Inbreng Nederlandse regering in de consultatie over het juridische raamwerk voor de bescherming van persoonsgegevens in de Europese Unie

Noodzaak voor een fundamentele herziening

1. De Nederlandse regering stelt het op prijs dat de Europese Commissie het initiatief heeft genomen voor een openbare consultatie over het juridische raamwerk voor de bescherming van persoonsgegevens in de Europese Unie. De Nederlandse regering maakt dan ook graag gebruik van deze gelegenheid om haar visie op enige vraagstukken die verbonden zijn met richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281) (hierna: de richtlijn) te geven. Zij is van oordeel dat de richtlijn op een aantal hoofdlijnen fundamenteel moet worden herzien. In onderstaande inbreng gaat de Nederlandse regering allereerst in op de initiatieven die zij zelf heeft genomen om de Nederlandse gegevensbeschermingsregelgeving te onderzoeken. Vervolgens gaat zij, mede aan de hand van de bij de realisatie van haar eigen voornemens ondervonden beperkingen die voortvloeien uit de richtlijn, in op enkele fundamentele problemen die eigen zijn aan de richtlijn. De Nederlandse regering komt daarbij met wijzigingsvoorstellen.

Eigen initiatieven van de Nederlandse regering

Evaluatie van de Wet bescherming persoonsgegevens

2. De Nederlandse regering vraagt in dat kader allereerst graag de aandacht voor een aantal initiatieven die zij zelf heeft genomen. In de periode 2007- 2009 heeft de Nederlandse regering de eigen gegevensbeschermingswetgeving (de Wet bescherming persoonsgegevens) die dient ter uitvoering van de richtlijn uitvoerig geëvalueerd. Uit die evaluatie is gebleken dat er in de samenleving sprake is van een nalevingstekort. De voordelen die de richtlijn en de Wet bescherming persoonsgegevens aan burgers en bedrijven kunnen bieden zijn nog niet voldoende bekend in de samenleving. Op de door de richtlijn gegarandeerde rechten van betrokkenen wordt verhoudingsgewijs weinig een beroep gedaan, omdat betrokkenen weinig bekend blijken met deze rechten. Daarnaast blijkt dat de naleving van de richtlijn en de wet in de praktijk nog niet van voldoende niveau is, omdat verantwoordelijken niet altijd bekend zijn met de verplichtingen die zij moeten naleven. Waar die bekendheid wel aanwezig is, ervaren verantwoordelijken echter administratieve lasten en geeft het grensoverschrijdend gegevensverkeer aanleiding tot ingewikkelde problemen.

Gegevensverwerking voor doeleinden verband houdend met de veiligheid

3. De Nederlandse regering heeft verder bijzondere aandacht gegeven aan de betekenis die gegevensverwerking heeft op het terrein van veiligheid van de samenleving. Om hun taken optimaal te kunnen vervullen, behoeven politie en andere instanties belast met de handhaving van alle aspecten van de openbare veiligheid alle nodige informatie, waaronder begrepen persoonsgegevens. Om hun taken effectief te kunnen uitvoeren moeten politie en andere hulpverleningsdiensten die persoonsgegevens ook onderling kunnen delen, echter met inachtneming van de nodige waarborgen voor de persoonlijke levenssfeer. Hierbij moet worden bedacht dat de veiligheid van de samenleving impliceert dat burgers moeten worden beschermd tegen aantasting van hun grondrechten op vrijheid, veiligheid en het ongestoord genot van het privé-leven. Dat kan inhouden dat onder omstandigheden inmenging in het recht op bescherming van persoonsgegevens onvermijdelijk is. Een bijzondere commissie heeft de Nederlandse regering geadviseerd meer aandacht te geven aan de onderlinge overdracht van persoonsgegevens tussen verantwoordelijken belast met veiligheidstaken. Daarbij heeft die bijzondere commissie geadviseerd een door haar opgesteld "richtinggevend kader" te gebruiken om te verzekeren dat verzameling, verwerking en verdere verwerking in de vorm van doorgifte van persoonsgegevens in overeenstemming met de Wet bescherming persoonsgegevens plaatsvindt en ook overigens met inachtneming van de beginselen die ten grondslag liggen aan de richtlijn.

Beleid van de Nederlandse regering

4. De Nederlandse regering neemt de uitkomst van de evaluatie van de Wet bescherming persoonsgegevens en het rapport van de bijzondere commissie serieus. Zij is voornemens om de komende jaren beleid en regelgeving op het gebied van de bescherming van persoonsgegevens te versterken op vier kernthema's. Het is van belang deze kernthema's uit te leggen. Zij zijn niet

slechts van belang voor de Nederlandse samenleving. Deze kernthema's raken ook de grondslagen van de richtlijn.

Versterking waarborgen bij de omgang met persoonsgegevens

5. Het *eerste kernthema* betreft het versterken van de waarborgen bij de omgang met persoonsgegevens. Risico's bij de omgang met persoonsgegevens moeten vooraf worden geïdentificeerd. Die risico's moeten met gerichte maatregelen worden weggenomen. Voor het veiligheidsdomein wordt een richtinggevend kader voorgesteld dat uitvoeringsinstanties en individuele professionals in staat stelt om op verantwoorde wijze om te gaan met persoonsgegevens. Het belang van de veiligheid van samenleving en de gerechtvaardigde aanspraken die burgers op bescherming door de overheid hebben, kan noodzaken tot het delen van persoonsgegevens tussen overheidsorganen onderling. De Nederlandse regering overweegt een voorstel aan het Parlement te doen deze regel wettelijk vast te leggen. Er wordt een helpdesk ingericht die ondersteuning zal bieden aan professionals bij het beantwoorden van de vragen wanneer en op welke wijze persoonsgegevens uitgewisseld kunnen worden.

Versterking van het extern toezicht op de bescherming van persoonsgegevens

6. Het *tweede kernthema* betreft een versterking van het extern toezicht op de bescherming van persoonsgegevens. Het geconstateerde nalevingstekort noodzaakt het toezicht op de naleving en de handhaving van de Wet bescherming persoonsgegevens te versterken. De Nederlandse regering zal het Parlement gaan voorstellen het College bescherming persoonsgegevens uit te rusten met ruimere bevoegdheden om bestuurlijke boetes op te leggen bij geconstateerde schendingen van de materiële bepalingen van de Wet bescherming persoonsgegevens.

Minder nadruk op procedures en controle vooraf

7. Het *derde kernthema* betreft minder nadruk op procedures en controle vooraf. Gebleken is dat instrumenten als de meldplicht en het voorafgaand onderzoek in de praktijk maar een beperkte bijdrage leveren aan de bescherming van de persoonlijke levenssfeer. Daartegenover staat dat deze instrumenten administratieve lasten opleveren voor burgers en bedrijven. De Nederlandse regering zal daarom initiatieven nemen die erop zijn gericht de meldplicht en het voorafgaand onderzoek alleen voor te schrijven voor de gevallen waarvoor dat in het belang van de bescherming van persoonsgegevens noodzakelijk is. Zij meent dat andere maatregelen minstens zo effectief kunnen zijn, vooral als die maatregelen door het bedrijfsleven zelf kunnen worden genomen.

Versterking van de positie van de burger

8. Het *vierde kernthema* betreft de versterking van de positie van de burger. De Nederlandse overheid moet in dat verband duidelijker en met meer eigentijdse middelen inhoud geven aan haar verplichting tot het geven van transparantie over de verwerkingen die onder haar verantwoordelijkheid plaatsvinden. Internetsites kunnen worden gebruikt om het inzage- en correctierecht uit te oefenen ten aanzien van de onder verantwoordelijkheid van de overheid verwerkte persoonsgegevens. Verder zal worden bezien hoe een eenvoudig vorm te geven klachtrecht kan worden ontwikkeld dat aanvullend ten opzichte van de bestaande privaatrechtelijke en bestuursrechtelijke rechtsbeschermingsmogelijkheden kan fungeren. Tenslotte zal worden bezien op welke wijze verplichtingen van overheidsinstellingen en bedrijven om persoonsgegevens beter te beveiligen moeten worden aangescherpt.

9. De Nederlandse regering heeft bovenstaande punten uitgewerkt in een formele reactie aan het Nederlandse Parlement. Deze reactie treft u bijgaand aan.

De relatie tussen de initiatieven van de Nederlandse regering en de werking van richtlijn nr. 95/46/EG

10. De Nederlandse regering meent dat veel van bovengenoemde punten ook nadere aandacht verdienen bij de nadere vormgeving van het juridisch raamwerk voor de bescherming van persoonsgegevens in de Europese Unie. Deze punten zijn naar het oordeel van de Nederlandse regering redenen voor een fundamentele herziening van de richtlijn. Zoals boven reeds is aangegeven, zijn de vier geïdentificeerde kernthema's nauw verbonden met de grondslagen van de richtlijn. Daarbij zal de aandacht in het bijzonder moeten uitgaan naar de volgende punten:

a. Het afschaffen van bestuursrechtelijke instrumenten gericht op het voorafgaand onder controle brengen van gegevensverwerkingen.
b. Het leggen van meer nadruk op privacywaarborgen die verantwoordelijken zelf kunnen treffen.
c. Het vergroten van het aantal varianten van intern toezicht.
d. Het garanderen van een robuust extern toezicht.
e. Het vergroten van de aandacht voor de positie van de burger.
f. Het duidelijker ondersteunen van de mogelijkheden voor gegevensverwerking door bestuur en rechtshandhaving.
g. Het verduidelijken van de positie van het EU-gegevensbeschermingsrecht ten opzichte van andere rechtsstelsels.
h. Het nader onderzoeken van de bruikbaarheid van de fundamentele begrippen van de richtlijn op de langere termijn.

Afschaffen van bestuursrechtelijke instrumenten gericht op het voorafgaand onder controle brengen van gegevensverwerkingen

Bestuursrechtelijke instrumenten in de richtlijn

11. De richtlijn voorziet in een tweetal instrumenten die beogen de betrokkene een zekere mate van transparantie te bieden over de verwerking van persoonsgegevens door verantwoordelijken. Het betreft de verplichting tot aanmelding van de verwerking (artikel 18 van de richtlijn) en het voorafgaand onderzoek (artikel 20 van de richtlijn). Hierboven gaf de Nederlandse regering aan dat de bepalingen uit de nationale uitvoeringswetgeving, waarin deze instrumenten nader zijn geregeld, zijn geëvalueerd. Uit de evaluatie is naar voren gekomen dat de werking van deze instrumenten onbevredigend is. Hierboven is al aangegeven dat de Nederlandse regering de terugdringing van de lasten voortvloeiend uit de meldplicht en het voorafgaand onderzoek heeft benoemd als een van de vier kernthema's die zij verder zal uitwerken op nationaal niveau. Een uitwerking op nationaal niveau brengt, bij een ongewijzigde richtlijn, onvermijdelijk beperkingen met zich. De Nederlandse regering meent dat een belangrijke winst kan worden geboekt, wanneer de richtlijn op dit onderdeel fundamenteel kan worden herzien.

Procedurele controles op gegevensverwerking vooraf achterhaald

12. De Nederlandse regering meent dat de ervaringen die uit de evaluatie van de nationale wetgeving zijn voortgekomen aangeven dat er bij de meldplicht en het voorafgaand onderzoek sprake is van een fundamenteel probleem dat op Europees niveau verdient te worden geadresseerd. De meldplicht en het voorafgaand onderzoek zijn naar het oordeel van de Nederlandse regering ongeschikte middelen gebleken om transparantie van gegevensverwerking te bereiken. Zij gaan in wezen uit van de gedachte dat gegevensverwerkingen voorafgaand aan de aanvang van de verwerking in zekere mate onder controle moeten worden gebracht. Een dergelijke benadering is bezien tegen de achtergrond van de mogelijkheden die de informatie- en communicatietechnologie biedt, achterhaald. Burgers en bedrijven willen hun eigen doeleinden bereiken door middel van het gebruikmaken van vaak complexe mogelijkheden die de informatie- en communicatietechnologie hen biedt. Zij dienen daarbij niet te worden gefrustreerd door formaliteiten die vooral een papieren betekenis hebben en vaak maar beperkte mogelijkheden bieden om betrokkenen werkelijk inzicht te bieden in de complexe doeleinden en middelen van gegevensverwerking.

Onjuiste verwachtingen en administratieve lasten bij controles vooraf op gegevensverwerkingen

13. De meldplicht en het voorafgaand onderzoek wekken ook bij verantwoordelijken een onjuiste verwachting. Een melding bij de toezichthouder wordt vaak ten onrechte gezien als een vorm van instemming van overheidswege, terwijl daarvan geen sprake is. Een voorafgaand onderzoek biedt die mogelijkheid wel, maar kost doorgaans veel tijd en inspanning en is uiteindelijk ook niet meer dan een momentopname. Wijziging in de verwerking noopt dan weer tot een nieuw tijdrovend onderzoek. De Nederlandse regering is van oordeel dat administratieve lasten voor burgers en bedrijfsleven die onvoldoende toegevoegde waarde hebben, moeten worden weggenomen. Meldplicht en voorafgaand onderzoek bij gegevensverwerking zijn daarvan bij uitstek voorbeelden.

Het leggen van meer nadruk op privacywaarborgen die verantwoordelijken zelf kunnen treffen

Meer aandacht nodig voor de werking van achterliggende normen

14. Het afschaffen van bestuursrechtelijke controle-instrumenten betekent niet noodzakelijkerwijs dat eenieder daarmee een algemeen, niet nader genormeerd recht op het verwerken van persoonsgegevens verwerft. Integendeel. Waar het volgens de Nederlandse regering om gaat is dat de normen die de voornaamste uitwerking vormen van het recht op bescherming van persoonsgegevens, zoals rechtmatigheid, doelbinding, redelijke bewaartermijnen, dataminimalisatie en de beveiligingsplicht meer rechtstreekse aandacht krijgen. Er zijn immers alternatieven voor de bestuursrechtelijke instrumenten denkbaar.

Voorbeeld van het door middel van het treffen van technische maatregelen inhoud geven aan materiële normen voor gegevensbescherming

15. De toepassing van technische maatregelen ("*Privacy by design*"), kan onder omstandigheden een veel zinvoller alternatief vormen. Zo ligt het in de bedoeling om het Nederlandse systeem van beprijzing van het weggebruik zodanig in te richten dat de in voertuigen aan te brengen technische voorzieningen slechts gegevens doorzenden over de afgelegde afstand en het toepasselijke tarief. Locatiegegevens worden in beginsel niet meegezonden. Op deze wijze wordt door middel van een technische voorziening inhoud gegeven aan normen als doelbinding en dataminimalisatie. Dergelijke maatregelen vergroten het vertrouwen van het publiek in een dergelijk systeem.

Meer nadruk op andere privacywaarborgen die verantwoordelijken zelf kunnen treffen

16. Het afschaffen van bestuursrechtelijke controles vooraf betekent naar het oordeel van de Nederlandse regering allerminst dat afbreuk kan worden gedaan aan het belang van transparantie. De Nederlandse regering bepleit om in plaats van instrumenten die beogen ex ante te werken, vooral de nadruk te leggen op het scheppen van waarborgen door verantwoordelijken zelf, in combinatie met een robuust stelsel van toezicht en handhaving achteraf. Uit de evaluatie van de Nederlandse wetgeving komt naar voren dat bedrijven en burgers wel degelijk het belang van gegevensbescherming herkennen als hun eigen belang. Inhoudelijke normen en instrumenten en waarborgen gericht op gegevensbescherming moeten zoveel mogelijk aansluiting zoeken bij de erkenning van dat eigen belang. Verantwoordelijken moeten daarom worden gestimuleerd om zelf voorafgaand aan een verwerking de risico's daarvan in een *Privacy Impact Assessment* te onderzoeken, deze risico's zelf openbaar te maken en daarbij aan te geven welke maatregelen zij hebben genomen om deze risico's weg te nemen. Bij voorkeur dienen verantwoordelijken zelf een intern toezicht op de gegevensbescherming te organiseren en betrokkenen de mogelijkheid te bieden om klachten in te dienen over vermeende schendingen van de op hen betrekking hebbende gegevens. De uitkomst van deze klachten dient openbaar te worden gemaakt. Dit klachtrecht zou aanvullend ten opzichte van de verzoeken om inzage en correctie en de mogelijkheid tot het inroepen van het recht van verzet moeten worden vormgegeven.
Verantwoordelijken kunnen voorts vertrouwenwekkende maatregelen treffen door betrokkenen eigener beweging in te lichten over het beleid dat zij voeren ter beveiliging van de door hen verwerkte persoonsgegevens en daarbij aan te geven hoe zij zullen handelen wanneer ondanks de verrichte inspanningen vertrouwelijke gegevens worden gecompromitteerd. Een algemeen geformuleerde meldplicht voor geconstateerde datalekken, al dan niet, afhankelijk van de ernst van de inbreuk gecombineerd met de verplichting om openbaar te maken welke maatregelen getroffen zijn om verdere schade en herhaling te voorkomen, kan daarvoor een oplossing zijn. Verder kan worden gedacht aan het nader uitwerken van de verplichting tot dataminimalisatie. Dat zou kunnen gebeuren door verantwoordelijken te verplichten openbaar te maken hoe lang zij persoonsgegevens bewaren, welke rechtvaardiging de bewaartermijn heeft en wat er met de persoonsgegevens gebeurt na afloop van de bewaartermijn. Een verplichting om persoonsgegevens periodiek te verwijderen of te vernietigingen zou ook een alternatief kunnen zijn.

Het vergroten van het aantal varianten van intern toezicht

17. Intern toezicht, zo blijkt uit de ervaringen in Nederland, is een onderschat instrument. Als sprake is van het bestaan van een interne toezichthouder op de gegevensbescherming in een publieke of private organisatie, dan betekent dit vrijwel steeds dat het belang van gegevensbescherming door de desbetreffende organisatie wordt erkend. Tegelijk moet worden geconstateerd dat een relatief klein aantal organisaties is overgegaan tot de aanstelling van een functionaris voor de gegevensbescherming als bedoeld in artikel 18, tweede lid, van de richtlijn. De Nederlandse regering meent dat dit mede is terug te voeren op een al te formele positie van deze functionaris. Dit is niet alleen een kwestie van de inrichting van de nationale wetgeving. Ook de positie van de functionaris in de richtlijn verdient heroverweging. Voor intern toezicht zouden naast de functionaris voor de gegevensbescherming minder in de structuur van bedrijven ingrijpende toezichthouders moeten kunnen worden aangesteld. De ervaring heeft

geleerd dat de verplichting in de richtlijn de functionaris voor de gegevensbescherming uit te rusten met formele toezichtsbevoegdheden eerder leidt tot het niet dan het wel aanstellen van dergelijke functionarissen. Alternatieven zijn voorhanden. De Nederlandse Wet politiegegevens introduceerde naast de functionaris voor de gegevensbescherming reeds de privacyfunctionaris die belast is met een eenvoudiger takenpakket. De Wet politiegegevens schrijft daarnaast periodieke privacyaudits door onafhankelijke personen voor, en roept ook protocolplichten in het leven.

Het garanderen van een robuust extern toezicht

18. Voor het extern toezicht dienen de nationale gegevensbeschermingsautoriteiten over toereikende mogelijkheden te beschikken om effectief te kunnen optreden tegen geconstateerde of dreigende ernstige schendingen van het recht op bescherming van persoonsgegevens. De Nederlandse regering is, zoals in bijgaand kabinetsstandpunt is beschreven, voornemens de bevoegdheid van het Nederlandse College bescherming persoonsgegevens om bestuurlijke boetes op te leggen uit te breiden en ook de hoogte van de sancties nader te bezien. Het gaat de Nederlandse regering daarbij vooral om het beter tot gelding te laten komen van de materiële normen die een uitwerking vormen van het recht op bescherming van persoonsgegevens. Tot dusverre werd in de Nederlandse wetgeving slechts de schending van administratieve verplichtingen met een punitieve sanctie bedreigd. Daarbij betrof het juist de verplichtingen in de sfeer van bestuursrechtelijke instrumenten. Bij een fundamentele herziening van de richtlijn behoort ook een herziening voor de aandacht van sanctionering van overtreding van de materiële normen.

Het vergroten van aandacht voor de positie van de burger

19. De burger, dan wel de betrokkene, krijgt in de richtlijn een aantal belangrijke rechten aangereikt, die hij, ondersteund door zijn nationale gegevensbeschermingswetgeving, kan uitoefenen. Het betreft de rechten van inzage, correctie en verzet. Daarnaast kan hij zijn recht op bescherming van persoonsgegevens in rechte uitoefenen. De vraag moet worden gesteld of deze rechten een volledige effectieve bescherming van het grondrecht bieden. Uitoefening van de rechten van inzage, correctie en verzet biedt niet altijd inzicht in de vraag waarom persoonsgegevens worden verwerkt en aan de hand van welke criteria zij verder worden verwerkt. Verantwoordelijken behoren uit eigen beweging inzicht te verschaffen in de categoriseringen die zijn aan hun verwerking te grondslag leggen. Verder lijkt het gerechtvaardigd te stellen dat geschillen over schending van het recht op bescherming van persoonsgegevens niet altijd op geld waardeerbaar zijn. De vraag is dan ook gerechtvaardigd of eenvoudige, laagdrempelige en kosteneffectieve klachtprocedures geen zinvolle aanvulling vormen op de bestaande instrumenten die de richtlijn biedt.
Het is denkbaar dat klachtenregelingen worden toegesneden op de eigenaardigheden van de sectoren van bedrijvigheid waarmee de betrokkene in aanraking komt. Zo heeft de betrokkene in zijn hoedanigheid van burger ten opzichte van de overheid een andere positie dan hij als consument heeft ten opzichte van een onderneming van wie hij diensten of goederen afneemt. Mogelijk moet er voor de betrokkene in zijn hoedanigheid van eindgebruiker van internetdiensten een aparte regeling worden getroffen.

Het duidelijker ondersteunen van de mogelijkheden voor gegevensverwerking door bestuur en rechtshandhaving

20. Bestuur en rechtshandhaving vervullen een aparte rol. Hun werkzaamheden zijn erop gericht om in een democratische samenleving de grondrechten van burgers mede gestalte te geven. Zij staan daarbij onder voortdurende controle van een gekozen volksvertegenwoordiging en van de rechter. Deze bijzondere rol komt in de richtlijn eigenlijk niet goed tot uitdrukking. Bestuur en rechtshandhaving behoeven voor de hun opgedragen taken in veel gevallen persoonsgegevens. Deze gegevens zullen in veel gevallen door bestuursorganen, de politie en justitie moeten kunnen worden gedeeld, ook in gevallen waarin bij de oorspronkelijke verzameling van de gegevens niet steeds kon worden voorzien dat daarvoor een noodzaak bestond. De rechtvaardiging van het verder verwerken van gegevens in de publiekrechtelijke sfeer is een zaak van fundamenteel belang, die verder gaat het afwegen van belangen in het kader van de bescherming van persoonsgegevens. Het grondrecht van de bescherming van persoonsgegevens staat niet op zichzelf, maar moet ook in zijn relatie tot andere, door het Handvest van de grondrechten van de Europese Unie gegarandeerde grondrechten worden beschouwd. Het recht op vrijheid en veiligheid van de persoon (artikel 6 van het Handvest) en het recht op eerbiediging van het privé-leven en van het familie- en gezinsleven (artikel 7 van het Handvest) verdienen evenzeer bescherming. Bestuur en rechtshandhaving dienen daarvoor zorg te dragen. Ten behoeve van de bescherming

van deze grondrechten moet de noodzaak worden erkend van het verwerken van persoonsgegevens. Vanzelfsprekend moeten daarbij de nodige waarborgen gelden, waaronder een adequate wettelijke grondslag, welke getoetst is aan de eisen die voortvloeien uit het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en uit het Handvest van de grondrechten.
Een fundamentele erkenning van dit belang behoort echter ook in de richtlijn tot uitdrukking te komen.

Het verduidelijken van de positie van het EU-gegevensbeschermingsrecht ten opzichte van andere rechtsstelsels

De verhouding van het gegevensbeschermingsregime van de Europese Unie tot dat van andere staten

21. Burgers en bedrijven zijn in toenemende mate voor hun werkzaamheden en andere ontplooiingsvormen afhankelijk van de verwerking van gegevens. Het functioneren van internet brengt noodzakelijkerwijs met zich dat die gegevens wereldwijd circuleren. Dat brengt weer met zich dat het belang van bescherming van persoonsgegevens zich niet beperkt tot de Europese Unie. In de Verenigde Staten, in de landen die bij de *Asian Pacific Economic Cooperation* zijn aangesloten, en in een aantal andere individuele derde landen heeft men zich dit belang ook aangetrokken. In deze landen zijn individueel of op collectieve basis uitgangspunten en regelgeving voor de gegevensbescherming vastgesteld. Die uitgangspunten en regelgeving vertonen zowel overeenkomsten als verschillen met het Europees recht.
De Europese Unie heeft in de afgelopen jaren belangrijke ervaring opgedaan met de confrontatie van Europees gegevensbeschermingsrecht met het gegevensbeschermingsrecht van derde landen. De werkingssfeer van de richtlijn is in 1999 uitgebreid tot de landen van de Europese Economische Ruimte. Daarnaast is ten aanzien van enkele derde landen vastgesteld dat zij in hun eigen interne recht een uit Europees perspectief passend niveau van gegevensbescherming hebben vastgesteld.

Ervaringen waaruit lering kan worden getrokken; het voorkomen en oplossen van conflicterende eisenvoortvloeiend uit verschillende rechtsstelsels

22. Er zijn echter ook andere ervaringen. Immers, de ervaringen met de *Safe Harbor Principles*, de diverse overeenkomsten op het gebied van de verzameling en doorgifte van passagiersgegevens met verschillende derde landen en de overdracht van financiële gegevens ten behoeve van het *Terrorist Finance Tracking Program* hebben naar het oordeel van de Nederlandse regering geleerd dat het niet altijd eenvoudig is derde landen ertoe te bewegen zich bij de vormgeving van het eigen gegevensbeschermingsrecht in alle gevallen te conformeren aan de beginselen van het Europees gegevensbeschermingsrecht. Vermeden moet worden dat verantwoordelijken in de Europese Unie geconfronteerd worden met conflicterende verplichtingen voortvloeiend uit verschillende rechtsstelsels of dat betrokkenen geconfronteerd worden met een tekortschietend gegevensbeschermingsregime. Dat speelt met name een rol bij de doorgifte van bijzondere persoonsgegevens. De richtlijn zou een regeling kunnen bevatten die de doorgifte van bijzondere persoonsgegevens aan derde landen toestaat, indien de noodzaak daartoe voortvloeit uit een zwaarwegend algemeen belang, aan die doorgifte een verdrag of bindend besluit van de Europese Unie aan ten grondslag ligt en er is voorzien in waarborgen voor de persoonlijke levenssfeer.
Naar het oordeel van de Nederlandse regering hebben de inspanningen die de *EU - US High Level Contact Group on information sharing and privacy and personal data protection* gewezen hoe de confrontaties tussen de rechtsstelsels van verschillende staten kunnen worden opgelost. Het wederzijds benoemen van overeenkomsten tussen de desbetreffende rechtsstelsels en het zoeken van oplossingen op de punten waar de desbetreffende rechtsstelsels verschillen vertonen, lijkt een vruchtbare weg. De Nederlandse regering meent dat deze weg in vergelijkbare gevallen vaker moet worden gevolgd.

Beproeven van de mogelijkheid van wederzijdse erkenning

23. De Nederlandse regering zou in dit opzicht ook willen wijzen op de mogelijkheid om binnen of buiten het kader van de richtlijn een instrument te ontwikkelen om tot een vorm van wederzijdse erkenning tussen de verschillende stelsels van gegevensbeschermingsrecht te komen. Een dergelijk instrument kan aanvullend zijn ten opzichte van de gevallen waarin het nemen van een beslissing over de passendheid van het niveau van gegevensbescherming in een derde land niet mogelijk blijkt. Het is denkbaar dat een systeem van wederzijdse erkenning uiteindelijk kan leiden tot een min of meer wereldwijd te hanteren gemeenschappelijke standaard voor de bescherming van persoonsgegevens.

Binding Corporate Rules

24. Al enige jaren blijkt het internationaal georganiseerde bedrijfsleven grote behoefte te hebben aan het werken met intern bindende gedragscodes voor de bescherming van persoonsgegevens ("*Binding Corporate Rules*"). Met betrekking tot de inhoud en de procedure heeft de artikel 29 Werkgroep reeds een aantal opinies vastgesteld. *Binding Corporate Rules* die worden vastgesteld in overeenstemming met de richtlijn is een zeer effectief instrument om gegevens van personeel en klanten van bedrijven op adequate wijze te beschermen bij doorgifte naar derde landen waar geen passend niveau van gegevensbescherming bestaat. De Nederlandse regering is van oordeel dat inmiddels de tijd rijp is om de richtlijn aan te vullen met een regeling over *Binding Corporate Rules*. Een dergelijke regeling zou ook moeten worden vastgesteld met gebruikmaking van het beginsel van wederzijdse erkenning. Daarbij kan als regel gelden dat wanneer Binding Corporate Rules door een nationale autoriteit voor de gegevensbescherming krachtens het nationale recht dat ter uitvoering van de richtlijn is vastgesteld, zijn goedgekeurd, deze beslissing als bindend wordt aangemerkt voor alle andere nationale autoriteiten. Een aantal stappen op dit gebied zijn reeds gezet door een aantal samenwerkende toezichthouders uit de Europese Unie. Verbreding en verdieping van dit initiatief is belangrijk.

Verhouding tot de EER

25. Verder is de Nederlandse regering van oordeel dat de beslissing die reeds in 1999 is genomen over de gelding van richtlijn in de landen die partij zijn bij de Overeenkomst inzake de Europese Economische Ruimte, maar die geen lidstaat zijn van de Europese Unie, op een duidelijker wijze in de richtlijn wordt geïncorporeerd dan thans het geval is. De ervaringen in Nederland hebben geleerd dat er onvoldoende duidelijkheid bestaat over de implicaties van het besluit van het Gemengd Comité nr. 83/1999 van 25 juni 1999 tot wijziging van Protocol no. 37 en bijlage XI (Telecommunicatiediensten) bij de EER-Overeenkomst (PbEG L 2000, 296).

Toepasselijkheid nationaal recht op gegevensverwerking en concernverhoudingen

26. De Nederlandse regering vestigt de aandacht op de bijzonderheden die de toepassing van artikel 4 van de richtlijn met zich brengt. Die bepaling brengt met zich dat de nationale wetgeving van het land waar de verantwoordelijke is gevestigd van toepassing is op een verwerking van persoonsgegevens die door die verantwoordelijke wordt verricht. Wanneer de verantwoordelijke vestigingen heeft in meer dan één lidstaat, heeft hij de verplichting om ervoor te zorgen dat elk van die vestigingen voldoet aan de verplichtingen die worden opgelegd door de toepasselijke nationale wetgeving. Het stelsel van de richtlijn geeft de lidstaten betrekkelijk ruime mogelijkheden om bij de omzetting van de richtlijn in nationaal recht de nodige regels vast te stellen. Hoewel dat gelet op de aard van de richtlijn een passende regel is, heeft dat onvermijdelijk tot gevolg dat er enige implementatieverschillen ontstaan tussen de lidstaten.
Dit verschijnsel is op zichzelf genomen niet principieel negatief te bejegenen, aangezien de verschillende lidstaten rekening moeten houden met de eisen die voortvloeien uit hun eigen rechtsstelsel. Echter, het mag er naar het oordeel van de Nederlandse regering niet toe leiden dat multinationale ondernemingen die over vestigingen in meer dan één lidstaat beschikken worden geconfronteerd met verplichtingen die van lidstaat tot lidstaat verschillen. De ervaring leert dat dit verschijnsel zich in ieder geval bij de meldplicht voordoet. De Nederlandse regering is van oordeel dat dit verschijnsel afbreuk doet aan hetgeen de richtlijn bevordert, te weten het vrij verkeer van persoonsgegevens.
Deze hindernis zou kunnen worden beëindigd door de meldplicht af te schaffen, hetgeen hierboven reeds is betoogd. Een alternatief zou meer harmonisatie kunnen zijn van een, naar het oordeel van de Nederlandse regering, zo ruim mogelijk vrijstellingenbeleid van de meldplicht.
Een hiermee verbonden vraagstuk is de onderlinge afstemming van de activiteiten van de toezichthoudende autoriteiten in de onderscheiden lidstaten. In het kader van de Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, als bedoeld in artikel 29 van de richtlijn worden reeds de nodige inspanningen geleverd om de toepassingspraktijk van de richtlijn te ondersteunen. Het ontwikkelen van een gemeenschappelijk toezichtsbeleid, het gezamenlijk inzetten op grensoverschrijdende risicoanalyses en daaraan gekoppelde handhavingsacties zou verder kunnen worden bevorderd.

Heroverweging van het begrippenapparaat

27. Tenslotte wijst de Nederlandse regering erop dat zich op langere termijn de noodzaak zal aandienen voor een meer fundamentele verandering van de betekenis van een aantal

basisbegrippen uit de richtlijn. Verschijnselen als "*cloud computing*" en "*Radio Frequency Identification*" leiden op den duur onvermijdelijk tot de noodzaak centrale begrippen uit de richtlijn als "persoonsgegeven"en "verantwoordelijke" opnieuw op hun bruikbaarheid voor de komende decennia te beoordelen. Het eindbeeld van deze ontwikkelingen in nog zo onzeker dat het onmogelijk is daarvoor nu al vastomlijnde standpunten in te nemen. Niettemin ligt hier wel een taak voor de Europese Unie.