Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

32 761 Verwerking en bescherming persoonsgegevens

Nr. 44

BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 oktober 2012

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.

Bij mijn brief van 29 juni 2012 (Kamerstukken II 2011/12, 32 761, nr. 34) heb ik u een eerste voortgangsrapportage gezonden. Bij brief van de Minister van Veiligheid en Justitie aan de Voorzitter van de Eerste Kamer der Staten-Generaal van 22 augustus 2012 (Kamerstukken I 2011/12, 32 317, CA) is verslag gedaan van hetgeen op de informele JBZ-Raad van 23 en 24 juli 2012 met betrekking tot beide wetgevingsvoornemens is besproken. Deze brieven zijn voor de Eerste Kamer aanleiding geweest enkele vragen te stellen in een brief van 2 oktober 2012. Het antwoord op deze vragen van de Eerste Kamer is verwerkt in de verslaglegging over de behandeling van artikel 33 van de Algemene verordening gegevensbescherming, onder het opschrift Raadswerkgroep 25 september 2012.

In deze brief doe ik verslag van de onderhandelingsronden die in juni, juli en september 2012 hebben plaatsgevonden.

Raadswerkgroep 27 en 28 juni 2012

In deze werkgroep heeft het voorzitterschap een kort verslag gedaan van de onderhandelingen in het kader van de Raad van Europa over de herziening van het op 28 januari 1981 te Straatsburg totstandgekomen verdrag ter bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag no. 108) (Trb. 1988, 7). Verslag is gedaan van de omstandigheid dat de EU en de lidstaten hun standpunten coördineren om het proces voor de totstandkoming van de verordening goed te laten sporen met de modernisering van het verdrag. De Commissie heeft haar zorg uitgesproken over het verschil tussen beide

kst-32761-44
ISSN 0921 - 7371
's-Gravenhage 2012

instrumenten op het gebied van de gevoelige gegevens en de procedures en criteria voor de vaststelling van het niveau van gegevensbescherming in derde landen. Nederland deelt die zorg.

De resterende tijd is geheel besteed aan de bespreking van de Algemene verordening gegevensbescherming.

Er is nader gesproken over de rechtsgrondslag. Zo is de vraag aan de orde gesteld of de verordening niet alleen op artikel 16 VWEU (gegevensbescherming) moet rusten, maar ook op art. 114 VWEU (interne markt). De Commissie is hier van oordeel dat art. 114 VWEU alleen aan de orde komt, voor zover dat noodzakelijk is om enkele technische wijzigingen aan te brengen in richtlijn 2002/58/EG, maar dat alle overige bepalingen berusten op art. 16 VWEU. Nederland kan daarmee instemmen. Verder is gesproken over de verhouding tussen de werkingssfeer van de verordening voor het Schengenacquis en de Europese Economische Ruimte. Deze discussie is voor Nederland hooguit van indirect belang.

Het voorzitterschap heeft melding gemaakt van een brief van de Working Party on Statistics van de EU. Deze Working Party maakt zich zorgen over de beperking van het aantal grondslagen voor de verwerking van persoonsgegevens voor statistische doeleinden, zonder duidelijk aanleiding. Nederland deelt dat standpunt en heeft dat bij de desbetreffende bepalingen (artikelen 9 en 14 tem 21) aan de orde gesteld.

Vervolgens is de artikelsgewijze behandeling voortgezet.

Bij artikel 9, tweede lid, dat betrekking heeft op de rechtvaardigingsgronden voor de verwerking van bijzondere persoonsgegevens heeft Nederland aandacht gevraagd – en deels verkregen – op de volgende punten.
Artikel 9, tweede lid, onder b, geeft rechtvaardigingsgronden voor de verwerking van bijzondere persoonsgegevens in het kader van het arbeidsrecht, indien daarvoor een grondslag bestaat in het Unierecht of dat van de lidstaten. Nederland kent geen afzonderlijk gegevensbeschermingsrecht voor het arbeidsrecht. Desgevraagd is de Commissie van oordeel dat uit deze bepaling geen verplichting voort vloeit deze afzonderlijke regels vast te stellen.
Artikel 9, tweede lid, onder f, gaf aanleiding tot de vraag of het gebruik van bijzondere persoonsgegevens in rechtsgedingen zich ook uitstrekt tot nevengeschillen en bezwaarschriftprocedures. Dit werd beoogd, aldus de Commissie.
Artikel 9, tweede lid, onder h, gaf aanleiding tot het stellen van kritische vragen met betrekking tot de verwerking van gezondheidsgegevens. De verwijzing naar artikel 81 impliceert een beperking van de mogelijkheden daartoe door verzekeraars. In artikel 81 is alleen sprake van verwerking met het doeleinde uitvoering van een ziektekostenverzekering, en niet van andere verzekeringen, zoals schade- en levensverzekeringen. Het is voor de desbetreffende verzekeraars essentieel die gegevens rechtmatig te kunnen verwerken met het oog op claimbeoordeling en fraudepreventie. Ook is de verwerking van strafrechtelijke gegevens door anderen dan partijen in de strafvorderlijke keten uitgesloten. Wat dit laatste betreft, is de verwachting dat de Commissie instemt met terugkeer naar de oude situatie, waarin dit is toegestaan. Wat het eerste punt betreft, blijft er reden tot zorg, omdat de Commissie meent dat de rechtvaardigingsgrond gezocht moet worden in de verzekeringsovereenkomst of toestemming van de betrokkene. Het Nederlandse standpunt is met diezelfde argumenten ook bestreden door andere lidstaten.
Artikel 9, tweede lid, onder j, gaf Nederland aanleiding te herhalen dat de toevoeging van «offences» belangrijk is om een zo breed mogelijk

toepassingsbereik te krijgen van het begrip «strafrechtelijke gegevens». Dat is zowel van belang voor verantwoordelijken die meer gegevens dan alleen strafrechtelijke veroordelingen moeten kunnen verwerken, als in het belang van de betrokkenen. Verdenkingen zijn immers geen veroordelingen en de onschuldspresumptie rechtvaardigt zonder meer een hoger niveau van gegevensbescherming.

Artikel 11 formuleert het accountabilitybeginsel in zeer algemene termen. Een verantwoordelijke moet eigener beweging tonen welke inspanning hij levert voor de bescherming van de onder zijn verantwoordelijkheid uitgeoefende persoonsgegevens. Nederland onderschrijft dit beginsel. Maar Nederland vraagt zich af of het niet erg algemeen is geformuleerd en daardoor teveel verantwoordelijken van zeer verschillende aard zonder goede reden over één kam scheert. De belasting voor het MKB kan immers zeer verstrekkend zijn. Dit gevoelen werd algemeen gedeeld. Het is aanleiding geweest voor een langdurige discussie in de werkgroep over het rechtskarakter van de verordening. Ik verwacht dat dit artikel in een tweede lezing nogmaals nadrukkelijk aan de orde komt.

Artikel 12 geeft algemene bepalingen over de procedures voor het uitoefenen van de rechten door de betrokkene en de manier waarop en termijnen waarbinnen de betrokkene daarop moet reageren. Er is gediscussieerd over nut en noodzaak van deze bepaling en ook over de vraag of de rechten niet altijd langs elektronische weg moeten kunnen worden uitgeoefend, in plaats van dit alleen voorwaardelijk toe te staan. Ook is gediscussieerd over de lengte van de reactietermijn. Nederland meent dat deze bepalingen voor verscherping vatbaar zijn. Wat de verplichting van de verantwoordelijke betreft om de betrokkene in te lichten over bepaalde rechtsmiddelen, is Nederland van oordeel dat dit ver gaat. Verantwoordelijken zijn niet noodzakelijkerwijs juridisch voldoende onderlegd om feilloos de weg naar de juiste rechter te wijzen. Een verwijzing naar het College bescherming persoonsgegevens is – vanzelfsprekend – wel passend.
Het is de intentie van de Commissie de uitoefening van rechten door de betrokkene kosteloos en zoveel mogelijk vormloos te laten plaatsvinden. Nederland wijst op de noodzaak een regeling te treffen voor kennelijk onredelijke verzoeken, niet alleen qua omvang, maar ook qua inhoud, en de mogelijkheid daarvoor een beperkt bedrag in rekening te brengen, net als onder de huidige richtlijn.

Bij artikel 13 heeft Nederland gevraagd om meer duidelijkheid ten aanzien van de afbakening van de kring van personen aan wie mededeling moet worden gedaan van een gehonoreerd verzoek om correctie. De vraag is of het werkelijk uitvoerbaar is voor de verantwoordelijke om ook partijen aan wie door een derde gegevens zijn verstrekt hierbij te verstrekken.

Artikel 14 bevat een van meest belangrijke bepalingen van de verordening, de informatieverplichting van de verantwoordelijke. Nederland steunt deze verplichting. Wel heeft Nederland gevraagd om verduidelijking bij een aantal onderdelen, zoals de positie van de functionaris voor de gegevensbescherming, de vraag of de verplichting impliceert dat voor elke verwerking bewaartermijnen moeten worden vastgesteld, en of vastgestelde bewaartermijnen voor nevengebruik moeten worden meegedeeld. Ook heeft Nederland opgemerkt dat een berekening van de administratieve lasten en nalevingskosten voortvloeiend uit deze omvangrijke bepaling ontbreekt.

Raadswerkgroep 11 en 12 juli 2012

Het aantredende Cypriotische voorzitterschap heeft aangekondigd zes vergaderingen van de raadswerkgroep van telkens twee dagen te agenderen. Tenminste een van de twaalf dagen wordt besteed aan de richtlijn. Daarnaast kondigt het voorzitterschap aan dat – vermoedelijk drie – afzonderlijke vergaderingen worden geagendeerd om over algemene («horizontale») vraagstukken te spreken. Die zullen worden gewijd aan de drie onderwerpen die op de informele JBZ Raad zijn behandeld. De eerste vergadering heeft op 12 oktober 2012 plaatsgevonden. In een volgende verslaglegging zal daaraan aandacht worden besteed. Het betreft geen formele raadswerkgroep, maar een «Friends of the Presidency»-vergadering. Daar vindt geen besluitvorming plaats. Die eerste vergadering zal het onderwerp delegatie van bevoegdheden aan de Commissie betreffen. Het voorzitterschap schort daarmee alle discussies over afzonderlijke delegatiegrondslagen op.

De rest van de vergadering is besteed aan voortzetting van de artikelsgewijze bespreking.

Bij het vervolg van de bespreking over artikel 14, tweede lid, heeft Nederland aandacht gevraagd voor het standpunt dat de betrokkene vooral geïnformeerd moet worden over de gevolgen van een weigering gegevens te verstrekken die verplicht verstrekt moeten worden in verband met de levering van een dienst of een zaak of een overheidsprestatie. Dat leidt immers tot het niet totstandkomen van een contract of overheidsbesluit. Bij vrijwillige verstrekking ligt het anders, want de verantwoordelijke hoort sowieso niet om meer gegevens te vragen dan hij nodig heeft. De Commissie heeft begrip geuit voor dat standpunt.
Bij artikel 14, vijfde lid, vraagt Nederland of geëxpliciteerd kan worden dat op grond van nationaal recht een uitzondering kan worden vastgesteld op de verplichting van de verantwoordelijke de betrokkene te informeren over gegevensverwerking. Daar zou natuurlijk wel een algemeen belang aan ten grondslag gelegd moeten worden. De Commissie lijkt die lezing te bevestigen.
Vele lidstaten, waaronder ook Nederland, achten het noodzakelijk dat de bestaande uitzondering op de informatieplicht voor verwerkingen voor statistische, historische en wetenschappelijke doeleinden wordt gehandhaafd.

Nederland heeft bij de behandeling van het recht op inzage (artikel 15) nadrukkelijk aandacht gevraagd voor een goede afstemming met artikel 14. Doordat de verplichting van de verantwoordelijke de betrokkene voorafgaand te informeren zo is uitgebreid, moet artikel 15 zodanig worden geredigeerd dat de toegevoegde waarde daarvan voor de betrokkene beter voor het voetlicht wordt gebracht. Het eerste lid heeft op precies dezelfde informatiestroom betrekking als artikel 14. De eigenlijke kern van het recht is in artikel 15, tweede lid, neergelegd. Nederland heeft met veel andere lidstaten ook gevraagd naar de consequenties van de keuze voor het zonder beperking in de tijd kunnen uitoefenen van het recht op inzage. In de geldende richtlijn kan het recht met redelijke tussenpozen worden uitgeoefend. Tenslotte heeft Nederland ook bij dit recht bepleit de uitzondering voor de verwerking voor statistische doeleinden te handhaven.

Het recht op correctie (artikel 16) heeft weinig aanleiding gegeven tot uitgebreide gedachtenwisselingen. Nederland heeft erop gewezen dat het recht op correctie ten aanzien van gegevens verwerkt in openbare registers die bij de wet zijn ingesteld in verband met de eisen van het rechtsverkeer afzonderlijke eisen stelt aan wijze van uitoefening ervan. De

identiteitsvaststelling van de betrokkene is van groot belang, aan de motivering moeten eisen kunnen worden gesteld en de mogelijkheid voor een afwijkende lezing van de betrokkene zou mogelijk gemaakt moeten worden. Tenslotte heeft Nederland ook bij dit recht bepleit de uitzondering voor de verwerking voor statistische doeleinden te handhaven.

Zoals kon worden verwacht is het recht om te worden vergeten (artikel 17) aanleiding geweest voor een fundamentele en een zeer langdurige gedachtenwisseling. In een algemene inleiding werden – ook door Nederland – de nodige vragen gesteld over het realiteitsgehalte van hetgeen de verordening belooft. De bepaling is uiterst omvangrijk. De bedoeling is goed, en het recht op wissen en afschermen moeten beslist behouden blijven. Maar de vraag is of de verantwoordelijke in het tijdperk van de sociale media in staat zal zijn te achterhalen bij welke derde zich gegevens bevinden, welke inspanningen hij daartoe redelijkerwijs kan en moet leveren, en wat er van de derde redelijkerwijs kan worden verwacht. De invloed van cloudcomputing en van het recht van derde landen waar gegevens zich kunnen bevinden is een extra complicatie. Ook moet dit recht geen afbreuk doen aan de uitingsvrijheid en de vrijheid informatie te vergaren.
Daarnaast heeft Nederland aangedrongen op verduidelijking van het eerste lid, onderdeel d.
Bij het tweede lid meent Nederland dat de relatie met exceptie voor persoonlijk en huishoudelijk gebruik, en de uitleg die daar door de Commissie aan is gegeven (verspreiding van data aan een onbekend aantal derden valt daarbuiten) verder moet worden doordacht. De vraag is of van een individuele burger die gegevens op internet plaatst, zonder dat hij zich bewust is, of zich redelijkerwijs bewust hoeft te zijn van de consequenties daarvan, kan worden gevergd dat hij allerlei verstrekkende maatregelen neemt. Ook moet de rol van hostingproviders die geen verantwoordelijkheid nemen voor de inhoud van via het platform verspreide gegevens worden verduidelijkt. En ook voor het recht om te worden vergeten geldt dat dit niet in volle omvang kan worden uitgeoefend ten aanzien van in openbare registers die bij de wet zijn ingesteld. Tenslotte heeft Nederland gesuggereerd dat bij deze bepaling proportionaliteitscriteria kunnen worden opgenomen, zoals de aard van de gegevens, wijze van verspreiding en kosten van tenuitvoerlegging.
Ten aanzien van het derde en vierde lid heeft Nederland gevraagd naar de verhouding tussen deze leden. Indien het bedoeling is dat hetzij de betrokkene, hetzij de verantwoordelijke, hetzij beiden de keuze hebben tussen het wissen of alleen afschermen van gegevens moet dit worden verduidelijkt. De Commissie betoogt dat beide rechten inderdaad naast elkaar staan, en dat elke in het vierde lid genoemde grond voor de verantwoordelijke aanleiding kan zijn tot een beperking van de gegevensverwerking of de gegevens te wissen. Verdere verduidelijking acht Nederland nodig bij de mogelijkheid om gegevens ten behoeve van bewijsvoering te bewaren. De vraag is of dat niet ook noodzaakt tot het bewaren ten behoeve van rechtsgedingen.
Ook het vijfde en zesde lid geven aanleiding tot vragen. Bij het vijfde lid is het de vraag of de betrokkene met zijn toestemming voor hervatting van de verwerking – na afscherming – ten behoeve van derden niet zelf een verwerkingsdoel schept. Bij het zesde lid is het de vraag welke zin deze bepaling heeft. Wanneer er immers sprake is van afscherming of beperking van de verwerking ligt het niet in de rede de verwerking, al dan niet geconditioneerd, te hervatten.

Het recht op dataportabiliteit (artikel 18) gaf in het algemeen aanleiding tot één centraal vraagpunt. Ook voor Nederland is het de vraag of dit recht niet zou moeten worden beperkt tot uitsluitend digitale toepassingen, tot de sociale media en de diensten van de informatiemaatschappij.

Daarnaast moet goed worden gelet op de toelaatbaarheid van de mogelijk uit dit recht voortvloeiende beperkingen van het mededingingsrecht of het recht op de intellectuele eigendom.

Raadswerkgroep 3 en 4 september 2012

Het voorzitterschap licht kort de resultaten toe van de informele JBZ-Raad van 23 en 24 juli 2012 van Nicosia. Bevestigd wordt dat de drie horizontale vraagstukken afzonderlijk zullen worden besproken in een «Friends of the Presidency» samenstelling.

De artikelsgewijze bespreking wordt voortgezet.

Ten aanzien van artikel 19 (het recht op verzet) concentreert Nederland zich vooral op de veranderingen die de verordening brengt in verhouding tot het bestaande artikel 14 van de richtlijn. De bewijslast voor de rechtvaardiging van het verzet ligt in de verordening op de verantwoordelijke. Dat is misschien verklaarbaar uit de wens de rechten van de betrokkene te verruimen, maar is moeilijk verenigbaar met de bevoegdheid van de verantwoordelijk zelf de doelstellingen van de verwerking vast te stellen. Verder is dit recht naar zijn aard niet toepasbaar ten aanzien van in openbare registers die bij de wet zijn ingesteld. Tenslotte moet er geen misverstand over bestaan of het recht van verzet tegen direct marketing absoluut of relatief is. De tekst van artikel 19, tweede lid, van de verordening moet in overeenstemming zijn met overweging 57.

De resolutie van de Raad van Europa over profileren heeft de Commissie aanleiding gegeven om het bestaande recht om niet te worden onderworpen aan volledig geautomatiseerde beslissingen die zijn gericht op het door middel van persoonsgegevens in beeld brengen van gedrag, voorkeuren, persoonlijkheid etc. te hernoemen. Artikel 20 refereert dan ook uitdrukkelijk aan profileren. Nederland acht die keuze juist, maar vraagt zich af waarom dan niet de goed bruikbare definitie van profileren uit de resolutie is overgenomen. Wij moeten de resultaten van de inspanningen in Straatsburg niet negeren. Als dit wordt nagelaten blijft artikel 20, tweede lid, dat de toelaatbaarheid van profilering regelt, te onbepaald. De vraag is dan ook of een gesloten lijst van profileringen niet bruikbaarder zou zijn, omdat die meer rechtszekerheid biedt.

Artikel 21 bevat de regeling van de beperkingen en uitzonderingen op de verplichting tot informatieverstrekking van de verantwoordelijke en de catalogus van rechten van de betrokkene.
Nederland is van oordeel dat de bestaande uitzondering voor staatsveiligheid en defensie ook in artikel 21 moet worden opgenomen. Verder is aandacht gevraagd voor de eis dat de mogelijkheid om beperkingen en uitzonderingen in de nationale wetgeving op te nemen, met zich brengt dat die nationale wetgeving gereed moet zijn op het tijdstip waarop de verordening gaat gelden. Het is daarom van groot belang om volstrekte helderheid te krijgen over de eisen die artikel 21, tweede lid, aan die nationale wetgeving stelt. Die eisen zijn nogal zwaar, terwijl de praktijk leert dat nauwelijks voorzienbaar is welke uitzonderingen zich zullen voordoen. Er moet dan ook noodgedwongen met een algemene formulering worden volstaan. Gedetailleerde eisen zullen het leven bemoeilijken. Verder heeft Nederland ook hier aandacht gevraagd over het ontbreken van een, wat Nederland betreft, gerechtvaardigde uitzondering voor statistische verwerkingen.

Artikel 22 is een beginselbepaling die een algemene verplichtingencatalogus voor de verantwoordelijke bevat. De verantwoordelijke dient in het

belang van de bescherming van persoonsgegevens een bepaald beleid te voeren en dit bekend te maken. Daartoe moet hij veel documentatie beschikbaar houden en aan allerlei verplichtingen voldoen.
Nederland is voorstander van het accountabilitybeginsel dat daaraan ten grondslag ligt. Dit beginsel dient volgens Nederland echter niet alleen met dwingende maatregelen te worden afgedwongen, maar ook met stimulerende maatregelen te worden ondersteund. Die laatste benadering wordt gemist. Verder geldt artikel 22 in beginsel in volle omvang voor alle verantwoordelijken, dus ook voor de kleine ondernemer, en zelfs, onder omstandigheden, de individuele burger. Het leidt ook tot een hogere belasting van de toezichthouders. Een risicogerichte benadering zou beter zijn geweest. Weliswaar kan de Commissie uitzonderingen op de verplichtingen toelaten, maar worden behoorlijk onderbouwde criteria daarvoor niet genoemd. Dit is niet aanvaardbaar. Dat is zo belangrijk, omdat naleving van deze bepaling veel kosten genereert. Die kosten zijn door de Commissie niet afzonderlijk berekend. Dat is een gemis. Veel lidstaten hebben dezelfde punten naar voren gebracht. Door een aantal lidstaten, waaronder Nederland, wordt gevraagd die berekening alsnog te verschaffen.
De Commissie lijkt vanwege het beginselkarakter van deze bepaling vooralsnog niet genegen hier veel aan te veranderen. Het valt daarom te verwachten dat de discussie over dit artikel wordt voortgezet.

Het uitgangspunt van «data protection by design and by default» (artikel 23) wordt door Nederland graag onderschreven. Nederland staat daarom positief tegenover deze bepaling. Wel kan die eenvoudiger worden vormgegeven, wanneer goed wordt geïnventariseerd welke verplichtingen in artikel 23, eerste lid, eigenlijk al worden afgedekt door de artikelen 14, 22 en 30. Met de kernbepaling van artikel 23, tweede lid, kan worden ingestemd. Wel verdient de voorziening met betrekking tot het voorkomen van ongericht verspreiden van gegevens nog nader afstemming met het recht op de vrijheid van meningsuiting en het zonder nodeloze grond beperken van het functioneren van sociale mediasites.

Nederland is voorstander van de regeling van de verhouding tussen gezamenlijke verantwoordelijken (artikel 24). Zeker wanneer differentiatie mogelijk is in de vorm van de rechtsverhouding tussen de betrokken verantwoordelijken. Nederland ziet daar veel in voor de publieke sector, zeker wanneer die regeling in concrete gevallen op publiekrechtelijke grondslag bij nationaal wettelijk voorschrift kan worden vastgesteld en de betrokkenen niet in het ongewisse worden gelaten tot welke verantwoordelijke zij zich moeten richten om hun rechten geldend te maken. Voor de private sector verdienen de verhoudingen binnen een concern nadere aandacht, omdat het niet noodzakelijk of wenselijk is daar steeds met contracten te werken. Interne instructies zijn in die verhoudingen ook werkbaar.

De regeling van het aanwijzen van vertegenwoordigers van niet in de EU gevestigde verantwoordelijken voor de verwerking van persoonsgegevens die betrekking hebben op EU-burgers (artikel 25), geeft aanleiding tot vragen. Nederland realiseert zich dat een dergelijke regeling in beginsel nodig is in verband met de territoriale reikwijdte van de verordening, maar wijst erop dat de verplichting nauwelijks handhaafbaar is. Als een verantwoordelijke geen vertegenwoordiger aanstelt, zal de sanctie daarop (een bestuurlijke boete op te leggen door de toezichthouder) niet in het desbetreffende land ten uitvoer kunnen worden gelegd. Het is bovendien de vraag of gegadigden voor deze functie wel kunnen worden gevonden, omdat het bekleden ervan uitsluitend verplichtingen en aansprakelijkheid genereert, en geen enkel aanwijsbaar voordeel. De ervaringen met de huidige regeling in Nederland zijn niet

positief. De Commissie geeft aan niet blind te zijn voor die bezwaren. Het alternatief, niets doen, vergroot volgens de Commissie echter het handhavingstekort.

Nederland steunt graag het voorstel voor een afzonderlijk artikel 26 waarin de positie van de verwerker (in de huidige Wet bescherming persoonsgegeven bewerker genaamd) wordt geregeld. Dat voorziet in een behoefte. Wel moet duidelijk worden welke positie de verwerker precies heeft. Anders dan onder het huidige recht wordt voorgesteld de verwerker expliciet en direct medeverantwoordelijk te maken voor het honoreren van verzoeken om uitoefening van de rechten van de betrokkene.
Nederland vraagt zich af of dit, ook met het oog op de duidelijkheid voor de betrokkene niet beter bij de verantwoordelijke kan worden gelaten.
Nederland is er voorstander van dat de rechtsverhouding tussen verantwoordelijke en verwerker niet alleen op privaatrechtelijke grondslag gestoeld hoeft te worden, zoals nu de perceptie is. Dit kan ook heel goed in algemeen verbindende voorschriften worden geregeld, uiteraard met het oog op de publieke sector. De Commissie heeft hierop met enig begrip gereageerd. Vrij algemeen weerklonk juist bij deze bepaling het gemis aan een expliciete verwijzing naar cloudcomputing en de consequenties daarvan. De Commissie kondigde aan eind september 2012 daarover een beleidsvoornemen vast te stellen.

Artikel 27 regelt de verplichting voor verantwoordelijk en verwerker om er zorg voor te dragen dat al degenen die onder hun verantwoordelijkheid persoonsgegevens verwerken dat uitsluitend op instructies doen, tenzij Unierecht of het recht van de lidstaten anders bepaalt. Nederland acht dit een wat ongebruikelijke bepaling. De bedoeling kan beter in een aansprakelijkheidsregeling of een geheimhoudingsbepaling worden geregeld.

Artikel 28 bevat een verplichting voor de verantwoordelijke om op een groot aantal nader uitgewerkte onderdelen documentatie bij te houden over de onder zijn verantwoordelijkheid verrichte verwerkingen. Deze verplichting komt in plaats van de bestaande verplichting alle verwerkingen te melden bij de toezichthouder, het College bescherming persoonsgegevens.
Nederland heeft aangegeven voorstander van het afschaffen van de meldplicht te zijn, maar bij dit artikel te vrezen voor een toename van de administratieve lasten. De effecten daarvan zijn helaas niet berekend.
Artikel 28, eerste lid, is voor Nederland een principiële zaak. In Nederland is die meldplicht zo opgezet, dat er ter vermijding van een vloed aan meldingen en ter beperking van de administratieve lasten een vrijstellingsregeling is vastgesteld. Er hoeft niet te worden gemeld wanneer het betreft een bij algemene maatregel van bestuur aangewezen type van verwerking betreft waarbij een inbreuk op de fundamentele rechten van de betrokkene onwaarschijnlijk is.
Het gaat daarbij om zeer veel voorkomende verwerkingen van eenvoudig karakter. Ledenadministraties van verenigingen, salarisadministraties van bedrijven en vergunningenadministraties van gemeenten, bijvoorbeeld.
Weliswaar geeft artikel 28, vierde lid, wel weer dat ook de Commissie openstaat voor beperking van de documentatieplicht, maar los van concrete formulering is dit punt zo belangrijk dat een beperking van de documentatieplicht in artikel 28, eerste lid, zou moeten worden verankerd. Dat kan ook op een verantwoorde manier gebeuren, want het instrument van de Privacy Impact Assessment is daar bij uitstek geschikt voor.
Nederland zal nog met een aantal concrete tekstvoorstellen komen.
Bovendien moet voorkomen worden dat de regeling meer belooft dan kan worden waargemaakt: 100% naleving is onmogelijk, zo leert de praktijk.

Nederland heeft op 20 september 2012 een lijst van schriftelijke voorstellen gebaseerd op bovenstaande standpuntbepalingen aan het Raadssecretariaat gezonden.

Het Voorzitterschap heeft besloten 25 september 2012 te wijden aan voortzetting van de behandeling van de verordening, en 26 september 2012 aan voortzetting van de behandeling van de richtlijn.

Raadswerkgroep 25 september 2012

De behandeling van artikel 28 is voortgezet. Daarbij bleek dat de bezwaren die Nederland ziet tegen artikel 28 door verschillende lidstaten worden herkend.
Ten aanzien van artikel 28, tweede lid, heeft Nederland herhaald dat een risicogerichte benadering moet leiden tot de mogelijkheid om te differentiëren in verplichtingen tot het bijhouden van documentatie. Niet elke verantwoordelijk hoeft deze verplichtingen in volle omvang te dragen.
Artikel 28, derde lid, zou uit wetssystematisch oogpunt ook bij de bevoegdheden voor de toezichthouder kunnen worden geregeld.
Over artikel 28, vierde lid, is door Nederland op reeds 4 september 2012 in algemene zin gesproken. Specifiek over onderdeel a van het vierde lid, verdient het aanbeveling expliciet te verwijzen naar artikel 2, tweede lid, onder d.

Artikel 29 regelt dat de verantwoordelijke gehouden is tot samenwerking met de toezichthouder. Het is de vraag of die bepaling systematisch op de juiste plaats staat. En het is ook de vraag of die samenwerking alleen bestaat in gevallen waarin de toezichthouder verzoekt om samenwerking. Nederland heeft naar voren gebracht dat het hier gaat om de uitoefening van overheidsbevoegdheden. Een medewerkingsplicht kan beter zonder die clausule worden geformuleerd.

Artikel 30 (de beveiligingsplicht) is in het raamwerk van de verordening een bijzonder belangrijke bepaling. Nederland is voorstander van een duidelijk omschreven verplichting terzake. Met het voorstel kan op hoofdlijnen zeker worden ingestemd. Maar er blijven wel vragen over de uitwerking van de bepaling. Nederland is met veel andere lidstaten van oordeel dat de effecten van cloudcomputing onvoldoende zijn toegelicht. Dat lijkt met name voor de handhaving van belang. De bepaling richt zich immers tot de verantwoordelijke en bewerker gelijkelijk. Wanneer de bewerker zich in een derde land bevindt kan die verplichting niet worden gehandhaafd, omdat de Europese toezichthouders daar niet bevoegd zijn. Het lijkt dan ook verstandig om de verantwoordelijke te verplichten in contractsvoorwaarden expliciete beveiligingsverplichtingen op te nemen, zodat die verplichtingen in ieder geval langs privaatrechtelijke weg kunnen worden gehandhaafd. Nederland is er verder voorstander van om de aanzetten voor een risicogerichte benadering van beveiligingsvraagstukken in artikel 30 beter uit te werken, en een expliciete verwijzing naar artikel 33 op te nemen.

In de artikelen 31 en 32 van de verordening is de meldplicht datalekken geregeld. Nederland is daar uitgebreid op ingegaan. Nederland is het eens met de Commissie dat de verordening een regeling over een meldplicht voor datalekken moet bevatten. Toegelicht is dat in Nederland wordt gewerkt aan een eigen wetsvoorstel voor de meldplicht datalekken. Dat wetsvoorstel is genotificeerd aan de Commissie, zodat de Commissie en de lidstaten daarvan kunnen kennisnemen.
Noch in artikel 4, onder (9), noch in artikel 31 of 32, is een duidelijk doel van de meldplicht neergelegd. Wel valt in overweging 67 te lezen dat «aanzienlijk economisch verlies, of maatschappelijke schade, met inbegrip

van identiteitsfraude voor het betrokken individu» voorkomen moet worden. Daar is Nederland het zeker mee eens, maar de vraag is of het niet verstandig is dat vast te leggen in de verordening.
Bij de behandeling van artikel 4, onder (9), is Nederland al ingegaan op het belangrijkste punt. De meldplicht van artikel 31 lijkt absoluut van aard te zijn. Elk geconstateerd beveiligingslek moet worden gemeld. Artikel 31, derde lid, onder c, lijkt alleen te impliceren dat wanneer er geen mogelijke nadelige effecten voor persoonsgegevens te duchten zijn geen aanbevelingen voor door de betrokkene te treffen maatregelen hoeven te worden gedaan.
Nederland denkt niet dat het verstandig is de meldplicht zo breed te omschrijven. Dit is onredelijk belastend voor verantwoordelijken, en voor toezichthouders. Het leidt bovendien tot een snelle maatschappelijke afwaardering van de effectiviteit van deze verplichting.
Een beperking van de meldplicht, vooral met het doel om een overvloed aan bagatelzaken te vermijden, is naar Nederland meent daarom nauwelijks ontkoombaar. Een redelijke beperking van de meldplicht kan op verschillende wijze worden bereikt. De meldplicht kan zich beperken tot specifek aangewezen risico's. De meldplicht kan ook met een algemene formulering worden beperkt. Die keuze is in Nederland vooralsnog gemaakt. Natuurlijk hebben beide varianten voor- en nadelen. Maar is toch wel verstandig iets te kiezen om de nadelen van het achterwege laten van iedere keuze te voorkomen.
De Commissie heeft bij de bespreking van artikel 4, onder (9), al verwezen naar de meldplicht in de e-Privacyrichtlijn (2002/58/EG). Dat acht Nederland verklaarbaar uit oogpunt van consistentie, maar toch minder goed vanuit de aard van de materie. De e-privacyrichtlijn is gericht tot een specifieke categorie verantwoordelijken. Van die categorie kan Nederland wel aanvaarden dat elke verwerking een zodanig risico voor de bescherming van persoonsgegevens oplevert, dat een algemeen geldende meldplicht acceptabel is. Dat risico is niet zonder meer aanwezig bij alle andere vormen van gegevensverwerking die niet specifiek door de e-privacyrichtlijn worden bestreken. Nederland stelt vervolgens aan de orde hoe zinvol de 24-uurstermijn van artikel 31 is. Het is zeker denkbaar dat 24 uur niet voldoende zijn om een goed overzicht te krijgen van alle aspecten van het datalek. De melding kan dan niet alle onderdelen van het tweede lid beslaan. Het is dan misschien onvermijdelijk de melding in meer fasen te laten plaatsvinden.
Vervolgens komt de vraag aan de orde welke toezichthouder bevoegd is een melding in ontvangst te nemen wanneer sprake is van gezamenlijke verantwoordelijkheid in de zin van artikel 24 die meer dan één lidstaat betreft. De vraag is dan of elke verantwoordelijke aan de toezichthouder in zijn eigen lidstaat moet melden. De vraag is ook of dit in concernverhoudingen (een «group of undertakings») kan worden overgelaten aan één onderdeel namens het hele concern, of dat dit de «main establishment» (hoofdvestiging) moet zijn.
Wat artikel 32, derde lid, betreft vraagt Nederland zich af of het verstandig is de toezichthouder een rol te geven bij beoordeling van de door de verantwoordelijke getroffen beveiligingsmaatregelen. Als de toezichthouder daar een rol krijgt, komt het erop neer dat deze een bepaalde medeverantwoordelijkheid krijgt voor het beveiligingsbeleid van de verantwoordelijke. De rollen van toezichthouder en verantwoordelijke worden dan niet goed onderscheiden. Bovendien kan onder omstandigheden een succesvol beroep op de openbaarheidswetgeving in de betrokken lidstaat leiden tot een verlaagde bescherming van bedrijfsgeheimen.

Artikel 33 bevat de verplichting om onder bepaalde voorwaarden een Privacy Impact Assessment (PIA) te houden. Nederland steunt deze verplichting. Het is terecht dat deze verplichting een afzonderlijke plaats in

de verordening verdient. Nederland meent dat de betekenis van de PIA nog kan toenemen wanneer deze kan worden gebruikt bij de vaststelling van het risiconiveau dat bepalend moet zijn voor de mate waarin bepaalde verplichtingen moeten worden opgelegd. Te denken valt aan aanstelling van een Data Protection Officer, de omvang van de documentatieplicht en het opleggen van een meldplicht voor datalekken. Dat moet in samenhang worden bezien met de toepassing van andere maatregelen met een zelfregulerend karakter, als certificering en gedragscodes.
Nederland heeft zich verder afgevraagd of het criterium «specifiek risico» voldoende onderscheidend is om de verplichting tot het houden van een PIA af te bakenen. Elke verwerking heeft immers een specifiek risico, groot of klein. Een hoog risico is dan een beter alternatief. Dat moet dan worden bezien in verband met artikel 33, tweede lid.
Artikel 33, tweede lid, onder b, geeft aanleiding tot de vraag of elke patiëntenadministratie nu aanleiding is voor het houden van een PIA. Dit zijn algemeen voorkomende verwerkingen van gezondheidsgegevens waarvan iedere patiënt weet dat hij erin voorkomt. Er zijn bovendien nationale wettelijke waarborgen voor de zorgsector.
Nederland heeft bezwaar gemaakt tegen artikel 33, tweede lid, onder c. Dat schrijft een PIA voor wanneer er sprake is van bewaking van openbaar toegankelijke ruimten, met name wanneer op grote schaal optisch-elektronische apparatuur wordt gebruikt. Het gaat hier om bewakingscamera's. Nederland vraagt zich af waarom dat nodig zou zijn. Het gebruik van bewakingscamera's voor het toezicht op de openbare weg of op anderszins voor het publiek toegankelijke plaatsen is al sinds de jaren «70 van de vorige eeuw een ingeburgerde maatregel. Zolang dit cameratoezicht duidelijk zichtbaar en kenbaar is gemaakt, is dat vanuit privacyoogpunt geen bijzonder risicovolle verwerking. Er zijn bovendien wettelijke waarborgen en er is toezicht op. Op de openbare weg en op voor het publiek toegankelijke plaatsen bestaat geen redelijke verwachting van eenieder dat hij of zij volkomen onbevangen zichzelf kan zijn. In Nederland is dat al sinds vele jaren vaste jurisprudentie van de hoogste rechter.
Nederland heeft navraag gedaan naar de bedoeling van artikel 33, vijfde lid. De ontheffing van de verplichting tot het houden van een PIA voor overheidsverwerkingen moet volgens Nederland niet alleen krachtens EU-recht, maar ook krachtens nationaal recht mogelijk zijn. Overweging 73 wijst daar toch op. Dit standpunt werd ook door veel andere lidstaten ingenomen. De Commissie heeft daarop gesuggereerd dat overweging 73 en artikel 33, vijfde lid, beter met elkaar in overeenstemming moeten worden gebracht.

Raadswerkgroep 26 september 2012

In de raadswerkgroep van 26 september is de artikelsgewijze bespreking van het voorstel voor de richtlijn voortgezet. Daarbij zijn de artikelen 5 tot en met 8 aan de orde gekomen.

Voor wat betreft artikel 5 heeft Nederland zich kritisch uitgelaten over de verplichting van artikel 5 om, voor zover mogelijk, onderscheid te maken tussen verschillende categorieën van betrokkenen. Tijdens een opsporingsonderzoek kan de status van een persoon eenvoudig veranderen, een dergelijke verplichting zal kunnen leiden tot aanzienlijke administratieve lasten voor de opsporingsinstanties, zonder dat aan dit onderscheid rechtsgevolgen zijn verbonden. Ook moet rekening moet worden gehouden met de noodzaak tot aanpassing van de informatiesystemen. Hieraan kunnen aanzienlijke kosten zijn verbonden, dit laat zich thans nog niet goed overzien. Gevraagd wordt naar de achterliggende reden voor dit voorstel en de toegevoegde waarde van deze verplichting voor de betrokkene. De Commissie heeft aangegeven dat de heeft als doel om de

persoonsgegevens zo goed mogelijk te beschermen. De passage «voor zover mogelijk» geeft voldoende armslag bij het inrichten van de systemen. De ernst van de interventie kan dan afhangen van de status van de persoon. Het gaat er namelijk om dat iedere categorie eigen rechtsgevolgen krijgt, bijvoorbeeld de autorisatie voor het inzien van persoonsgegevens en een bewaartermijn. De Commissie hecht aan de opgenomen categorieën, maar staat open voor verbeteringen.

Eenzelfde standpunt heeft Nederland ingenomen ten aanzien van de in artikel 6 opgenomen verplichting om, voor zover mogelijk, onderscheid te maken naar de graad van juistheid en betrouwbaarheid van persoonsgegevens en gegevens die op feiten zijn gebaseerd te onderscheiden van gegevens die op een persoonlijk oordeel zijn gebaseerd. Daarbij heeft de Nederlandse delegatie gewezen op het nationale systeem voor de classificatie van criminele inlichtingen, dat binnen de Nederlandse politie wordt gebruikt ten behoeve van de afscherming van dergelijke gegevens. Voor het vertrouwen tussen de lidstaten bij de uitwisseling van gegevens kan het van groot belang zijn dat duidelijkheid bestaat over de verdere verwerking van gevoelige opsporingsgegevens in de ontvangende lidstaat, inclusief de kring van personen die toegang hebben tot de verstrekte gegevens. Het huidige voorstel bevat echter geen regels over de verdere verwerking van de verstrekte gegevens door de ontvangende lidstaat en de toegang daartoe. Daarbij zou ook bekeken kunnen worden of de toegang tot de gegevens kan worden beperkt door middel van een systeem van autorisaties. De Commissie heeft aangegeven dat dit voorstel is ontleend aan Aanbeveling R (87) 15 van de Raad van Europa (art. 3, tweede lid). Het onderscheid tussen harde en zachte informatie kan van belang zijn voor de uitwisseling van gegevens aan derden. De Commissie zal nader kijken naar de wenselijkheid van regels voor de verstrekking van persoonsgegevens aan derden.

Naar aanleiding van de regels over de rechtmatigheid van de verwerking in artikel 7 heeft Nederland erop gewezen dat de politie niet alleen is belast met de opsporing van strafbare feiten, als onderdeel van de strafrechtelijke handhaving van de rechtsorde, maar ook met de handhaving van de openbare orde en de hulpverlening. Laatstgenoemde taken vallen echter niet onder de reikwijdte van de ontwerprichtlijn maar onder de ontwerpverordening. Op basis van de tekst van de onderdelen c en d kan er echter verwarring ontstaan over de toepasselijkheid van de ontwerprichtlijn. Verder heeft Nederland de vraag opgeworpen of de verwerking van persoonsgegevens met het oog op het opstellen van statistieken over gepleegde strafbare feiten of strategische analyses onder de reikwijdte van de ontwerprichtlijn dan wel de ontwerpverordening valt. Tenslotte heeft Nederland gevraagd of er aanleiding bestaat ook regels op te nemen over de onverenigbare verwerking van persoonsgegevens, naar het model van de ontwerpverordening. De Commissie heeft aangegeven de reikwijdte van de ontwerprichtlijn te zullen verhelderen, in het bijzonder ten aanzien van de verhouding met bestuursrechtelijk optreden en de gegevensverwerking ten behoeve van statistische doelen.

Inzake de in artikel 8 neergelegde regels over de verwerking van bijzondere categorieën van persoonsgegevens (ras, etnische afkomst, politieke opvattingen e.d.) heeft Nederland gevraagd naar de betekenis van het tweede lid, onderdeel c. Het verbod op de verwerking van dergelijke gegevens is namelijk niet van toepassing als de verwerking betrekking heeft op gegevens die kennelijk door de betrokkene openbaar zijn gemaakt. Het lijkt niet wenselijk dat de bescherming van gevoelige persoonsgegevens niet van toepassing zou zijn op grond van gedragingen van de betrokkene zelf. Verder heeft de Nederlandse delegatie erop gewezen dat in het huidige kaderbesluit dataprotectie wordt uitgegaan

van het criterium van de strikte noodzaak, en bepleit aan te sluiten bij de meer restrictieve benadering van het kaderbesluit. Tenslotte heeft de Nederlandse delegatie gepleit voor een duidelijke koppeling van de ontheffing van het verbod op de verwerking van gevoelige persoonsgegevens aan de uitvoering van de rechtmatige taak door de bevoegde autoriteit. De Commissie heeft aangegeven dat onderdeel c van het tweede lid is ontleend aan de Privacyrichtlijn van 1995 (art. 8, tweede lid, richtlijn 95/46/EG). Er zijn overigens geen concrete voorbeelden bekend van de toepassing van dit onderdeel. Het absolute verbod van het eerste lid dekt het criterium van de strikte noodzaak af.

De staatssecretaris van Veiligheid en Justitie,
F. Teeven