

## **Fiche 2: Mededeling bescherming persoonsgegevens**

### **1. Algemene gegevens**

#### ***Titel voorstel***

Mededeling van de Commissie aan het Europees Parlement, de Raad, Het Europees Economisch en Sociaal Comité en het Comité van de Regio's: 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie'

#### ***Datum Commissiedocument***

4 november 2010

#### ***Nr. Commissiedocument***

COM (2010) 609

#### ***Pre-lex***

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:NL:PDF>

#### ***Nr. impact assessment Commissie en Opinie Impact-assessment Board***

Niet opgesteld

#### ***Behandelingstraject Raad:***

Raadswerkgroep DAPIX, JBZ-Raad

#### ***Eerstverantwoordelijk ministerie***

Ministerie van Veiligheid en Justitie

### **2. Essentie voorstel**

De Commissie heeft een mededeling uitgebracht waarin kaders worden geschetst voor een herziening van de privacyrichtlijn (richtlijn nr. 95/46/EG). De herziening is ingegeven door de voortschrijdende technische ontwikkelingen. Volgens de Commissie zijn de grondslagen van de richtlijn nog altijd geldig en zou het technologie-neutrale karakter ervan bewaard moeten blijven. Niettemin zijn er enkele onderwerpen die een uitdaging vormen. Dit betreft:

- de omgang met de gevolgen van nieuwe technologieën;
- de noodzaak tot uitwerking van de internemarktdimensie;
- verbetering van de mogelijkheden voor internationale gegevensdoorgifte;
- effectievere handhaving van het gegevensbeschermingsrecht;
- meer samenhang in het totale wettelijke kader.

In de mededeling worden deze uitdagingen nader uitgewerkt. Dit brengt de Commissie tot voorstellen op het gebied van de verbetering van de rechten van personen, verbetering van de dimensie van de interne markt, de globale betekenis van gegevensbescherming en een steviger institutioneel kader voor de handhaving van de gegevensbeschermingswetgeving. Ook zal de herziening van de regels voor de bescherming van persoonsgegevens bij de politieke en justitiële samenwerking in strafzaken tussen de lidstaten van kaderbesluit nr. 2008/977/JBZ hierin worden betrokken.

De Commissie kondigt voor medio 2011 een uitgewerkt voorstel aan tot herziening van het wettelijk kader voor gegevensbescherming in de EU.

**3. Kondigt de Commissie acties, maatregelen of concrete wet- en regelgeving aan voor de toekomst? Zo ja, hoe luidt dan het voorlopige Nederlandse oordeel over bevoegdheidsvaststelling, subsidiariteit en proportionaliteit en hoe schat Nederland de financiële gevolgen in?**

De Commissie kondigt voor 2011 wetgevingsvoorstellen aan. Bevoegdheidsvaststelling is gebaseerd op art. 16 VWEU. Nederland acht dit de juiste rechtsgrondslag.

*Subsidiariteit:* Het is nog niet duidelijk hoe de Commissie het EU-optreden precies vorm wil geven, maar over het algemeen beoordeelt Nederland de subsidiariteit van EU-regelgeving inzake de bescherming van persoonsgegevens positief. Voor de verwerking van persoonsgegevens door EU-instellingen en door lidstaten, als ze activiteiten verrichten die binnen het toepassingsbereik van het EU-recht vallen, is een aanpak op EU-niveau noodzakelijk.

*Proportionaliteit:* Ook hierover kan, bij gebrek aan duidelijkheid over de inhoud en de keuze van de vorm van het nieuwe rechtsinstrument, nog geen uitsluitel worden gegeven. Hierbij is van belang of een nieuw instrument dezelfde ruimte aan beleids marge laat als onder de bestaande richtlijn (95/46) het geval is en of ook de gegevensbescherming in het kader van de politieke en justitiële samenwerking, thans geregeld in kaderbesluit 2008/977/JBZ, onderdeel zal vormen van het aangekondigde nieuwe rechtsinstrument.

*Financiële gevolgen:* afgewacht moet worden in hoeverre het voorstel voor een herziening van het wettelijk kader voor de gegevensbescherming financiële consequenties heeft. Het lijkt thans echter niet waarschijnlijk dat er directe consequenties zijn voor de rijksbegroting of de begrotingen van de decentrale overheden. In paragraaf 2.1.4 van de mededeling worden bij wijze van flankerend beleid suggesties gedaan voor bewustwordingscampagnes. De Commissie zal onderzoeken of daarvoor medefinanciering uit de EU-begroting kan plaatsvinden. Nagegaan wordt ook of op de lidstaten een verplichting kan worden gelegd om bewustwordingscampagnes te houden. Nederland is geen voorstander van het verplicht voorschrijven van deze campagnes. Hier zullen zeker financiële gevolgen uit voortvloeien. Onbekend is nog hoe groot die gevolgen zouden zijn. Eventuele nationale financiële gevolgen dienen te worden ingepast op de begroting van de beleidsverantwoordelijke departementen conform de gangbare regels budgetdiscipline.

**4. Nederlandse positie over de mededeling**

Het kabinet wijst allereerst op de erkenning van het belang van privacybescherming in het regeerakkoord. Het kabinet staat dan ook positief ten opzichte van het initiatief van de Commissie om te komen tot een herziening van de privacyrichtlijn in het licht van de voortschrijdende technische ontwikkelingen. Het kabinet is het eens met de Commissie dat de hoofddoelstellingen van de richtlijn behouden moeten blijven. Op hoofdlijnen kan de analyse van de problemen met de richtlijn door de Europese Commissie worden onderschreven. Wel plaatst het kabinet aantekeningen bij enkele onderdelen van de bekendmaking. Deze aante-

keningen komen hierna, gezien het belang van de bescherming van persoonsgegevens, uitvoerig aan de orde.

Het kabinet streeft ernaar binnenkort in een aan de Kamer toegezegde brief een nadere visie op privacy te presenteren. In die brief zal worden ingegaan op de verhouding tussen de in het regeerakkoord in het vooruitzicht gestelde maatregelen ter verbetering van de privacy en komende ontwikkelingen in Europees verband.

## **Het kabinet plaatst aantekening bij de navolgende paragrafen van de mededeling.**

### **2.1 Versterking van de rechten van individuen**

#### *2.1.1 In alle omstandigheden individuen een passende bescherming verzekeren*

Het begrip "persoonsgegevens" is een van de centrale begrippen in de EU-privacyrichtlijn. Wanneer sprake is van een persoonsgegeven, kunnen individuen aan bestaande EU-instrumenten aanspraak maken op de bescherming van die gegevens, onder meer omdat die instrumenten de voor de verwerking verantwoordelijken bepaalde verplichtingen opleggen. De betrekkelijk open en technologie-neutraal geformuleerde omschrijving van dat begrip heeft het voordeel van flexibiliteit. Nadeel hiervan is dat de precieze reikwijdte van dit begrip niet altijd duidelijk is. De Commissie wil nader onderzoeken welke consequenties aan de toepassing van dit begrip moeten worden verbonden in situaties die voortvloeien uit nieuwe technologieën.

- Het kabinet is van oordeel dat niet slechts het begrip "persoonsgegeven", maar alle centrale begrippen van de richtlijn gestructureerd op bruikbaarheid voor de toekomst moeten worden onderzocht. Zo zal het bijvoorbeeld noodzakelijk zijn duidelijker af te bakenen of e-mailadressen en IP-adressen moeten worden aangemerkt als persoonsgegeven. Een meer fundamentele herziening betekent ook dat de begrippen "verantwoordelijke", "verwerker" en "verwerken van persoonsgegevens" in de herziening moeten worden betrokken. Ook is het van belang de werking van deze begrippen in concernverhoudingen nader te beoordelen. Zo is het als gevolg van het veelvuldig uitbesteden van de verwerking van persoonsgegevens naar andere EU-lidstaten of naar derde landen vooral voor betrokkenen in de desbetreffende landen moeilijk te begrijpen dat zij zich voor de uitoefening van de hen toegekende rechten op inzage, correctie en verzet moeten wenden tot een verantwoordelijke in een ander land. De consequenties voor de internationale dimensie van gegevensbescherming dienen bij die herziening te worden betrokken.

#### *2.1.2 Grotere transparantie voor de betrokkenen*

De Commissie stelt vast dat het essentieel is dat de betrokkenen door de voor de gegevensverwerking verantwoordelijke goed en duidelijk worden geïnformeerd over hoe en door wie hun persoonsgegevens worden verwerkt, voor welke redenen, voor welke termijn en welke rechten de betrokkenen hebben. Dit geldt in het bijzonder voor kinderen, omdat zij zich minder bewust zijn van de risico's en de rechten in verband met de verwerking van hun persoonsgegevens. De Commissie overweegt opnemings in het wettelijk kader van een algemeen beginsel van transparante verwerking van persoonsgegevens, van specifieke verplichtingen voor verantwoordelijken over te verstrekken informatie bij specifieke vormen van gegevensverwerking, en de ontwikkeling van EU-standaardmodellen daarvoor ("privacy information

notices"). Verder denkt de Commissie aan het voorschrijven van een algemene meldplicht voor gevallen van doorbreking van beveiligingsmaatregelen voor de bescherming van persoonsgegevens.

- Het kabinet is van mening dat er geen noodzaak is de algemene formulering van de transparantieverplichting (artikelen 10 en 11 van de richtlijn en 33 en 34 van de Wbp) te herzien. Wel is het kabinet voorstander van specifieke transparantieverplichtingen voor het *profilen* en gedragsgericht adverteren. Een EU-brede standaardverklaring kan zinvol zijn. In het kader van de verwerking van passagiersgegevens zijn daarvoor reeds nuttige modellen ontwikkeld.
- Wat de bescherming van jeugdigen betreft, is het verstandig eerst initiatieven af te wachten. De Commissie is nog weinig uitgesproken. Het is enerzijds zinvol om vooral de positie van jongere kinderen aandacht te geven, maar anderzijds moet gewaakt worden voor de neiging om voorschriften te formuleren die niet goed aansluiten op de huidige maatschappelijke ontwikkelingen. De te kiezen leeftijdsgrens moet corresponderen met de realiteit van het zelfstandig functioneren van jongeren op internet. De Wbp hanteert voor het zelfstandig functioneren van betrokkenen in het dataproctierecht een leeftijdsgrens van 16 jaar.
- De uitbreiding van de meldplicht voor doorbrekingen van beveiligingsmaatregelen kan zonder meer worden gesteund. Terzake bereidt het kabinet reeds wetgeving voor.

### 2.1.3 Grotere zeggenschap over de eigen gegevens

De Commissie wil het beginsel van gegevensminimalisatie (zo min mogelijk gegevens verwerken voor het beoogde doel) versterken. De voorwaarden waaronder de rechten van inzage, correctie en verzet kunnen worden uitgeoefend zouden moeten worden verbeterd. Gedacht wordt aan verplichtende reactietermijnen, uitoefening van rechten langs elektronische weg en kosteloze uitoefening van het recht op inzage.

Een recht om te worden vergeten (dat neerkomt op het verplicht wissen van persoonsgegevens na afloop van een bewaartermijn of na het intrekken van de toestemming voor die verwerking door de betrokkene) zou de Commissie willen expliciteren. Verder zou gegevensportabiliteit (recht om eigen gegevens van de ene naar de andere dienstverlener over te dragen) kunnen worden geïntroduceerd.

- Het kabinet is van oordeel dat het beginsel van dataminimalisatie in de wetgeving reeds voldoende duidelijk is verankerd. Wel zou het goed zijn om de onderlinge verhouding tussen de beginselen van doelbinding en dataminimalisatie uiteen te zetten. De voorwaarden voor de uitoefening van de rechten van inzage, correctie en verzet behoeven op zichzelf genomen geen herziening. Kostenloze uitoefening van het recht van inzage vereist wetswijziging. Dat lijkt weinig bezwaarlijk. Het Rijk brengt in de regel geen kosten in rekening voor het voldoen aan verzoeken om inzage.
- Het recht om te worden vergeten roept vragen op. Dit recht bestaat in zekere zin al, omdat uit het intrekken van een gegeven toestemming of het verstrijken van een bewaartermijn toch al voortvloeit dat persoonsgegevens niet langer mogen worden verwerkt. Het kabinet meent dan ook dat primair moet worden ingezet op ondersteuning van die mogelijkheden. Daarnaast roept het de vraag op hoe het recht om te worden vergeten moet worden geëffectueerd ten opzichte van derden die per-

soonsgegevens eerder rechtmatig hebben verwerkt, zeker als daar nog een grensoverschrijdend effect aan is verbonden.

- Een recht op gegevensportabiliteit lijkt zonder kostenverhaal in ieder geval in de private sector niet eenvoudig uitvoerbaar. Het vergt bij de exploitanten van sociale netwerksites vermoedelijk ICT-investeringen. Deze exploitanten bevinden zich bovendien dikwijls buiten de EU.

#### *2.1.4 Bewustmaking*

De Commissie neemt waar dat de burgers in de EU zich onvoldoende bewust zijn van de manier waarop met hun gegevens wordt omgegaan. Zij wil medefinanciering van bewustwordingscampagnes uit de EU-begroting bevorderen en overweegt een wettelijke verplichting tot het opzetten van deze campagnes.

- Het kabinet onderkent dat ook in Nederland sprake is van een relatief gering privacybewustzijn en een nalevingtekort. Dat blijkt uit de evaluatie van de Wbp. Tegen bewustwordingscampagnes op Europees en nationaal niveau bestaat op zich geen bezwaar. In Nederland zijn door het ministerie van Veiligheid en Justitie al enkele succesvolle campagnes gehouden. Aan een wettelijke verplichting daartoe bestaat echter geen behoefte.

#### *2.1.5 Zorgen voor geïnformeerde en vrije toestemming*

De Commissie constateert dat de vereisten voor toestemming in de wetgeving en de praktijk van de lidstaten uiteenlopen. Bovendien blijkt het geven en intrekken van toestemming in een online-omgeving afhankelijk te zijn van instellingen van internetbrowsers.

- Het opnieuw bezien van de vereisten voor een rechtsgeldige toestemming zou deel moeten uitmaken van een meer fundamentele herbezinning op het begrippenapparaat van de richtlijn. Van exploitanten van internetbrowsers mag gerichte aandacht worden verwacht voor de wijze waarop toestemming wordt gevraagd en verleend.

#### *2.1.6 Corrigerende maatregelen en doeltreffender sancties*

De Commissie wil nagaan of collectiefbelangacties, zogeheten "class actions", een versterking kunnen opleveren van de positie van de betrokkene. Daarmee wordt bedoeld dat de dataproductietoezichthouders of collectiefbelangorganisaties namens een groep betrokkenen of burgers een rechtsvordering bij de rechter kunnen instellen, die specifiek gericht is op de handhaving van het gegevensbeschermingsrecht. Verder wordt nagegaan of het sanctie-instrumentarium van de dataproductietoezichthouders voldoet. Zo nodig kan worden voorgeschreven dat moet worden voorzien in strafsancities.

- Het kabinet meent dat "class actions" (collectiefbelangacties) een nuttige aanvulling van de rechten van betrokkenen kunnen vormen. Nederland kent in de artikelen 3:305a en 3:305b van het Burgerlijk Wetboek al een algemene regeling van bepaalde rechtsvorderingen voor collectieve belangen. De "class actions" die de Commissie in gedachten heeft zouden met name kunnen worden benut voor de gevallen waarin er tussen meer betrokkenen en een verwerker van persoonsgegevens een relatie bestaat die een beslissing om de gang naar de privacytoezichthouder of naar de rechter te maken kan beïnvloeden. Te denken valt aan de collectieve behartiging van de belangen van consumenten, werknemers en patiënten. Er moet echter wel aan een aantal voorwaarden worden voldaan. Voorkomen moet worden

dat deze "class actions" leiden tot een claimcultuur. Nederland is daarom geen voorstander van "class actions" die zijn gericht op het vorderen van schadevergoeding in geld. Deze acties zouden dan gericht kunnen zijn op het collectief inroepen van de andere rechten die de richtlijn toekent, of het vorderen van een verklaring voor recht. Verder geldt dat de collectiefbelangactie die wordt ingeleid door een privacytoezichthouder een behoorlijke legitimiteit in maatschappelijk opzicht moet hebben. In Nederland is het College bescherming persoonsgegevens een bestuursorgaan dat immers primair het algemeen belang dient. Ook overigens moet nog het nodige worden onderzocht. Zo verdient de regeling van de kosten van dergelijke procedures aandacht. Hetzelfde geldt voor een behoorlijke inbedding van de actie in het burgerlijk procesrecht.

- Het ministerie van Veiligheid en Justitie bereidt reeds wetgeving voor ter versterking van het sanctie-instrumentarium van het Cbp.

### *2.1.7 Bescherming van gevoelige gegevens*

De Commissie wil nagaan of de huidige opsomming van gevoelige gegevens in de richtlijn volstaat en of er voldoende duidelijkheid bestaat over de voorwaarden waaronder deze kunnen worden verwerkt. De Commissie denkt aan een verduidelijking van de positie van DNA-gegevens.

- Hoewel DNA-gegevens op het niveau van de richtlijn reeds beschermd zijn via gezondheidsgegevens, geeft de ontwikkeling van de wetenschap en de techniek naar het oordeel van het kabinet voldoende aanleiding om voor DNA-gegevens en andere biometrische gegevens een afzonderlijk gegevensbeschermingsregime te overwegen. Deze gegevens worden immers op steeds bredere schaal toegepast voor identificatiedoeleinden, in de strafvordering en de strafrechtstoepassing en in de medische en biologische wetenschap. Met de toename van het gebruik neemt ook de behoefte toe de samenleving te beschermen tegen mogelijk misbruik van deze gegevens.

## **2.2 Uitwerking van de internemarktdimensie**

### *2.2.1 Vergroting van de rechtszekerheid en scheppen van gelijke voorwaarden voor verantwoordelijken voor gegevensverwerking*

De Commissie stelt dat als gevolg van de beleidsruimte die de richtlijn aan de lidstaten biedt implementatieverschillen tussen de lidstaten zijn ontstaan. Dat tast in de opvatting van de Commissie de interne markt aan, aangezien bedrijven daardoor in verschillende lidstaten met verschillende wettelijke regelingen worden geconfronteerd. De Commissie noemt als bijzondere gebieden van aandacht de verwerking van persoonsgegevens voor de arbeidsvoorziening en voor gezondheidsdoeleinden.

- Vanuit het bedrijfsleven verneemt ook het kabinet dat implementatieverschillen tussen de lidstaten de oorzaak is van uitvoeringsproblemen, juist in de gevallen van grensoverschrijdend gegevensverkeer. In ieder geval voor wat betreft de meldplicht van gegevensverwerkingen is het juist dat er sprake is van uiteenlopende regimes die het bedrijfsleven confronteren met extra lasten. Over de toepassing van materiele inhoud van de richtlijn worden minder klachten geuit.
- De thans onder de richtlijn bestaande vrijheid om op deelterreinen regels te stellen met een aanvullende functie ten opzichte van de richtlijn, biedt de lidstaten gele-

genheid om rekening houdend met hun eigen behoeften regels te stellen die de instemming van betrokkenen hebben. Juist waar het betreft de organisatie van het arbeidsbestel en de organisatie van de gezondheidszorg zijn er grote verschillen tussen de lidstaten. Die verschillen gaan veel verder dan alleen de omgang met persoonsgegevens. Verplichtingen tot het stellen regels met betrekking tot de gegevensverwerking in die sectoren zijn zonder voldoende draagvlak bij alle betrokkenen niet in alle opzichten van toegevoegde waarde. Het kabinet hecht grote waarde aan het bestaan van een afdoende draagvlak.

- De Commissie geeft nog geen uitsluitsel over de vraag of zij kiest voor één of meer nieuwe richtlijnen, voor één of meer verordeningen, of voor een combinatie van beide. De uiteindelijke keuzes kunnen verstrekkende gevolgen hebben voor het Nederlands gegevensbeschermingsrecht en de daarin thans nog aanwezige nationale beleidsruimte.

### *2.2.2 De administratieve belasting verminderen*

De Commissie stelt voor het bestaande systeem van de meldplicht te vereenvoudigen en meer te systematiseren, mogelijk door middel van een registratieformulier dat in de hele EU zou kunnen gelden. Daarmee zouden de administratieve lasten kunnen worden verkleind.

- Het kabinet is teleurgesteld over de keuze van Commissie om afschaffing van de meldplicht en het voorafgaand onderzoek niet te overwegen. De meldplicht en het voorafgaand onderzoek zijn administratieve formaliteiten zijn die thans geen redelijk doel meer dienen, maar wel administratieve lasten opleveren. Beide instrumenten zijn een reflectie van de gedachte dat enige vorm van voorafgaande controle op de verwerking van persoonsgegevens de bescherming van die gegevens bevordert. Dat acht het kabinet niet geloofwaardig meer, alleen al omdat een meldplicht moeilijk handhaafbaar is door het onafzienbare aantal gegevensverwerkingen dat in beginsel onder de meldplicht valt, en een voorafgaand onderzoek niet meer dan een momentopname is.

### *2.2.3 Verduidelijken van de regels met betrekking tot het toepasselijke recht en de verantwoordelijkheden van de lidstaten*

De Commissie wijst op het groeiend aantal gevallen van jurisdictieconflicten. Die vloeien voort uit de omstandigheid dat steeds meer verwerkers en bewerkers van persoonsgegevens in verschillende lidstaten van de EU, in de EER of in derde landen gevestigd zijn. Betrokkenen kunnen daardoor hun rechten moeilijker uitoefenen.

- Het is terecht dat de Commissie aandacht vraagt voor dit probleem. De complexiteit van dit probleem maakt het ook begrijpelijk dat hier nader onderzoek naar moet worden gedaan. Vermoedelijk kunnen deze problemen niet volledig worden opgelost voor de gevallen waarin sprake van relaties met derde landen. Mogelijk kan er op de lange termijn worden gedacht aan wederzijdse erkenning van gegevensbeschermingsregimes in derde landen.

### *2.2.4 Uitbreiden van de verantwoordelijkheden van de voor verwerking verantwoordelijke*

De Commissie stelt de noodzaak tot vermindering van administratieve lasten tegenover de noodzaak de richtlijn beter na te leven. De Commissie stelt dat de verplichtingen van de verantwoordelijke duidelijker moeten worden omschreven, zonder dat er echter sprake is

van toename van administratieve lasten. De Commissie denkt in dat verband aan de verplichte aanstelling van een functionaris gegevensbescherming en aan een grotere toepassing van "Privacy Impact Assessments (PIA's)" en van "Privacy Enhancing Technologies (PET's)".

- In zijn algemeenheid kan worden onderschreven dat het bestaande nalevingstekort van de gegevensbeschermingswetgeving zich zowel voordoet bij de overheid als bij het bedrijfsleven. Wat het bedrijfsleven betreft, realiseren in zijn algemeenheid alleen grotere bedrijven zich in voldoende mate dat een behoorlijke zorg voor de persoonsgegevens ook een kwestie is van welbegrepen eigenbelang. Grote bedrijven staan niet afwijzend tegenover het inbouwen van privacywaarborgen in de bedrijfsvoering, als onderdeel van het meer omvattende "compliance". Dat valt te vergelijken met de wijze waarop bedrijven verantwoordelijk hoe zij zich conformeren aan het vennootschap- en jaarrekeningenrecht.
- Middelgrote en kleine bedrijven hebben een lastiger positie. Erkend moet worden dat voor die groep bedrijven de naleving van de wetgeving een relatief zware belasting kan zijn.
- Wat de overheid betreft, is het beleid op rijksniveau belegd bij de minister van BZK. Dat beleid concentreert zich op vermindering van de lasten voor de burger en het formuleren van een recht op eenmalige gegevensverstrekking van de burger aan de overheid. Vermindering van lasten voor de burger betekent ook bij de constatering van fouten in een verwerking onder verantwoordelijkheid van de overheid, de overheid ook eigener beweging de afnemers in de keten informeert over die fouten. Daarnaast dient de overheid adequaat te reageren op gevallen van identiteitsfraude.
- Het kabinet betwijfelt of dit nalevingstekort bij voorkeur moet worden bestreden door verplichtende maatregelen. Met name de verplichting tot aanstelling van een functionaris voor de gegevensbescherming betekent nogal wat. In Duitsland en Frankrijk bestaat die verplichting. In Duitsland geldt die plicht in ieder geval voor de overheid en voor bedrijven waarbij 20 personen of meer belast zijn met gegevensverwerking. Het is naar de overtuiging van het kabinet niet omvang van een onderneming of instelling die maatgevend moet zijn voor de vraag welke privacybevorderende maatregelen moeten worden getroffen, maar de aard van de gegevensverwerking. In Nederland bestaat bovendien een sterke voorkeur om de eigen verantwoordelijkheden van het bedrijfsleven te benadrukken en zonder nodeloze ingrepen in de bedrijfshuishoudingen de weg naar zelfregulering te wijzen. Overigens moet erkend worden dat gebleken is dat aanstelling van een functionaris voor de gegevensbescherming of een "privacy officer" in een organisatie ertoe leidt dat de Wbp beter wordt nageleefd.
- In het kabinetsstandpunt naar aanleiding van de rapporten evaluatie Wbp en de Adviescommissie veiligheid en de persoonlijke levenssfeer (Kamerstukken II 2009/10, 31051, nr. 5) is daarom reeds de voorkeur gegeven aan prikkels voor het bedrijfsleven boven verplichtende maatregelen. Het kabinet huldigt die visie nog steeds.
- Ook het kabinet is voorstander van de uitwerking van het "accountability" beginsel. Dat houdt in dat afschaffing van administratieve lasten plaatsvindt in ruil tegen een openlijk en openbaar rekenschap afleggen over de verwerking van persoonsgegevens, over de doeleinden die daarmee worden gediend, over aantal en aard van de



gegevens die worden verwerkt, en over de partijen aan wie die ter beschikking worden gesteld. Daarbij moet ook informatie worden gegeven over de interne naleving van verplichtingen en wijze waarop verzoeken om inzage, correctie en verzet en klachten worden behandeld. Nadere uitwerking van het accountability-principe, gecombineerd met een selectief toezicht gebaseerd op risicoanalyses kunnen van groot belang zijn bij de verlichting van de werkdruk bij de privacytoezichthouders. Dat lijkt beter bij de Nederlandse situatie te passen. Een uitwerking van dit beginsel op Europees niveau verdient sterk de voorkeur boven een uitsluitend nationale uitwerking daarvan.

- In genoemd kabinetsstandpunt is het belang van "privacy by design" bij het formuleren van overheidsbeleid en het ontwerp van ICT onderstreept. Uit ervaring blijkt dat vooral bij gegevensverwerkingen met grote maatschappelijke gevolgen het in een vroegtijdig stadium van ontwerp nadrukkelijk rekening houden met de privacy-aspecten in een later stadium acceptatieproblemen voorkomt. Het met dit middel te bereiken doel (het uit oogpunt van de bescherming van persoonsgegevens zo veel mogelijk kiezen voor het zo min mogelijk belastende beleid of systeemontwerp) staat niet op zichzelf. Het nadrukkelijker toepassen van het beginsel van dataminimalisatie, het vaker hanteren van het principe van "opt in" bij de verwerking van persoonsgegevens ("privacy by default") en het nadrukkelijker afwegen van de vraag of centrale of decentrale databases nodig zijn, moet daarbij ook worden betrokken.
- Ook is in het kabinetsstandpunt gewezen op het nut van Privacy Impact Assessments in en buiten het veiligheidsdomein.
- Het kabinet ziet overigens in de mededeling aanleiding nader te bezien hoe de eigen wetgevingsvoornemens die zijn aangekondigd in het regeerakkoord zich verhouden tot de mededeling en de komende herziening van de richtlijn. De Kamers zullen daarover nader worden bericht.

#### *2.2.5 Aanmoediging zelfregulering en onderzoek naar EU-certificeringsregelingen*

De Commissie constateert dat de wettelijke mogelijkheden tot zelfregulering maar beperkt worden benut. Zij blijft van oordeel dat zelfregulering een belangrijk instrument is. De Commissie onderzoekt of een EU-privacycertificering kan worden ontwikkeld.

- Ook in Nederland wordt er spaarzaam gebruik gemaakt van de zelfreguleringsinstrumenten die de richtlijn biedt. Er worden relatief weinig functionarissen voor de gegevensbescherming aangesteld zowel bij het bedrijfsleven, als bij de overheid. Slechts bij de rijksoverheid en de politie ligt dat anders. Er zijn verder slechts acht gedragscodes voor enkele sectoren van bedrijvigheid vastgesteld. Het kabinet steunt de Commissie overigens op dit punt, omdat zelfregulering aansluit bij het Nederlandse beleid om bedrijven en branches hun eigen verantwoordelijkheid te gunnen en hen daar zonodig ook op aan te spreken.
- Wanneer EU-privacycertificaten kunnen worden ontwikkeld met een goede betrouwbaarheid, dan zal dat goede diensten kunnen verlenen bij de ontwikkeling van nieuwe ICT-initiatieven. Het kabinet steunt dit punt.

### **2.3 Herziening van de voorschriften inzake gegevensbescherming in het kader van de politieke en justitiële samenwerking in strafzaken**

Met het Verdrag van Lissabon is er een einde gekomen aan de pijlerstructuur van de Europese Unie en zijn er nieuwe algemene rechtsgrondslagen in het leven geroepen voor het grondrecht op bescherming van persoonsgegevens binnen de Unie, voor alle onderdelen van het Unierecht, behoudens het gemeenschappelijk buitenlands en veiligheidsbeleid.

De Commissie stelt vast dat het kaderbesluit nr. 2008/977/JBZ over de uitwisseling van persoonsgegevens in het kader van de politie en justitie samenwerking een belangrijke stap voorwaarts is, maar dat er meer werk dient te worden gedaan. Het kaderbesluit heeft nu alleen betrekking op de overdracht van persoonsgegevens tussen de lidstaten onderling in het kader van de politie en justitie samenwerking in strafzaken, maar niet op de binnenlandse verwerking van deze gegevens.

Een andere tekortkoming is volgens de Commissie dat er geen onderscheid wordt gemaakt tussen de verschillende categorieën van gegevens op basis van betrouwbaarheid en dat gegevens over feiten worden onderscheiden van gegevens over opvattingen. Bovendien vervangt het kaderbesluit niet de specifieke regels op deelterreinen van de politie en justitie samenwerking, die thans in de EU van toepassing zijn, zoals Europol, Eurojust, het Schengen Informatiesysteem (SIS) en het Douaneinformatiesysteem (CIS).

De Commissie overweegt dat de doelstelling van een coherent en toegankelijk systeem van gegevensbescherming noodzaakt tot een herziening van bestaande regels op het gebied van de politie en justitie samenwerking in strafzaken te overwegen, inclusief de gegevensverwerking op nationaal niveau waarbij, voor zover noodzakelijk, kan worden voorzien in geharmoniseerde beperkingen op de rechten van betrokkenen. De Commissie benadrukt dat dit niet uitsluit dat specifieke regels voor gegevensbescherming gelden binnen het algemene kader, gelet op de specifieke aard van deze deelterreinen. De behoefte aan specifieke regels, bijvoorbeeld over de verwerking van genetische gegevens of het onderscheid tussen verschillende categorieën van personen, moet daarbij worden betrokken.

In 2011 zal een consultatie worden gehouden over de meest effectieve wijze om het toezicht op de bestaande systemen op EU-niveau te herzien. Op langere termijn zal de behoefte aan sectorspecifieke regels in de afzonderlijke rechtsinstrumenten nader worden bekeken.

- Naar aanleiding daarvan merkt het kabinet op dat kaderbesluit nr. 2008/977/JBZ ook in Nederland nog niet is geïmplementeerd. Het wetsvoorstel is inmiddels bij de Tweede Kamer ingediend. Er moet ook nog een evaluatie door de Commissie plaatsvinden. Die behoort te worden betrokken bij de beleidsvorming op EU-niveau. De voornemens van de Commissie tot herziening van het kaderbesluit zijn dan ook enigszins prematuur.
- In beginsel behoeft tegen een uitgangspunt waarin voor het terrein politie en justitie wel dezelfde *rechtsbeginselen* gelden als die op grond van de richtlijn bestaan, maar waarin *rechtsregels* verschillen omdat de aard van het werkterrein dat rechtvaardigt, geen bezwaar te worden gemaakt.
- Wel moet tenminste vaststaan dat de rechten op inzage, correctie en afscherming en ook het transparantiebeginsel niet op dezelfde manier ten uitvoer kunnen worden gelegd als in andere overheidssectoren of de private sector. Conflicten met het onderzoeksbelang mogen zich niet voordoen. Daarbij heeft het kabinet grote reserves bij de gedachte om bij het verwerken van persoonsgegevens onderscheid te maken tussen categorieën van personen. Dit is niet goed werkbaar. De status van een persoon kan immers gedurende de verwerking veranderen. Een getuige kan verdachte worden, of omgekeerd, terwijl de betrouwbaarheid van de gegevens niet bij voorbaat

vaststaat. Het onderzoek van politie en justitie is er juist op gericht om die betrouwbaarheid van de gegevens vast te stellen.

- Ten slotte is voor Nederland ook van belang dat het hoge beschermingsniveau van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens kan worden gehandhaafd.

## **2.4 De wereldwijde dimensie van gegevensbescherming**

### *2.4.1 De regels voor internationale doorgifte van gegevens verduidelijken en vereenvoudigen*

Doorgifte van persoonsgegevens aan derde landen is mogelijk wanneer het betreffende derde land beschikt over een passend niveau van gegevensbescherming. De beoordeling of een dergelijk niveau in een derde land aanwezig is, is op grond van de richtlijn primair een taak van de Commissie. De Commissie wijst erop dat de huidige richtlijn geen inhoudelijke beoordelingsmaatstaven kent en dat het kaderbesluit in het geheel niet voorziet in een dergelijk instrument. Ook wijst de Commissie erop dat sommige lidstaten eigen procedures voor de beoordeling van gegevensbeschermingsniveaus van derde landen kennen. Daaraan is het risico van onderling afwijkende beoordelingen verbonden. Bovendien kennen die procedures evenmin inhoudelijke beoordelingsmaatstaven.

Doorgifte van gegevens aan derde landen waarin geen passend beschermingsniveau heerst, is mogelijk wanneer gebruik wordt gemaakt van standaardcontractbepalingen die door de Commissie zijn vastgesteld. Deze bepalingen, aldus de Commissie, zijn echter alleen toepasbaar in situaties waarin sprake is van contracten tussen verwerkers onderling en tussen verwerkers en bewerkers.

Voor de structurele doorgifte van gegevens tussen overheden moeten de Europese Unie of de lidstaten volgens de Commissie verdragen sluiten of andere instrumenten toepassen.

Voor de grensoverschrijdende doorgifte van gegevens tussen ondernemingen binnen een concern is het instrument "Binding Corporate Rules" (BCR's) beschikbaar. De Commissie constateert dat aan dit mechanisme nog veel kan worden verbeterd.

De Commissie meent dan ook dat er aanleiding is het gehele stelsel van internationale doorgiften van gegevens te verbeteren.

- De visie van de Commissie om het gehele stelsel van grensoverschrijdende gegevensoverdrachten te verbeteren verdient naar het oordeel van het kabinet krachtige ondersteuning. Nederland heeft met zijn open economie en exportbelangen en als vestigingsplaats voor de hoofdzetel van grote ondernemingen een duidelijk belang bij een soepel toepasbaar regime voor de doorgifte van gegevens naar derde landen.
- De Commissie wijst terecht op de tekortkomingen van de bestaande procedures voor de vaststelling van de passendheid van het niveau van gegevensbescherming in derde landen. Deze zullen sneller moeten verlopen. Inhoudelijke invulling van de toetsingscriteria hoeven niet gedetailleerd te worden vastgelegd. Ook met een aantal globaal geformuleerde criteria kan vruchtbaar worden gewerkt. Wederzijdse erkenning van rechtstelsels kan daarbij het uitgangspunt zijn. Mogelijk behoeft dan voor de betrokkene niet zozeer het land van herkomst van de verwerking aanknopingspunt zijn voor de uitoefening van zijn rechten, maar het recht van het land waar de betrokkene zich bevindt.
- De afschaffing van de nationale bevoegdheden tot beoordeling van de passendheid van gegevensbeschermingsniveaus in derde landen is reeds geregeld in het bij de

Tweede Kamer aanhangige wetsvoorstel tot wijziging van de Wet bescherming persoonsgegevens in verband met administratieve lasten (Kamerstukken 31 841).

- De standaardcontractbepalingen zijn een nuttig instrument. Nederland steunt de verdere ontwikkeling van deze contracten actief.
- Het kabinet is van oordeel dat de Commissie verder zou kunnen gaan. Het is denkbaar dat bepaalde categorieën gegevensverwerkingen kunnen worden aangemerkt als verwerkingen waarbij een inbreuk op de fundamentele rechten onwaarschijnlijk is, zodat doorgifte van deze gegevens naar derde landen zonder aanvullende garanties mogelijk is, zolang dit in overeenstemming is met de algemene bepalingen van de richtlijn. De aard van de gegevens, en de kringen van betrokkenen, verzenders en ontvangers van de gegevens zijn belangrijke andere criteria die in dit verband moeten worden aangelegd.
- Er kan zonder meer worden ingestemd met de ontwikkeling van aanvullende instrumenten op EU-niveau met een vergelijkbare strekking, zoals een modelverdrag met derde landen waarin structurele doorgiften tussen overheden kunnen worden geregeld, of modelbesluiten van de Commissie. Op nationaal niveau zal het vergunningvereiste als aanvullende grondslag voor gegevensdoorgifte naar derde landen echter nog niet kunnen worden gemist.
- Het belang van BCR's kan moeilijk worden overschat. Het strategisch belang voor de EU is potentieel groot, omdat daarmee de toepassing van inhoudelijk EU-recht naar derde landen kan worden geëxporteerd. Het belang voor multinationale ondernemingen is ook groot, omdat een BCR de interne procedures stroomlijnt, en het privacybewustzijn bevordert. Momenteel mankeert er echter nog veel aan een vlotte vaststelling van de procedures voor de goedkeuring. Dat wordt veroorzaakt doordat BCR's geen zelfstandig regime in de richtlijn kennen. Daardoor moet worden teruggegrepen op nationaal recht. Dat nationaal recht kan inhoudelijk verschillend zijn tussen de lidstaten. Ernstiger is dat de procedures per lidstaat aanzienlijk kunnen verschillen. Een groep dataproductietoezichthouders - waaronder het Cbp - behandelt dit probleem inmiddels. Het kabinet stelt dit op prijs. Een echte oplossing ligt in een uitdrukkelijke regeling van de BCR op richtlijn niveau, gecombineerd met een procedure waarbij één nationale toezichthouder of instantie voor de hele EER geldende goedkeuringen voor die BCR's afgeeft. Wellicht vallen hier ook modellen te ontwikkelen.

#### *2.4.2 Bevordering van universele beginselen*

De Commissie geeft aan dat gegevensverwerking een wereldwijde activiteit is. Dat betekent ook dat de beginselen voor gegevensbescherming zoveel mogelijk universele gelding moeten hebben. De Commissie is van oordeel dat het wettelijk kader van de EU ijkpunt is geweest voor derde landen bij het vaststellen van eigen gegevensbeschermingsregels. De Commissie ziet daarom een belangrijke rol weggelegd voor de EU om een stuwende kracht te blijven achter de ontwikkeling en bevordering van internationale wettelijke en technische normen. Ook ziet de Commissie een meer belangrijke rol weggelegd voor technische normalisatie.

- Het belang van de EU om op mondiale schaal een rol te spelen bij de ontwikkeling en vaststelling van normen voor gegevensbescherming kan in beginsel worden onderschreven. Verdergaande samenwerking van de EU in internationale verbanden kan worden onderschreven.

- De betekenis van technische normalisatie voor gegevensbescherming is, ook op EU-niveau, nog onvoldoende ontwikkeld. Het is positief dat de Commissie hiervoor aandacht vraagt.
- Een kanttekening is wel op zijn plaats. De ervaring leert dat het niet eenvoudig is om met landen die zich bij de vormgeving van hun gegevensbeschermingsrecht op andere hoofdlijnen dan de EU oriënteren overeenstemming te bereiken over onderdelen van het gegevensbeschermingsrecht.

## **2.5 Een betere institutionele regeling voor handhaving van de voorschriften inzake gegevensbescherming**

In een recent arrest van het Hof van Justitie van de EU (9 maart 2010, C-518/07 Commissie/Duitsland) is nog eens onderstreept dat de eis van volledige onafhankelijkheid van de nationale dataproductietoezichthouders serieus moet worden genomen. De Commissie wijst erop dat aan de nationale toezichthouders voldoende bevoegdheden en middelen moeten worden toegekend, zowel op nationaal niveau, als voor hun aandeel in de (verplichte) onderlinge samenwerking. Die onderlinge samenwerking speelt zich deels af in de artikel 29-Werkgroep, waarin alle toezichthouders uit de lidstaten en de EDPS de Commissie adviseren over de uitvoering van de richtlijn. Verder is er collectief georganiseerd toezicht op verschillende gegevensverwerkingen op EU-niveau, zoals het Schengeninformatiesysteem.

- Nederland voldoet ook met huidige regeling in de Wbp en andere wetgeving aan zijn verplichtingen om de dataproductietoezichthouder in staat te stellen zijn taak op redelijke wijze te kunnen uitvoeren.
- In het kabinetsstandpunt naar aanleiding van de rapporten over de evaluatie van de Wbp en de Adviescommissie veiligheid en de persoonlijke levenssfeer is reeds aangekondigd dat verdere kwalitatieve verbetering van de positie van het Cbp gezocht kan worden in aanscherping van het sanctieregime. Gedacht kan worden aan invoering van de bestuurlijke boete bij overtreding van de materiële regels van de Wbp en verscherping van de strafrechtelijke sanctionering. Ook overigens zal dan kunnen worden gezien of de bepalingen in de Wbp waarin de handhaving is geregeld in alle opzichten voldoet aan de richtlijn.