeft geen opmerkingen ingebracht over het recht van correctie.

#### *Artikel 17*

Dit artikel regelt de rechten van de betrokkene bij strafrechtelijke onderzoeken en procedures. Nederland heeft aangegeven dat de voorgestelde bepaling de nodige vragen oprept. Deze bepaling moet niet te ruim uitgelegd kunnen worden, zodat deze ook van toepassing is op gegevens die onderdeel vormen van een gerechtelijk dossier zonder dat er sprake is van een gerechtelijke procedure. Nederland heeft voorgesteld de tekst meer af te stemmen op die van artikel 4, vierde lid, van het bestaande kaderbesluit dataprotectie. De Commissie stelt dat dit artikel niet beoogt om bepaalde rechten voor te schrijven of het strafprocesrecht te beïnvloeden. Misschien is het beter om de strekking van deze bepaling op te nemen in de overwegingen, dit zal nader worden bezien.

Nederland kijkt met tevredenheid terug op de wijze waarop het Cyprisch voorzitterschap de onderhandelingen over beide instrumenten door een lastige fase heeft weten te leiden.

De staatssecretaris van Veiligheid en Justitie,  
F. Teeven