Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1999–2000

27 043 Toepassing van artikel 25 en 26 van Richtlijn 95/46/EG (gegevensverkeer tussen de EU en derde landen)

Nr. 1

BRIEF VAN DE MINISTER VAN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

's-Gravenhage, 9 maart 2000

Tijdens de plenaire behandeling van het wetsvoorstel bescherming persoonsgegevens (kamerstuknr. 25 892) november jl. heb ik toegezegd U nader te informeren over de toepassing van artikel 25 en 26 van Richtlijn 95/46/EG (gegevensverkeer tussen de EU en derde landen). De bijgevoegde nota strekt tot nakoming van deze toezegging.

De Minister van Justitie,
A. H. Korthals

KST44454
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2000

GEGEVENSVERKEER TUSSEN DE EUROPESE UNIE EN DERDE LANDEN

1. Inleiding

In het voorstel van Wet bescherming persoonsgegevens dat op 23 november 1999 door de Tweede Kamer is aanvaard (Kamerstukken I 1999–2000, 25 892, nr. 92), zijn bepalingen opgenomen omtrent het gegevensverkeer tussen de lidstaten van de Europese Unie en derde landen. Deze vloeien rechtstreeks voort uit de artikelen 25 en 26 van Richtlijn 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 (Pb EG no. L281, hierna: de richtlijn). De hierin neergelegde hoofdregel is dat vanuit de lidstaten slechts persoonsgegevens mogen worden doorgegeven aan landen buiten de Unie indien het desbetreffende land een «passend beschermingsniveau» waarborgt.

Deze bepalingen worden van steeds groter belang. De intensiteit van het internationale gegevensverkeer is de laatste jaren sterk toegenomen. Dit is in belangrijke mate het gevolg van technologische ontwikkelingen. Met behulp van Internet en daarmee verband houdende technieken worden op steeds omvangrijke schaal gegevens uitgewisseld tussen personen en instanties overal ter wereld. Vanuit een economisch perspectief bezien is het van groot belang dat dit gegevensverkeer zich verder kan ontwikkelen. Tegelijkertijd rijst echter de vraag op welke wijze burgers tegen mogelijke inbreuken op hun persoonlijke levenssfeer worden beschermd. De uitwisseling kan immers persoonsgegevens betreffen die in de EU ingevolge de richtlijn wettelijke bescherming genieten buiten de EU niet of in minder mate aanwezig is. De door de richtlijn gestelde voorwaarde dat een derde land in beginsel dient te beschikken over een passend beschermingsniveau, dient tegen deze achtergrond te worden bezien.

De toepassing van de EU-richtlijn dient aldus nadrukkelijk te worden bezien in de context van de ontwikkelingen op het gebied van de elektronische snelweg. Onlangs is aan de Tweede Kamer medegedeeld dat in mei van dit jaar de notitie «Internationalisering en recht op de elektronische snelweg» aan de Tweede Kamer zal worden toegezonden (Kamerstukken II 1999/2000, 25 880, nr. 9). Hierin zal worden ingegaan op de verschillende activiteiten die in internationaal verband op dat terrein plaatsvinden en de Nederlandse inzet daarbij. Het toetsingskader zoals verwoord in de nota «Wetgeving voor de elektronische snelweg» (Kamerstukken 1997/98, 25 880, nrs. 1–2) geldt bij het bepalen van deze inzet als uitgangspunt. Hierin wordt onder meer een duidelijke voorkeur uitgesproken voor mondiale oplossingen voor vraagstukken betreffende de elektronische snelweg. De artikelen 25 en 26 van de EU-richtlijn bieden hiervoor de benodigde ruimte; het biedt een toetsingskader voor de relatie tussen de EU en derde landen op het terrein van de bescherming van persoonsgegevens.

In de onderhavige nota komt de vraag aan de orde op welke wijze invulling wordt gegeven aan de hiervoor genoemde bepalingen van de EU-richtlijn inzake bescherming van persoonsgegevens. Daartoe zal allereerst een korte schets worden gegeven van het geldende recht in de situatie voorafgaand aan de inwerkingtreding van Richtlijn 95/46/EG (par. 2). Vervolgens zal worden ingegaan op de betekenis van de artikelen 25 en 26 van de richtlijn en de wijze waarop deze zijn omgezet in het wetsvoorstel (par. 3). Daarna volgt uit het hoofdbestanddeel van deze nota: de nadere invulling van de in de richtlijn vastgelegde uitgangspunten. Daarbij zal in het bijzonder worden ingegaan op de dialoog tussen de EU

en de VS die tot dusverre als het gaat om de toepassing van artikel 25 en 26, de meeste aandacht heeft gekregen (par. 4).

Vooraf zij nog opgemerkt dat de bepalingen uit de richtlijn uitsluitend van toepassing zijn op activiteiten die binnen de werkingssfeer van het EG-recht vallen. De doorgifte van bijvoorbeeld van politiële gegevens vanuit de EU naar een derde land zijn derhalve niet aan het regime van artikel 25 en 26 onderworpen. Dit laat onverlet dat er op EU-niveau soms vergelijkbare regels bestaan met het oog op activiteiten die vallen buiten het EG-recht. Een voorbeeld daarvan is artikel 18 van de Europol-overeenkomst. Dergelijke bepalingen blijven in deze nota verder buiten beschouwing.

2. Geldend recht voorafgaand aan Richtlijn 95/46/EG

Het gegevensverkeer met andere landen was in de periode voorafgaand aan de inwerkingtreding van de richtlijn summier geregeld. De huidige Nederlandse wetgeving vormt daar nog de weerslag van. In artikel 49, tweede lid, van de Wet persoonsregistraties (WPR) wordt bepaald dat het verboden is vanuit Nederland gegevens te verstrekken aan of te betrekken van een zich elders bevindende persoonsregistratie waarop de WPR niet van toepassing is, voor zover bij algemene maatregel van bestuur is verklaard dat door zodanig verstrekken of betrekken de persoonlijke levenssfeer van de betrokken persoon ernstig kan worden benadeeld. Dit betekent derhalve dat het gegevensverkeer met andere landen is toegestaan, tenzij bij algemene maatregel van bestuur anders is bepaald. De omgekeerde regel waarbij een algemeen verbod op internationaal gegevensverkeer zou gelden behoudens bij algemene maatregel van bestuur te omschrijven uitzonderingen, is bij de totstandkoming van de WPR nadrukkelijk afgewezen. De toenmalige regering meende dat het in de WPR gekozen systeem meer dan dat van een algemeen verbod met uitzonderingen, geschikt was om prompt te reageren op gebleken of dreigende misstanden (Kamerstukken II 1984–1985, 19 095, nrs. 1–3, p. 51). De noodzaak voor een dergelijke reactie is tot dusverre niet gebleken; een algemene maatregel van bestuur zoals hiervoor bedoeld is nooit tot stand gekomen.

Op Europees niveau golden in de periode voorafgaand aan de inwerkingtreding van de richtlijn alleen regels krachtens het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van het individu in verband met de geautomatiseerde registratie van persoonsgegevens (Trb. 1981, 8). Een verdragsstaat mag het gegevensverkeer met een andere verdragsstaat in beginsel niet verbieden of aan een bijzondere vergunning binden met het motief om de persoonsgegevens van zijn burgers te beschermen (art. 12, tweede lid). De achterliggende gedachte hiervan is dat een verdragsstaat voldoet aan de in het verdrag neergelegde privacy-beginselen en derhalve daarin voor verdragsstaten geen reden kan zijn gelegen om hun onderlinge gegevensverkeer te beperken of uit te sluiten. Deze bepaling is tot op zekere hoogte vergelijkbaar met artikel 1, tweede lid, van de richtlijn dat belemmeringen van het gegevensverkeer tussen de EU-lidstaten verbiedt. Anders dan de richtlijn bevat het verdrag daarentegen geen regels omtrent het gegevensverkeer met staten die geen partij zijn bij het verdrag. Buiten de landen van de Europese Unie zijn thans Zwitserland, Noorwegen, Hongarije, IJsland en Slovenie partij. De verwachting is dat in de toekomst meer lidstaten van de Raad van Europa zullen volgen.

Vergelijkbare normen zijn te vinden in de OESO-richtlijnen van 23 december 1980. Ook hierin is als uitgangspunt geformuleerd dat – ervan uitgaande dat de lidstaten voldoen aan de in de richtlijn vervatte begin-

selen – de lidstaten van de OESO zich onthouden van beperkingen van de uitwisseling van persoonsgegevens tussen het eigen land en andere lidstaten. Dit zou anders kunnen zijn indien zou blijken dat een bepaalde lidstaat de in de OESO-richtlijn neergelegde beginselen nog niet daadwerkelijk naleeft of indien de uitvoer van gegevens een ontduiking van de eigen wetgeving zou opleveren. Dit laatste zou zich kunnen voordoen indien persoonsgegevens via een andere lidstaat worden doorgegeven aan een andere staat die geen lid is van de OESO en niet voldoet aan de gestelde minimumnormen. Tijdens de ministeriële conferentie van de OESO over e-commerce in Ottowa in oktober 1998 is een verklaring aangenomen waarin bovengenoemde richtlijnen zijn herbevestigd en tevens is vastgesteld dat de lidstaten terzake van het gebruik van mondiale netwerken zullen streven naar privacybescherming welke op de richtlijnen van 1980 zijn gebaseerd. Naast de Europese landen zijn onder meer de Verenigde Staten, Canada, Japan, Nieuw-Zeeland en Australië lid van de OESO.

3. Inhoud Richtlijn 95/46/EG

Het grensoverschrijdend gegevensverkeer is in Richtlijn 95/46/EG veel gedetailleerder geregeld dan voorheen het geval was. Daarbij gaat het om een regeling van het gegevensverkeer tussen de lidstaten van de Europese Unie en landen van buiten de Unie (derde landen). Het gegevensverkeer tussen de lidstaten onderling is ingevolge de richtlijn volledig vrij. Een belangrijke doelstelling van de richtlijn was immers om in het kader van de totstandbrenging van de interne markt het vrij verkeer van gegevens binnen de Unie mogelijk te maken door middel van harmonisatie van het niveau van gegevensbescherming. Het gegevensverkeer tussen de lidstaten onderling blijft hier verder buiten beschouwing.

Omtrent het gegevensverkeer tussen de EU-lidstaten en derde landen is de hoofdregel neergelegd in artikel 25, eerste lid. Hierin wordt bepaald dat lidstaten persoonsgegevens slechts naar een derde land mogen worden doorgegeven indien dat land een passend beschermingsniveau biedt. Wat een «passend beschermingsniveau» is wordt in de richtlijn niet nader geregeld. Een en ander hangt af van de omstandigheden van het geval. Blijkens artikel 25, tweede lid, dient ter beoordeling van het beschermingsniveau in een derde land in het bijzonder rekening te worden gehouden met:
– de aard van de gegevens;
– het doel van de voorgenomen verwerking;
– de duur van de voorgenomen verwerking;
– het land van herkomst en het land van eindbestemming;
– de algemene en sectoriële rechtsregels die in het desbetreffende derde land van toepassing zijn;
– de beroepscodes en veiligheidsmaatregelen die in het desbetreffende derde land van toepassing zijn.

De Commissie kan – na raadpleging van het Comite van vertegenwoordigers van de EU-lidstaten als bedoeld in artikel 31 van de richtlijn – officieel verklaren dat een bepaald land een passend beschermingsniveau biedt (art. 25, zesde lid). De lidstaten dienen in dat geval de nodige maatregelen te treffen om het besluit van de Commissie uit te voeren. In de praktijk betekent dit dat lidstaten voor zover nodig wettelijke of andere belemmeringen binnen de nationale rechtsorde moeten wegnemen ten einde het gegevensverkeer met het desbetreffende derde land onbelemmerd te kunnen laten plaatsvinden. Overigens is het oordeel van de Commissie niet in alle gevallen doorslaggevend. Indien de Commissie met haar beslissing afwijkt van het advies van het genoemde Comite kan de Raad met een gekwalificeerde meerderheid een andere beslissing nemen.

Op grond van artikel 26 zijn uitzonderingen op de in artikel 25 neergelegde hoofdregel mogelijk. In de eerste plaats kan een lidstaat toestemming geven voor een doorgifte of een categorie van doorgiften van persoonsgegevens naar een derde land waar geen passend beschermingsniveau is, indien degene die voor de verwerking verantwoordelijk is met het oog op de bescherming van de persoonlijke levenssfeer voldoende waarborgen biedt. Dit vloeit voort uit artikel 26, tweede lid. De richtlijn biedt uitdrukkelijk de mogelijkheid om deze waarborgen via modelcontracten tot stand te brengen. Krachtens artikel 26, vierde lid, kan de Commissie – na raadpleging van het Comite van regeringsvertegenwoordigers als bedoeld in artikel 31 van de richtlijn – besluiten dat bepaalde modelcontractbepalingen voldoende waarborgen bevatten en aldus een basis kunnen vormen voor gegevensverkeer vanuit de EU-lidstaten met de betrokken verantwoordelijken buiten de EU.

Daarnaast noemt de richtlijn in artikel 26, eerste lid, enkele specifieke situaties waarin gegevensverkeer mogelijk is met derde landen die geen passend beschermingsniveau bieden. Deze bepaling dient restrictief te worden geïnterpreteerd. Doorgifte van gegevens mag onder meer plaatsvinden indien de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven. Opdat betrokkene op volwaardige wijze zijn toestemming kan geven is nodig dat deze adequaat wordt geinformeerd. Niet voldoende is dat betrokkene van een voorgenomen doorgifte in kennis is gesteld en de betrokkene geen bezwaar heeft gemaakt. Voorts is een verstrekking aan een derde land mogelijk indien deze noodzakelijk is ter uitvoering van een overeenkomst of voor de sluiting of uitvoering van een overeenkomst die in het belang is van de betrokkene. In deze context zijn als voorbeelden genoemd verstrekkingen die noodzakelijk zijn voor vliegticketreservaties alsmede doorgiften die noodzakelijk zijn voor het verrichten van een internationale betaling via een bank of door middel van een creditcard. Ook is verstrekking aan een derde land mogelijk indien een vitaal belang van de betrokkene in het geding is, bijvoorbeeld indien beschikbaarheid van gegevens in het derde land dringend gewenst in het geval de betrokkene aldaar het slachtoffer is geworden van een ongeval of een ernstige ziekte. Ten slotte is doorgifte mogelijk indien deze noodzakelijk of wettelijk verplicht is vanwege een zwaarwegend algemeen belang, alsook doogiften vanuit openbare registers die krachtens de wet bedoeld zijn om door het publiek te worden geraadpleegd.

De artikelen 25 en 26 van de richtlijn zijn omgezet in artikel 76, 77 en 78 van het voorstel van Wet bescherming persoonsgegevens. Daarbij is de richtlijn letterlijk gevolgd. Op grond van artikel 78 dient de minister van Justitie besluiten van de Commissie omtrent het beschermingsniveau in derde landen bij ministeriele regeling in het Nederlandse recht te verankeren. Ook is de minister bevoegd om in concrete situaties na advies van de Registratiekamer een vergunning af te geven voor een doorgifte van gegevens naar een derde land dat niet beschikt over een passend beschermingsniveau. Deze bevoegdheid vindt haar basis in artikel 26, tweede lid, van de richtlijn.

4. Toepassing Richtlijn 95/46/EG

4.1 Algemene uitgangspunten

De artikelen 25 en 26 van de richtlijn zoals hiervoor uiteengezet, bevatten verschillende gronden waarop gegevensverkeer tussen de EU en derde landen kan worden toegestaan. Afhankelijk van de situatie in het desbetreffende derde land zal moeten worden bezien welke van deze mogelijkheden in aanmerking komen en welke procedure vervolgens moet worden doorlopen om een bepaald gegevensverkeer daadwerkelijk te realiseren.

Er bestaat geen rangorde tussen deze mogelijkheden; in de richtlijn is ook geen voorkeur uitgesproken voor een van de beschikbare opties. De toepassing van artikel 25 of 26 hangt af van de specifieke omstandigheden van het concrete geval.

In de afweging tussen de geschetste mogelijkheden kunnen verschillende factoren een rol spelen. Artikel 25 biedt het voordeel van de rechtszekerheid. Is eenmaal op EU-niveau vastgesteld dat een derde land geheel of voor bepaalde categorieën van gevallen beschikt over een passend niveau van bescherming, dan zijn de lidstaten in beginsel niet langer bevoegd om op basis van een oordeel over de situatie in dat derde land het gegevensverkeer te beperken of te blokkeren. Toepassing van artikel 25 vergt evenwel een uitgebreid en doorgaans gecompliceerd onderzoek naar het desbetreffende rechtssysteem. Artikel 26 gaat daarentegen uit van beoordeling per afzonderlijk geval en biedt hierdoor meer flexibiliteit. Vooraf is evenwel tot op zekere hoogte onzeker in hoeverre een bepaalde doorgifte op een van de in artikel 26 aangegeven gronden doorgang kan vinden.

Uit de richtlijn blijkt dat primair binnen de lidstaten moet worden beoordeeld of voldaan is aan de voorwaarden van artikel 25 en 26. Het ligt evenwel niet voor de hand dat elke lidstaat bij de toepassing van deze bepalingen zijn eigen koers vaart. De relatie tussen de lidstaten van de EU en derde landen is bij uitstek een terrein waar de betrokken actoren gezamenlijk beleid dienen te ontwikkelen. Dit verklaart ook dat in artikel 25 en 26 van de richtlijn aan de Commissie belangrijke bevoegdheden zijn toegekend. Deze dienen steeds in samenspraak met de lidstaten te worden uitgeoefend.

Het gemeenschappelijk beleid van de Commissie en de lidstaten is er op gericht om voor bepaalde derde landen vast te stellen dat geheel of gedeeltelijk sprake is van een passend beschermingsniveau. Beslissingen van de Commissie op grond van artikel 25, zesde lid, van de richtlijn kunnen leiden tot rechtszekerheid in het gegevensverkeer tussen de EU en derde landen. Dit is uit economisch oogpunt van grote betekenis. Er is een gemeenschappelijk belang van de EU en derde landen om de mogelijkheden die de richtlijn op dit punt biedt, optimaal te benutten.

Bij de toepassing van artikel 25 doen zich evenwel verschillende moeilijkheden voor. Zoals gezegd is een gedegen onderzoek nodig om aan de hand van vooraf te bepalen maatstaven te kunnen beoordelen in hoeverre het beschermingsniveau in een bepaald land daadwerkelijk toereikend is. Daarbij kan niet worden volstaan met een toetsing van de toepasselijke regels, maar zal ook een zeker inzicht moeten bestaan in de uitvoerings- en handhavingspraktijk. Een extra complicatie bestaat ten aanzien van federale landen waar het beschermingsniveau kan verschillen per deelstaat. Voorbeelden hiervan zijn de VS, Zwitserland, Canada en Australië. Ten slotte speelt een rol dat sommige landen omtrent de bescherming van persoonsgegevens een geheel andere systematiek volgen dan de EU-richtlijn. De vraag rijst op welke wijze de vanuit het EU-perspectief geformuleerde maatstaven in een anders ingericht systeem van rechtsbescherming moeten worden geïnterpreteerd. Dit probleem speelt onder meer een rol in de dialoog tussen de EU en de VS waarop hierna (par. 4.3) nog wordt ingegaan.

Daarnaast zijn er onderwerpen die binnen de EU zelf moeten worden behandeld. Allereerst is de vraag welke invulling moet worden gegeven aan het begrip «passend beschermingsniveau». Zoals hierna zal worden aangegeven (par. 4.2) heeft de op artikel 29 van de richtlijn ingestelde werkgroep, bestaande uit vertegenwoordigers van de nationale toezichthouders (hierna: de artikel 29-werkgroep) hiervoor criteria ontwikkeld.

Thans bevinden wij ons in de fase waarin aan de hand van de toetsing van het beschermingsniveau in een aantal landen bezien wordt in hoeverre deze criteria bruikbaar zijn. Op grond van de ervaringen die daarbij zijn opgedaan, zal vastgesteld moeten worden in hoeverre aanpassing of verdere precisering van deze criteria noodzakelijk is. Eenzelfde problematiek is aan de orde bij de toepassing van artikel 26, vierde lid. Hierin wordt bepaald dat de Commissie kan beslissen dat modelcontracten «voldoende waarborgen» bevat als basis voor gegevensverkeer met derde landen. Ook hier zal de nadere invulling nog de nodige aandacht vergen. In paragraaf 4.5 komen wij hier nog op terug.

Een ander belangrijk probleem waarover thans nog overleg plaatsvindt betreft de rechtsgevolgen van een beslissing van de Commissie ex artikel 25, zesde lid. Sommige lidstaten hebben zich op het standpunt gesteld dat een dergelijke beslissing de bevoegdheid van de lidstaten onaangetast laat om in specifieke omstandigheden het gegevensverkeer te blokkeren op basis van een eigen oordeel over de situatie in het desbetreffende derde land. Naar hun oordeel vloeit dit voort uit de in de nationale rechtsorde geldende beginselen betreffende de rechtsbescherming van de burger. Andere lidstaten – waaronder Nederland – alsmede de Commissie menen daarentegen dat de op de richtlijn gebaseerde Commissiebeslissing voorrang heeft boven het nationale recht en aldus aan de blokkeringsbevoegdheid van de lidstaten als hiervoor bedoeld een einde maakt. Dit is ook in overeenstemming met de ratio van artikel 25, zesde lid. Met de vaststelling dat een bepaald derde land beschikt over een passend beschermingsniveau (met inbegrip van een goede rechtsbescherming voor de burger) wordt rechtszekerheid beoogd. Deze wordt niet gerealiseerd indien de lidstaten – ondanks een beslissing ex artikel 25, zesde lid – de onbeperkte bevoegdheid houden om een doorgifte te verbieden of te beperken op basis van een eigen oordeel over het beschermingsniveau in het desbetreffende derde land. Thans bereidt de Commissie een gemeenschappelijke oplossing voor waarbij in de beslissing van de Commissie zelf een zeer beperkte bevoegdheid van de lidstaten wordt vastgelegd om een doorgifte tijdelijk op te schorten. Dit zou alleen zijn toegestaan indien zou blijken dat het beschermingsniveau in een derde land in een concreet geval wordt ontdoken en als gevolg daarvan onherstelbare schade dreigt.

Uit het voorgaande blijkt dat beslissingen op grond van artikel 25, zesde lid, complex zijn en de nodige voorbereiding vergen. Uit het feit dat een beslissing met betrekking tot een derde land vooralsnog ontbreekt, mag dan ook niet worden afgeleid dat in dat land geen passend beschermingsniveau voorhanden is. Veel landen dienen nog nader worden onderzocht om te bezien of en op welke termijn zij voor een positieve vaststelling in aanmerking komen. Met een aantal landen is nog overleg gaande. In paragraaf 4.2 en 4.3 komen wij hier nog op terug.

4.2 Invulling «passend beschermingsniveau»

Voorafgaand aan de inwerkingtreding van Richtlijn 95/46/EG heeft de op artikel 29 van deze richtlijn gebaseerde werkgroep, bestaande uit vertegenwoordigers van de nationale toezichthouders, uit eigen beweging op 24 juli 1998 een advies uitgebracht omtrent de invulling van de artikelen 25 en 26 (DG XV D/5025/98). Een van de hoofdelementen van het advies omvat de criteria op basis waarvan beoordeeld zou moeten worden in hoeverre een derde land beschikt over een passend beschermingsniveau in de zin van artikel 25, eerste lid. Noch de Commissie, noch de lidstaten hebben omtrent dit advies een officieel standpunt ingenomen. In de praktijk blijkt evenwel dat de in het advies geformuleerde maatstaven een belangrijke leidraad vormen.

In het voormelde advies wordt in het kader van de beoordeling van het beschermingsniveau van het derde land een onderscheid gemaakt tussen de inhoud van de toepasselijke voorschriften en de instrumenten om de handhaving ervan te garanderen. Met betrekking tot de inhoud van de gegevensbescherming dienen volgens de artikel 29-werkgroep de navolgende beginselen te gelden:

1. *Specificiteit*. Gegevens moeten met een specifiek doel worden verwerkt en mogen enkel worden gebruikt en doorgegeven als dat niet onverenigbaar is met het doel van de doorgifte. Op dit beginsel zijn alleen uitzonderingen mogelijk als bedoeld in artikel 13 van de richtlijn.

2. *Kwaliteit en evenredigheid*. De gegevens moeten correct en geactualiseerd zijn. Zij moeten bovendien passend en relevant zijn met het oog op het doel van de doorgifte.

3. *Transparantie*. Aan de burger moet informatie worden verstrekt over het doel van de gegevensverwerking en de identiteit van degene die in het derde land voor de verwerking verantwoordelijk is, alsmede alle informatie die nodig is om een eerlijke gegevensverwerking te garanderen. Uitzonderingen op deze informatieplicht zijn alleen mogelijk binnen de grenzen zoals aangegeven van artikel 11, tweede lid en 13 van de richtlijn.

4. *Beveiliging*. Degene die verantwoordelijk is voor de gegevensverwerking moet technische en organisatorische beveiligingsmaatregelen treffen die in overeenstemming zijn met de risico's van de verwerking. Degenen die onder het gezag van de verantwoordelijke staat – met inbegrip van in opdracht verwerkende verwerkers – mag alleen op basis van zijn instructies gegevens verwerken.

5. *Rechten geregistreerden*. Burgers moeten recht hebben op toegang tot de eigen gegevens, alsmede recht op rectificatie indien de omtrent hem verwerkte gegevens onjuist blijken. In bepaalde situaties moeten betrokkenen ook het recht hebben om zich tegen verwerking van zijn gegevens te verzetten. Uitzonderingen op deze rechten zouden alleen moeten worden toegestaan in de gevallen als bedoeld in artikel 13 van de richtlijn.

Daarnaast heeft de werkgroep van toezichthouders maatstaven geformuleerd voor de handhaving in het derde land. De volgende eisen dienen in hun visie te gelden:

1. *Adequaat niveau van naleving*. Het niveau van naleving moet adequaat zijn; dit hang af van verschillende factoren. Allereerst is er de mate waarin zowel burgers als degenen die gegevens verwerken op de hoogte zijn over hun rechten en plichten. Uiteraard kan een goede voorlichting daartoe bijdragen. Voorts is de naleving van privacybeginselen afhankelijk van de mogelijkheid om bij de overtreding daarvan doeltreffende sancties op te leggen. Ook de mogelijkheid van directe controle door toezichthoudende autoriteiten, auditors of andere controleurs kan van invloed zijn.

2. *Verlening van bijstand*. Burgers moeten worden bijgestaan bij de uitoefening van hun rechten. Zij dienen hun rechten snel, doeltreffend en zonder hoge kosten te kunnen uitoefenen. Dit impliceert volgens de werkgroep tevens een institutioneel mechanisme voor onafhankelijk onderzoek van klachten.

3. *Passende schadeloosstelling*. Indien schade wordt geleden als gevolg van overtreding van privacyvoorschriften, dient deze op passende wijze te worden vergoed.

Omtrent de betekenis van de aldus geformuleerde eisen dient het navolgende in aanmerking te worden genomen. In de eerste plaats dienen zij steeds te worden geplaatst in de context van de tekst van de richtlijn. Artikel 25, eerste lid, stelt nadrukkelijk niet als voorwaarde dat het derde land voldoet aan het beschermingsniveau van de richtlijn zelf. Vereist is alleen dat de bescherming in het derde land gegeven de omstandigheden als «passend» valt te beschouwen. De soms bestaande neiging om de genoemde criteria te interpreteren overeenkomstig de desbetreffende bepalingen van de richtlijn is derhalve niet of althans niet zonder meer juist. Zo kan aan een derde land bijvoorbeeld niet de eis worden gesteld dat – in de geest van artikel 28 van de richtlijn – een onafhankelijke, toezichthoudend overheidsorgaan is ingesteld dat specifiek gericht is op de bescherming van persoonsgegevens. Deze eis is niet realistisch en miskent bovendien dat de handhaving van beschermingsbeginselen ook langs andere weg kan worden gerealiseerd.

Voorts gaat de richtlijn uit van een op de concrete situatie gerichte beoordeling van het beschermingsniveau. Dit veronderstelt dat niet steeds dezelfde criteria behoeven te gelden. Dit is ook het uitgangspunt van de artikel 29-werkgroep. In sommige gevallen zullen in verband met de omvang van het risico van een bepaalde doorgifte aanvullende eisen moeten gelden, in andere gevallen zal het mogelijk zijn van bepaalde vereisten af te zien. Bovenbedoelde criteria dienen in dit licht bezien te worden beschouwd als uitgangspunt voor de beoordeling van het beschermingsniveau in het derde land in kwestie.

4.3 Dialoog met de VS

Sinds twee jaar is er een intensieve dialoog gaande tussen de EU en de Verenigde Staten over het gegevensverkeer vanuit de EU naar de VS. De Amerikaanse regering streeft naar een verklaring van de Europese Commissie dat Amerikaanse bedrijven die zich gebonden achten aan bepaalde beginselen, voldoen aan het door de artikel 25, eerste lid, van de richtlijn vereiste beschermingsniveau. Door middel van een dergelijke verklaring kan zeker worden gesteld dat het toenemende gegevensverkeer via de electronische snelweg tussen de desbetreffende actoren in de EU en de VS zich verder kan blijven ontwikkelen.

Mede in verband met het grote belang van de uitwisseling van gegevensverkeer voor de internationale handelsbetrekkingen worden de besprekingen namens de VS gevoerd door het Amerikaanse ministerie van Handel. Namens de EG treedt de Commissie op. Haar taak is de voorstellen van de VS te toetsen aan de richtlijn en de daarop gebaseerde maatstaven. De Commissie wordt bijgestaan door het Comite van regeringsvertegenwoordigers ex artikel 31 van de richtlijn en de eerder genoemde artikel 29-werkgroep. Voorts is sinds de inwerkingtreding van het Verdrag van Amsterdam ook het Europees Parlement direct in de procedure betrokken. Overigens heeft de EU toegezegd om gedurende de lopende besprekingen op de voet van artikel 25 van de richtlijn geen doorgiftes aan de VS zullen worden geblokkeerd.

De lange duur van de lopende dialoog moet worden gezien tegen de achtergrond van het fundamentele verschil tussen de Amerikaanse en Europese benadering van het vraagstuk van gegevensbescherming. In veel Europese landen bestaat van oudsher algemene privacywetgeving. Een van overheidswege ingestelde onafhankelijke autoriteit is doorgaans belast met het toezicht op de naleving van de wet. Deze benadering klinkt op Europees niveau reeds door in het eerder genoemde Verdrag van de Raad van Europa van 1981. Het Verdrag is mede geïnspireerd door artikel

8 EVRM waarin het recht op bescherming van het prive-leven als grondrecht is verankerd. De EU-richtlijn van 1995 bouwt op deze traditie voort.

Anders dan in de EU-lidstaten bestaat in de VS geen algemene wetgeving voor de bescherming van persoonsgegevens. Er bestaat slechts wetgeving op een enkel deelterrein. De Amerikaanse benadering steunt hoofdzakelijk op het principe van zelfregulering. Indien er in het maatschappelijk verkeer problemen ontstaan met verwerkingen van persoonsgegevens, wordt de oplossing daarvan in beginsel overgelaten aan de vrije markt. Hieraan ligt de veronderstelling ten grondslag dat bedrijven het zich niet kunnen permitteren om onzorgvuldig om te gaan met persoonsgegevens van burgers, omdat als gevolg hiervan het vertrouwen van de consument dreigt te worden verspeeld. In deze context zijn de afgelopen jaren in de VS op grond van particulier initiatief verschillende zelfreguleringsmechanismen ontstaan: organisaties die tegen een (soms hoge) vergoeding het privacybeleid van bedrijven toetsen en controleren. In geval van een positief resultaat wordt een keurmerk afgegeven waarmee de desbetreffende bedrijven zich ten opzichte van hun klanten kunnen afficheren. Bij herhaalde overtreding van de privacyregels kan het keurmerk worden ingetrokken. Bij deze organisaties kunnen burgers ook een klacht indienen die volgens vooraf bepaalde procedures worden behandeld.

De invalshoek van het Amerikaanse systeem van zelfregulering is derhalve vooral gericht op behoud van het vertrouwen van de consument en niet primair – zoals doorgaans in Europa – op de bescherming van het recht op privacy als grondrecht. Dit verklaart ook dat bepaalde privacyprincipes in de VS veel nadruk krijgen, terwijl andere beginselen op weerstand stuiten. Centraal staat de vrije keuze van de consument. Deze moet goede informatie kunnen krijgen op basis waarvan hij zelf kan aangeven op welke wijze met zijn persoonsgegevens kan worden omgegaan. Daarnaast moet hij kunnen klagen bij een daartoe geëigende instantie. Deze principes zijn in overeenstemming met het gedachtengoed van Richtlijn 95/46/EG. Het doelbindingsprincipe dat in diezelfde richtlijn centraal staat, stuit in de VS daarentegen op de nodige bezwaren. De neiging om in de particuliere sector het gebruik van gegevens voor andere doeleinden dan waarvoor ze oorspronkelijk zijn verzameld, aan banden te leggen, is gering, mits de vrije keuze van de consument is gewaarborgd. Een voorwaarde in deze benadering is wel dat de burger op de hoogte is of kan zijn van de wijze waarop zijn persoonsgegevens worden gebruikt.

De rol van de overheid is in deze constellatie beperkt. Deze is gericht op de goede werking van de markt. Overheidsingrijpen is alleen dan aan de orde indien de marktwerking door oneerlijke concurrentie wordt verstoord. Bedrijven die zich schuldig maken aan misleiding van de consument of anderszins oneerlijke praktijken kunnen in de regel door de Federal Trade Commission (FTC) of een andere publieke toezichthouder worden aangepakt. Niet-naleving van door het desbetreffende bedrijf zelf gepubliceerd privacybeleid kan worden gesanctioneerd met hoge boetes. Dit zal in de praktijk echter alleen gebeuren indien zelfreguleringsmechanismen hebben gefaald. De invalshoek van de FTC is dus een geheel andere dan die van de Europese toezichthouders. Niet de bescherming van de persoonlijke levenssfeer als zodanig fungeert als toetssteen, doch de zorgvuldige omgang met de consument in de context van eerlijke concurrentie. Dit laat onverlet dat de FTC bereid en ook in staat lijkt om in voorkomende gevallen tegen privacyschendingen door het bedrijfsleven adequaat op te treden.

Gezien de aldus beschreven verschillen is begrijpelijk dat de betrokken partijen over en weer veel tijd hebben moeten investeren in het verkrijgen van inzicht in de wederzijdse posities. Daarnaast is het lastig gebleken om

oplossingen te vinden die passen in de systematiek van artikel 25, eerste lid, van de richtlijn. Vanwege het ontbreken van algemene regels was het voor de Commissie onmogelijk een verklaring af te geven inhoudende dat de VS in algemene zin zou beschikken over een «passend niveau van bescherming». Een andere mogelijkheid zou zijn geweest om de situatie in de VS per sector te beoordelen. Deze beoordeling is evenwel zeer gecompliceerd. De VS kent een verbrokkeld systeem van regels en beschermingsmechanismen dat op bepaalde terreinen ook nog eens per staat kan verschillen. Bovendien zijn bedrijven in toenemende mate in verschillende sectoren actief, zodat ingewikkelde grensgevallen zich gemakkelijk kunnen voordoen.

Om die reden heeft de Amerikaanse regering een alternatieve constructie voorgesteld. Dit houdt kort gezegd in dat de EU-verklaring alleen geldt voor Amerikaanse bedrijven die vrijwillig verklaren dat zij zich zullen houden aan een aantal door de Amerikaanse regering geformuleerde beginselen van gegevensbescherming (de zgn. Safe Harbour Principles). De voorgestelde constructie lijkt een goede basis voor een voor beide partijen bevredigende oplossing. De dialoog met de VS gaat op dit moment niet meer primair over de aanvaarding van de Safe Harbour-constructie als zodanig, maar vooral over de inhoud van de Safe Harbour Principles en de daaraan te geven interpretatie. Met name de op de handhaving betrekking hebbende beginselen bleken tijdens de besprekingen nog steeds de nodige vragen en knelpunten op te leveren.

De inzet van de Nederlandse regering is om in samenspraak met de andere lidstaten en de betrokken Europese instellingen zo spoedig mogelijk – mogelijk reeds binnen enkele weken – te komen tot een positief resultaat. Daarbij dient in aanmerking te worden genomen dat de afgelopen twee jaar reeds veel is bereikt. De Amerikaanse voorstellen bevatten belangrijke bouwstenen die voor de desbetreffende bedrijven kunnen leiden tot een passende bescherming van persoonsgegevens. Gelet op de in de voorstellen voorziene evaluatiebepaling zal op termijn moeten worden bezien hoe de Safe Harbour-constructie in de praktijk heeft gewerkt en in hoeverre deze op grond van de opgedane ervaringen aanpassing behoeft.

Het voorgaande laat onverlet dat de huidige voorstellen nog op een enkel punt kunnen worden verbeterd. Daarbij gaat het in het bijzonder om onderwerpen die een goede werking van de Safe Harbour-constructie moeten verzekeren. Algemeen wordt de opvatting gedeeld dat een toegankelijke lijst beschikbaar moet zijn waaruit ondubbelzinnig blijkt welke bedrijven wel en welke bedrijven niet of niet meer tot de Safe Harbour behoren. Dit is bijvoorbeeld van belang in situaties waarin een bedrijf verklaard heeft zich aan de Safe Harbour-principes te houden en waar vervolgens na onderzoek door daartoe bevoegde instanties blijkt dat de beginselen systematisch worden overtreden. De vraag is welke gevolgen aan dergelijke omstandigheden kunnen worden verbonden binnen de grenzen van het Amerikaanse rechtssysteem. Voorts wordt onder meer nog gesproken over de inpassing van enkele specifieke Amerikaanse wetten in het Safe Harbour-systeem, de rol die de Europese toezichthouders zouden kunnen spelen bij de handhaving van de Safe Harbour-principes en het overgangsrecht.

4.4 Situatie in andere derde landen

De langdurige en intensieve besprekingen met de VS lijken er soms toe leiden dat de relaties met andere derde landen op de achtergrond raken. Niettemin onderhoudt de Commissie met velen van hen contacten. Dit geldt in de eerste plaats voor de Europese landen die kandidaat zijn om

toe te treden tot de Europese Unie. Deze zullen bij een eventuele toetreding moeten voldoen aan de eisen van Richtlijn 95/46/EG, omdat deze behoort tot het «acquis communautaire». Op termijn zal derhalve een ander niveau van bescherming moeten worden gerealiseerd dan van derde landen krachtens artikel 25, eerste lid, wordt gevergd. In de tussentijd zou evenwel een beslissing van de Commissie op grond van artikel 25, zesde lid, met het oog op de voortzetting en verdere ontwikkeling van het onderlinge gegevensverkeer uitkomst kunnen bieden.

In de tweede plaats bestaan er contacten met de landen die geen lid zijn van de Europese Unie, maar wel partij zijn bij het eerder genoemde Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van het individu in verband met de geautomatiseerde registratie van persoonsgegevens. Gezien de gebondenheid van deze landen aan de daarin vervatte beginselen en de aldaar aanwezige nationale wetgeving, beschikken deze landen op veel punten over een «passend niveau van bescherming». Te verwachten valt dat na consultatie van het Comite van regeringsvertegenwoordigers de Commissie op zeer korte termijn op grond van artikel 25, zesde lid, een positieve beslissing zal nemen met betrekking tot Zwitserland en Hongarije. Omdat het de eerste beslissingen zouden zijn op deze grond, zal vanwege de te verwachten precedentwerking de motivering van de beslissing nog de nodige aandacht behoeven. Het overleg hierover is nog gaande.

Naast de Europese landen zijn er – afgezien van de VS – ook contacten gelegd met landen buiten Europa. Dit geldt in het bijzonder voor Canada, Japan, Australië en Nieuw-Zeeland. Op de kortere termijn lijken Canada en Australië – na totstandkoming van de aldaar in voorbereiding zijnde wetswijzigingen – voor een beslissing ex artikel 25, zesde lid, van de richtlijn in aanmerking te kunnen komen. Voorts zijn er contacten geweest met derde landen waarmee de EU samenwerkings- of associatieovereenkomsten heeft gesloten. In een deel van deze overeenkomsten zijn inmiddels specifieke bepalingen inzake gegevensbescherming opgenomen. Een voorbeeld hiervan vormt Mexico. Op de langere termijn is een beslissing ex artikel 25, zesde lid, van de richtlijn ten aanzien van sommige van deze landen wellicht mogelijk.

4.5 Modelcontracten

Zoals hiervoor uiteengezet biedt artikel 26, vierde lid, van de richtlijn de mogelijkheid voor de Commissie om vast te stellen dat bepaalde modelcontracten voldoende waarborgen bieden met het oog op de bescherming van de persoonlijke levenssfeer en andere fundamentele rechten en vrijheden. Het contract als instrument voor internationale gegevensuitwisseling is niet nieuw. Reeds in 1992 hebben de Raad van Europa, de International Chamber of Commerce (ICC) en de Europese Commissie gezamenlijk een studie laten verrichten naar de inrichting van contracten met het oog op internationaal gegevensverkeer. In een aantal lidstaten worden al met dit doel contracten gebruikt.

In verband met de toepassing van artikel 26, vierde lid, is de vraag wat moet worden verstaan onder «voldoende waarborgen». Met de artikel 29-werkgroep zijn wij van oordeel dat het in de rede ligt om uit te gaan van vergelijkbare criteria als bij de bepaling van het passende beschermingsniveau in de context van artikel 25, zesde lid. In zijn eerder genoemde advies heeft de werkgroep dit verder uitgewerkt. In samenspraak met de Commissie en de andere lidstaten zal moeten worden onderzocht in hoeverre deze criteria in de context van een contractuele relatie een specifieke vertaling behoeven. Daarbij dient in aanmerking te worden genomen dat het – anders dan in artikel 25 – doorgaans gaat om

gegevensdoorgiften waarbij in het desbetreffende derde land geen passend beschermingsniveau aanwezig is en derhalve oplossingen dienen te worden gezocht die zijn toegesneden op de situatie in het concrete geval.

Met name als het gaat om de handhaving kunnen zich problemen voordoen. In bepaalde gevallen is het wellicht mogelijk dat contractueel wordt vastgelegd dat degene die vanuit de EU gegevens verstrekt, verantwoordelijk blijft voor de gegevensverwerking die in het derde land wordt uitgevoerd. De ontvanger in het derde land is dan verwerker die slechts mag handelen conform de instructies van de Europese verantwoordelijke. Een andere mogelijkheid is dat degene die gegevens doorgeeft contractueel aansprakelijk blijft voor schade als gevolg van overtreding door de ontvanger van de overeengekomen beginselen van gegevensbescherming. De eerstgenoemde kan daarop in een of meer de EU-lidstaten worden aangesproken.

Thans onderzoekt de Commissie de mogelijkheden om te komen tot een adequate toepassing van artikel 26, vierde lid. Dit zou kunnen leiden tot voorstellen omtrent een of meer modelcontracten waarin is voorzien in de door de richtlijn vereiste waarborgen. Deze zullen tezijnertijd worden besproken met de lidstaten en de nationale toezichthouders. Voorts is van belang dat de ICC op dit terrein initiatieven heeft genomen en in juli 1999 is gekomen met een concept voor modelbepalingen (Model clauses for use in contracts involving transborder data flows, 13 juli 1999). Deze zullen bij de verdere behandeling van het vraagstuk door de Commissie en de lidstaten in de overwegingen moeten worden betrokken.

Naast de toepassing van artikel 26, vierde lid, zijn ook verdere ontwikkelingen op nationaal niveau te verwachten. Zoals hiervoor aangegeven kan de minister van Justitie op grond van artikel 77, tweede lid, van het voorstel van Wet bescherming persoonsgegevens een vergunning afgeven voor doorgiften naar een derde land zonder een passend beschermingsniveau. Aan een dergelijke vergunning dienen de nadere voorwaarden te worden verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer en andere fundamentele rechten te waarborgen. Deze waarborgen kunnen – mede in het licht van artikel 26, tweede lid, van de richtlijn – voortvloeien uit contractuele bepalingen. In overleg met de Registratiekamer – het toekomstige College bescherming persoonsgegevens – zal nader worden bezien op welke wijze deze bevoegdheid dient te worden uitgeoefend.

4.6 Handhaving

Bij het toezicht op de naleving van artikel 25 en 26 dient onderscheid te worden gemaakt tussen enerzijds de situatie waarin het derde land krachtens een beslissing van de Commissie beschikt over een passend beschermingsniveau als bedoeld in artikel 25, eerste lid, en anderzijds de situatie waarin een dergelijke beslissing niet voorhanden is. In het eerste geval ligt de bescherming op een zodanig niveau dat in beginsel het gegevensverkeer vanuit de EU ongestoord kan plaatsvinden. Het derde land draagt in dat geval zorg voor de handhaving van de beginselen van gegevensbescherming voor zover het gaat om de verwerking van gegevens die na ontvangst uit de EU in het desbetreffende derde land plaatsvinden. De hiervoor beschreven criteria (par. 4.2) ter bepaling van het beschermingsniveau gaan daar ook van uit. Volgens deze criteria behoort een derde land te beschikken over adequate handhavingsmechanismen.

Indien een passend beschermingsniveau in het derde land aanwezig is, is de rol van de EU bij het toezicht op de naleving beperkt. In de eerste

plaats dient de Commissie in samenspraak met de lidstaten op regelmatige tijdstippen te bezien of het beschermingsniveau in een derde land nog steeds aan de gestelde maatstaven voldoet. Daartoe zullen in de beslissingen van de Commissie als bedoeld in artikel 25, zesde lid, evaluatiebepalingen worden opgenomen. Daarnaast is een bescheiden rol weggelegd voor de nationale toezichthoudende autoriteiten. Deze kunnen in bepaalde situaties EU-burgers voorzien van informatie en advies omtrent de situatie in derde landen. Het ligt in de rede dat daartoe tevens contacten zullen worden onderhouden met de instanties die in het derde land zijn belast met de handhaving. Denkbaar is dat de toezichthoudende autoriteiten van de EU-landen op dit terrein hun activiteiten zullen coördineren. Zonodig zal ook de Commissie daarin worden betrokken. Zoals hiervoor uiteengezet (par. 4.1) zullen nationale instanties daarnaast een zeer beperkte bevoegdheid krijgen om een specifieke doorgifte naar een derde land met een passend beschermingsniveau tijdelijk op te schorten. Dit zal alleen zijn toegestaan indien zou blijken dat het beschermingsniveau in het derde land in een concreet geval wordt ontdoken en als gevolg daarvan ernstige schade dreigt.

De situatie is geheel anders indien een beslissing op grond van artikel 25, zesde lid, niet of nog niet is genomen. In dat geval geldt dat doorgifte van gegevens naar een derde land behoudens uitzonderingen, niet is toegestaan. De nationale toezichthoudende autoriteiten – voor Nederland de Registratiekamer, tevens het toekomstige College bescherming persoonsgegevens – zullen erop moeten toezien dat dit verbod wordt nageleefd. Het ligt in de rede dat zij zich bij het toezicht zullen richten op de categorieën van doorgiften die uit een oogpunt van bescherming van de persoonlijke levenssfeer bijzondere risico's opleveren. In het eerder genoemde advies van 24 juli 1998 heeft de werkgroep van nationale toezichthouders de volgende risicodragende categorieën onderscheiden:

– doorgiften waarbij gevoelige gegevens zijn betrokken als bedoeld in artikel 8 van de richtlijn (vgl. artikel 16 van het voorstel van Wet bescherming persoonsgegevens);
– doorgiften die een financieel risico inhouden (bv. creditcardbetalingen via Internet);
– doorgiften die een gevaar voor de veiligheid van de personen inhouden;
– doorgiften die verband houden met beslissingen die voor de betrokkene van groot belang zijn (bv. werving en selectie, promotie, kredietverlening);
– doorgiften die schade kunnen toebrengen aan de eer en goede naam van betrokkene;
– herhaalde doorgifte van grote hoeveelheden gegevens (bv. via Internet verwerkte electronische gegevens);
– doorgiften die betrekking hebben op versleutelde of geheime verzameling van gegevens (zoals «Internet-cookies» of electronische visitekaartjes);
– doorgiften die anderszins een duidelijke inbreuk op de persoonlijke levenssfeer vormen (bv. ongewenste telefonische contacten).

Indien het College in het kader van zijn toezichthoudende taak stuit op doorgiften naar een derde land dat niet behoort tot de categorie derde landen met een passend beschermingsniveau, kunnen zich verschillende situaties voordoen. In de eerste plaats dient te worden nagegaan of een van de in artikel 26 bedoelde uitzonderingen van toepassing is. Denkbaar is dat de desbetreffende doorgifte op basis van een toereikende contractuele bepaling of een van de andere in artikel 26, eerste lid, genoemde gronden plaatsvindt. Een andere mogelijkheid is dat de doorgifte ingevolge een door de minister ex artikel 77, tweede lid, van het voorstel van Wet bescherming persoonsgegevens afgegeven vergunning is toege-

staan. In al deze gevallen is de doorgifte naar het derde land – ondanks de afwezigheid van een passend beschermingsniveau – rechtmatig.

Indien evenwel geen van de in artikel 26 van de richtlijn bedoelde gronden van toepassing is, is de doorgifte onrechtmatig. In dat geval is de verantwoordelijke verplicht de doorgifte alsnog te beëindigen en de gevolgen van eerdere doorgiften zo mogelijk ongedaan te maken. Zonodig kan het College op grond van artikel 65 van het voorstel van Wet bescherming persoonsgegevens ter handhaving van deze verplichting bestuursdwang toepassen. De algemene bepalingen van de Algemene wet bestuursrecht zijn hierop van toepassing. Dit impliceert dat het College in plaats van bestuursdwang ook een last onder dwangsom kan opleggen.

Indien het College stuit op doorgiften waarbij na nader onderzoek duidelijk kan worden vastgesteld dat het desbetreffende derde land niet beschikt over een passend beschermingsniveau, dient de minister van Justitie hierover te worden geinformeerd. Indien hij het oordeel van het College deelt zal hij ingevolge artikel 78, eerste lid, onder a, de Commissie hiervan in kennis stellen. Vervolgens kan de Commissie op grond van artikel 25, vierde lid, van de richtlijn na raadpleging van de lidstaten beslissen dat een land niet beschikt over het vereiste beschermingsniveau. Doorgifte naar een derde land ten aanzien waarvan zulks door de Commissie is vastgesteld, zal krachtens artikel 75, eerste lid, van het voorstel van Wet bescherming persoonsgegevens strafbaar worden gesteld.

5. Slot

De artikelen 25 en 26 Richtlijn 95/46/EG inzake de doorgifte van gegevens van de EU naar derde landen krijgen in verband met het exponentieel toenemende internationale gegevensverkeer, een steeds grotere betekenis. Vanuit een economisch perspectief bezien is het van groot belang dat dit gegevensverkeer zich verder kan ontwikkelen. Krachtens Europees recht is dit in beginsel echter alleen aanvaardbaar indien derde landen waarnaar gegevens worden getransporteerd, ter bescherming van de persoonlijke levenssfeer en andere fundamentele rechten beschikken over een passend beschermingsniveau.

Uit deze nota blijkt dat het Europese beleid terzake van toepassing van de artikelen 25 en 26 Richtlijn 95/46/EG nog niet volledig tot ontwikkeling is gekomen. Naar onze opvatting moeten de Commissie en de lidstaten zich de komende tijd intensief inspannen om te komen tot verklaringen, inhoudende dat bepaalde derde landen beschikken over een «passend beschermingsniveau». Naar de mening van de Nederlandse regering liggen hier de nodige mogelijkheden. Voorts dient er een Europees beleid tot stand te komen inzake modelcontracten als mogelijke basis voor gegevensverkeer. In het kader van de in artikel 33 voorziene evaluatie van Richtlijn 95/46/EG zal ten slotte aandacht dienen te worden besteed aan de werking van artikel 25 en 26 en de wijze waarop deze in de praktijk worden gehandhaafd. Het betreft immers een geheel nieuw object van regelgeving op Europees niveau. De eerstkomende jaren zullen de ervaringen op dit terrein nauwlettend moeten worden gevolgd. Zo nodig zullen aanpassingen of preciseringen van de richtlijn overwogen dienen te worden.