COLLEGE BESCHERMING PERSOONSGEGEVENS

Nota derde landen. De doorgifte van persoonsgegevens naar derde landen in het kader van de WBP

Diana Alonso Blas, LL.M.
Senior beleidsmedewerker
Internationale zaken

Inhoudsopgave

Inleiding

Hoofdstuk 11 (artikelen 76-78) van de Wet bescherming persoonsgegevens (WBP) van 6 juli 2000[1] bevat een speciale regeling voor de doorgifte van persoonsgegevens vanuit Nederland naar derde landen. Met een derde land wordt een land buiten de EU bedoeld. De vereisten van artikelen 76 t/m 78 WBP werden aangenomen als uitwerking van Hoofdstuk IV van Europese Richtlijn 95/46/EG van het Europese Parlement en van de Raad van de Europese Unie van 24 oktober 1995, over de bescherming van personen met betrekking tot de verwerking van en het vrije verkeer van persoonsgegevens[2].
Deze Richtlijn heeft twee doelen: enerzijds beoogt de Richtlijn een hoog beschermingsniveau te bieden voor het recht op privacy met betrekking tot de verwerking van persoonsgegevens en anderzijds beoogt de Richtlijn vrij verkeer van dergelijke gegevens binnen de Europese Unie[3] mogelijk te maken. Als persoonsgegevens naar een derde land moeten worden doorgegeven, wordt daaraan door deze Richtlijn speciale voorwaarden verbonden. Doorgifte mag alleen plaatsvinden als daarbij wordt voldaan aan de vereisten van de Richtlijn.

Dit beleidsdocument biedt een leidraad voor de toepassing en interpretatie van dit hoofdstuk van de WBP voor iedereen die persoonsgegevens naar derde landen wil doorgeven. Er worden voorbeelden gegeven om de bedoeling van het document te verduidelijken en in het laatste hoofdstuk is een aantal praktijkvoorbeelden opgenomen. Natuurlijk worden daarin niet alle problemen behandeld waar een verantwoordelijke in de praktijk mee wordt geconfronteerd. Het College bescherming persoonsgegevens (CBP) benadrukt daarbij dat de meeste praktische vragen alleen kunnen worden beantwoord in het licht van de specifieke omstandigheden die per geval zullen verschillen; met andere woorden, een oplossing vinden vereist doorgaans maatwerk.

Dit document is gericht op artikelen 76 t/m 78 WBP; er wordt alleen naar andere artikelen van deze wet verwezen als dat nodig is voor het begrip van de tekst. Het spreekt voor zich dat alle overige bepalingen van de WBP van kracht blijven. Een eventuele doorgifte naar derde landen die onder het toepassingsgebied van de wet valt, is alleen rechtmatig als wordt voldaan aan alle bepalingen van de WBP die op dat specifieke geval van toepassing zijn[4].

[1] Staatsblad 2000, nr. 302.
[2] Publicatieblad van de Europese Gemeenschappen L 281, p. 31, 23 november 1995. Hierna te noemen “de Richtlijn”.
[3] Aangezien de Richtlijn eveneens van toepassing is op de landen van de Europese Economische Ruimte, wordt aldaar hetzelfde regime gevolgd. Waar in de tekst EU wordt genoemd, dient dan ook EU/EER te worden gelezen.
[4] Voor alle andere vragen over de toepassing van de WBP, zie het memorie van toelichting bij de wet of de richtlijnen die door het Ministerie van Justitie zijn gepubliceerd (“Handleiding voor bewerkers van persoonsgegevens”). Een Engelstalige versie hiervan is beschikbaar op: http://www.minjust.nl:8080/a_beleid/thema/wbp/manual/handleidingwbpuk.pdf

Daarbij moet niet worden vergeten dat, aangezien de WBP een implementatie is van de Richtlijn in de Nederlandse wet, de tekst van de Richtlijn soms een belangrijke rol speelt voor een correcte interpretatie van de bepalingen van deze wet. Daarom wordt in dit document op enkele plaatsen naar de Richtlijn verwezen. Er wordt ook een aantal documenten aangehaald dat door de zogeheten werkgroep voor de bescherming van personen met betrekking tot de verwerking van persoonsgegevens[5] werd goedgekeurd, aangezien ze waardevolle interpretaties bieden van diverse aspecten van de Richtlijn. De praktijk heeft uitgewezen dat deze documenten vaak de basis vormen voor discussies die in Brussel worden gevoerd over grensoverschrijdend gegevensverkeer.

De Minister van Justitie en het CBP spelen beide een belangrijke rol met betrekking tot de toekenning van vergunningen, een van de belangrijkste onderwerpen van dit document. De Minister is bevoegd een definitieve beslissing te nemen over een aanvraag voor een vergunning, waarbij hij rekening houdt met het advies van het CBP. Het CBP vervult voor de Minister een adviserende rol en fungeert tegelijkertijd als een toezichthoudend orgaan voor de betreffende verwerkingsprocedures, niet alleen op het moment dat er over de aanvraag wordt besloten, maar ook nadat de vergunning is toegewezen.
De Minister van Justitie is verplicht het CBP zijn mening te vragen voordat de vergunning wordt toegekend. Volgens de tekst van een memorie van toelichting bij de WBP[6], speelt het advies van het CBP in dit verband een belangrijke rol; het draagt bij tot de kwaliteit van de besluitvorming over vergunningen vanwege de deskundigheid en ervaring van het college op dit gebied.

Dit document werd opgesteld door College bescherming persoonsgegevens. Om de procedure voor de toekenning van vergunningen sneller en gebruiksvriendelijker te doen verlopen, hebben het CBP en het Ministerie van Justitie echter overeenstemming bereikt over de hoofdlijnen van dit document. Zodoende hebben het college en het Ministerie een gemeenschappelijk inzicht in deze materie ontwikkeld, hetgeen hen in staat stelt deze gevallen op consequente en samenhangende wijze te behandelen.

[5] Deze werkgroep is opgericht op grond van Artikel 29 van de Europese Richtlijn, die de samenstelling en het takenpakket ervan bepaalt. Zie voor meer informatie het artikel van ALONSO BLAS, D., *Towards an uniform application of the European Data Protection Rules: The role of the Article 29 Working Party* (Naar een eenduidige toepassing van de Europese Regels inzake Gegevensbescherming: De rol van de Werkgroep als bedoeld in Artikel 29) in *Privacy & Informatie*, 4e jaargang, nummer 1, februari 2001. Alle door de werkgroep goedgekeurde documenten zijn beschikbaar op de website van de Europese Commissie: http://www.europa.eu.int/comm/privacy
[6] Pagina 195.

1. Toepassingsgebied van de voorschriften en algemene overwegingen

De regeling die in hoofdstuk 11 WBP is vastgelegd, geldt voor alle situaties waarin een verantwoordelijke binnen het toepassingsgebied van deze wet beoogt persoonsgegevens door te geven aan een derde land.

1.1. Toepassingsgebied van de WBP

Het toepassingsgebied van de WBP is vastgelegd in artikel 4. De WBP is van toepassing op de verwerking van alle persoonsgegevens in het kader van de activiteiten van een vestiging van een verantwoordelijke in Nederland. Het is dan ook noodzakelijk in de eerste plaats vast te stellen wie de verantwoordelijke is, ofwel de persoon die daadwerkelijk verantwoordelijk is voor de verwerking; in de tweede plaats moet bepaald worden of de verwerking plaatsvindt in het kader van de activiteiten van zijn/haar vestiging in Nederland.

De WBP is ook van toepassing op de verwerking van persoonsgegevens door of voor verantwoordelijken die niet in het rechtsgebied van de Europese Unie zijn gevestigd, waarbij ten behoeve van de verwerking van persoonsgegevens gebruik wordt gemaakt van apparatuur, geautomatiseerd of anderszins, die op Nederlands grondgebied is geplaatst, tenzij dergelijke apparatuur alleen wordt gebruikt voor transport door het rechtsgebied van dit land. Dit is bijvoorbeeld het geval als een verantwoordelijke die buiten de Europese Unie is gevestigd, gebruik maakt van cookies om in Nederland[7] persoonsgegevens te verzamelen, of die gebruik maakt van een in Nederland gevestigde bewerker.

Waar de WBP van toepassing is, moeten alle relevante bepalingen van de wet worden nageleefd. Of persoonsgegevens al dan niet rechtmatig mogen worden verwerkt en doorgegeven aan derden wordt altijd op nationaal niveau bepaald, los van mogelijke internationale aspecten van de doorgifte. Een van de verplichtingen die middels deze wet is vastgelegd, luidt dat verantwoordelijken hun verwerkingen moeten aanmelden bij het College bescherming persoonsgegevens, tenzij ze onder een van de uitzonderingen vallen die zijn vastgelegd in het koninklijk besluit van 7 mei 2001[8] voor vrijstelling van melding.

1.2. Wat is een doorgifte van persoonsgegevens?

Vaak wordt de term “doorgifte van persoonsgegevens” geassocieerd met activiteiten waarbij persoonsgegevens van het ene naar het andere land worden verstuurd, bijvoorbeeld door verzending van documenten op papier of in elektronische vorm via de post of via e-mail. Dat is inderdaad een vorm van doorgifte, maar er zijn andere situaties die ook onder deze definitie vallen: alle gevallen waarbij een verantwoordelijke een activiteit uitvoert met het doel persoonsgegevens beschikbaar te stellen aan een derde persoon die in een derde land is

[7] Zoals genoemd in het document van de Artikel 29-werkgroep ‘Een geïntegreerde EU-benadering van online Gegevensbescherming’, aangenomen op 21 november 2001, WP 37 en het ‘Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites’, aangenomen op 30 mei 2002, WP 57.

[8] Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet Bescherming Persoonsgegevens (Vrijstellingsbesluit WBP), Staatsblad 2001 250.

gevestigd. De memorie van toelichting bij de WBP[9] stelt dat het begrip "doorgifte" in artikel 76 WBP verwijst naar het beschikbaar maken van persoonsgegevens aan een persoon buiten het rechtsgebied van een van de landen van de Europese Unie.

Het volgende is een voorbeeld van een verwerking die onder de definitie van doorgifte valt: een multinational die wereldwijd actief is, besluit gegevens over haar werknemers beschikbaar te stellen aan alle dochterondernemingen. Daartoe wordt een database of een server geïnstalleerd in een van de landen waar de multinational is gevestigd. Alle dochterondernemingen hebben toegang tot de database en kunnen persoonsgegevens invoeren, bekijken of downloaden, wat in de praktijk inhoudt dat het verkeer van persoonsgegevens zijn oorsprong vindt in elk van de betrokken landen.Gegevens worden dus zowel ontvangen door de database, als vanuit de database naar de diverse landen verzonden. Als gevolg daarvan worden persoonsgegevens geografisch gezien verplaatst van Nederland naar diverse derde landen.

Een vraag die in dit verband vaak wordt gesteld, betreft informatie die op een website wordt gepubliceerd. Betekent het feit dat informatie op het internet potentieel toegankelijk is vanuit een willekeurige locatie op de wereld, dat de activiteit van het plaatsen van persoonsgegevens op een website altijd moet worden beschouwd als doorgifte naar derde landen? Deze vraag werd door een Zweedse rechter voorgelegd aan het Europese Hof van Justitie in Luxemburg met betrekking tot een prejudiciële uitspraak in de zogenaamde zaak Lindqvist[10].
De Nederlandse overheid heeft in dit geval een aantal bevindingen ingediend, in het bijzonder met betrekking tot het begrip doorgifte. De Nederlandse overheid is van mening dat de term doorgifte moet worden opgevat als een activiteit die bewust wordt ondernomen met als doel de verzending van persoonsgegevens vanuit het rechtsgebied van een Lidstaat naar een derde land. Informatie beschikbaar stellen via het internet door middel van een website is een vorm van publicatie. Verschillende vormen of methoden van publicatie of ontsluiting van persoonsgegevens kunnen verschillende methoden van bescherming vereisen. Het afdrukken van namen en telefoonnummers in een papieren telefoongids is iets anders dan het plaatsen van dezelfde gegevens op een CD-ROM of publicatie daarvan op een publiekelijk toegankelijke website. Al deze verschillende vormen van ontsluiting van gegevens brengen specifieke risico's met zich mee die allemaal op verschillende manieren moeten worden benaderd.
Een element dat in deze discussie een rol zou kunnen spelen is of de betreffende webpagina in feite aan een plaatselijk publiek is gericht (in de zaak Lindqvist was de website in het Zweeds gesteld) of dat de beheerder van de website zich tot een internationaal publiek wil richten (bijvoorbeeld door dezelfde webpagina in verschillende talen aan te bieden en door de website onder de aandacht te brengen via andere internationale websites en publicaties).
De zaak Lindqvist is nog in behandeling, zodat deze vraag op dit moment nog niet definitief kan worden beantwoord.

Een doorgifte is een vorm van verwerking volgens de definitie van artikel 1, onder b WBP. Dat houdt in dat een doorgifte pas rechtmatig is als deze voldoet aan alle vereisten van de WBP: er bestaat een wettelijke grondslag voor de verwerking (artikel 8), de gegevens worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7), in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze (artikel 6), de

[9] Memorie van toelichting, Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3, pagina 193.
[10] Rechtszaak C-101/01, Bodil Lindqvist versus Åklagarkammaren i Jönköping (Openbare Aanklager in Jönköping, Zweden).

gegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9) enzovoorts.
De noodzaak te voldoen aan alle vereisten van de WBP voor rechtmatige verwerking is van toepassing op alle vormen van doorgifte, naar een Lidstaat van de Europese Unie of naar een derde land. De bepalingen van hoofdstuk 11 WBP gelden daarnaast ook voor alle doorgiftes naar een derde land.

1.3. Op welke vormen van doorgifte zijn deze bepalingen van toepassing?

Zoals hierboven al werd aangegeven, moet elke doorgifte van persoonsgegevens (naar een Lidstaat of een derde land) voldoen aan de algemene vereisten van de WBP voor wettige en rechtmatige verwerking.

Er zijn geen andere eisen waaraan moet worden voldaan voor doorgiftes van persoonsgegevens tussen Lidstaten. Zoals de Richtlijn aangeeft in artikel 1, lid 2, mogen Lidstaten het vrije verkeer van persoonsgegevens binnen de Europese Unie niet beperken of verbieden om redenen die verband houden met de bescherming van de privacy van de betrokkenen.
Dat houdt in dat mits de verwerking voldoet aan de algemene vereisten van de WBP, de persoonsgegevens vrijelijk mogen worden doorgegeven binnen de Europese Unie. De bepalingen van hoofdstuk 11 WBP zijn in die situaties niet van toepassing.

De bepalingen van hoofdstuk 11 WBP zijn van toepassing op de doorgifte van persoonsgegevens naar derde landen, los van het feit of deze doorgifte plaatsvindt tussen twee verantwoordelijken of tussen een verantwoordelijke en een bewerker. De memorie van toelichting bij de WBP[11] benadrukt het feit dat het algemene verbod op de doorgifte van persoonsgegevens naar derde landen, tenzij wordt voldaan aan de bepalingen van hoofdstuk 11, zowel aan verantwoordelijken als aan bewerkers is gericht. Echter, het is inherent aan de aard van de bewerker dat hij alleen bevoegd is persoonsgegevens door te geven naar een derde land als hem daartoe opdracht wordt gegeven door de verantwoordelijke; een bewerker mag niet op eigen initiatief beslissen over doorgifte van gegevens. Dit document gaat dan ook uit van het feit dat er altijd een verantwoordelijke is die beslist over een doorgifte naar een derde land.

Net als alle andere bepalingen van de WBP is hoofdstuk 11 zowel op de publieke als de private sector van toepassing. Ondernemingen en organisaties in de publieke sector moeten allen aan deze voorschriften voldoen bij de doorgifte van persoonsgegevens naar een derde land. Verschillen in de aard van de verantwoordelijke kunnen echter gevolgen hebben voor de beoordeling van een specifieke situatie. Sommige uitzonderingen van artikel 77, lid 1 betreffen bijvoorbeeld situaties in de publieke sector.

1.4. Vanaf welke datum is de WBP van kracht?

Bij Koninklijk Besluit van 5 juli 2001[12] werd 1 september 2001 aangewezen als de datum waarop de WBP van kracht zou worden. Dat hield in dat alle nieuwe verwerkingen vanaf die datum moesten voldoen aan alle bepalingen van de WBP.

---

[11] Pagina 193.
[12] Besluit van 5 juli 2001, houdende vaststelling van het tijdstip van inwerkingtreding van de Wet Bescherming Persoonsgegevens, Staatsblad 2001 337.

Degenen die verantwoordelijk zijn voor verwerkingen die al voor die datum werden gestart, hebben volgens artikel 79, lid 1 WBP één jaar de tijd om ervoor te zorgen dat de verwerkingen aan de WBP voldoet.

Deze bepalingen zijn ook van toepassing op doorgiftes naar derde landen, hetgeen inhoudt dat doorgiftes die op 1 september 2001 al waren gestart, binnen één jaar na die datum zodanig moeten zijn aangepast dat ze voldoen aan de vereisten van de WBP. Nieuwe doorgiftes moeten direct vanaf het begin voldoen aan hoofdstuk 11 WBP.

2. De bepalingen van de WBP over grensoverschrijdend gegevensverkeer naar derde landen in drie stappen

Artikelen 76 t/m 78 WBP bevatten gedetailleerde voorschriften met betrekking tot doorgiftes van persoonsgegevens naar derde landen. Deze bepalingen vormen de uitwerking van hoofdstuk IV van de Richtlijn in de Nederlandse wetgeving. Op basis van de principes die in de Richtlijn zijn vastgelegd, wordt in de WBP een methode in drie stappen uiteengezet.

1. Als algemeen principe geldt dat persoonsgegevens alleen mogen worden doorgegeven naar landen met een passend beschermingsniveau.
2. Als het betreffende land geen passend beschermingsniveau kan bieden, kan de doorgifte alsnog rechtmatig plaatsvinden als deze onder een van de uitzonderingen valt die in de WBP zijn vastgelegd.
3. Als dat niet het geval is, kan de Minister van Justitie op verzoek van de verantwoordelijke en na advies te hebben ingewonnen van het College bescherming persoonsgegevens, een vergunning voor de doorgifte afgeven.

Elk van deze stappen wordt hieronder besproken.

Hierbij moet allereerst worden opgemerkt dat de volgorde waarin deze stappen worden genomen niet verplicht is voor de verantwoordelijke. Hij kan bijvoorbeeld besluiten een vergunning aan te vragen zonder de uitzonderingen van de wet te hebben geanalyseerd, of als hij denkt dat het te riskant is te vertrouwen op de aanwezigheid van passende bescherming in een derde land (bijvoorbeeld als er geen besluit van de Europese Commissie bestaat over dat land) of op een van de uitzonderingen.

De Richtlijn geeft de Lidstaten een beperkte speelruimte, niet alleen voor de nationale implementatie van de bepalingen van de Richtlijn maar ook met betrekking tot de verdeling van bevoegdheden op internationaal niveau voor beleid op dit gebied.
In dat opzicht is het belangrijk te bedenken dat artikel 25, lid 6 van de Richtlijn de Europese Commissie de bevoegdheid geeft een beoordeling te geven van het beschermingsniveau in een derde land.

Een dergelijk besluit van de Europese Commissie heeft directe gevolgen voor de Lidstaten. In dit kader bepaalt artikel 78 WBP dat, wanneer een besluit op Europees niveau is genomen, de Minister van Justitie bij Ministeriele regeling of beschikking vastlegt dat:

- de doorgifte naar een land buiten de Europese Unie verboden is;
- een land buiten de unie geacht wordt een passend beschermingsniveau te waarborgen, of
- een op grond van artikel 77 (2) verleende vergunning wordt ingetrokken of gewijzigd.

Daarnaast houdt hetzelfde artikel 78 WBP een verplichting in voor de Minister de Europese Commissie op de hoogte te stellen als, naar zijn mening, een derde land geen passend beschermingsniveau biedt en de Europese Commissie te informeren over vergunningen die ingevolge artikel 77, lid 2 zijn afgegeven. Zoals hierna wordt toegelicht, zijn de Europese Commissie en de andere Lidstaten gerechtigd hun mening te geven met betrekking tot dergelijke kennisgevingen van de Minister.

2.1. Is er sprake van een passend beschermingsniveau? (Artikel 76)

Het algemene principe dat in artikel 76 WBP is vervat, luidt dat persoonsgegevens alleen naar een derde land mogen worden doorgegeven als dat land, onverminderd de naleving van de wet, een passend beschermingsniveau waarborgt. Dit principe is op de Richtlijn gebaseerd, die de Lidstaten verplicht te garanderen alleen doorgiftes naar een derde land toe te staan als dat land een passend beschermingsniveau waarborgt.

2.1.1. Wat is passende bescherming?

Noch de WBP, noch de Richtlijn geeft een definitie van het begrip "passend beschermingsniveau". Beide wetsteksten bevatten echter een overzicht van omstandigheden waarmee rekening moet worden gehouden bij het beoordelen van een passend karakter in een specifiek geval[13]. Dit betreft:

- de aard van de gegevens;
- het doeleinde en de duur van de beoogde verwerking(en);
- het land van herkomst en het land van eindbestemming;
- de rechtsregels, zowel algemeen als sectorieel, die in het betreffende land van kracht zijn en
- de regels van het beroepsleven en de veiligheidsmaatregelen die in het derde land / land van eindbestemming worden nageleefd.

In een brief d.d. 9 maart 2000[14] heeft de Minister van Justitie de Tweede Kamer geïnformeerd over de toepassing van artikelen 25 en 26 van de Richtlijn. In deze brief verwijst de Minister naar de documenten die door de artikel 29-werkgroep zijn uitgegeven en die betrekking hebben op de interpretatie van artikelen 25 en 26 van de Richtlijn. Deze documenten zijn gebundeld verschenen op 24 juli 1998 als document WP 12[15].
De artikel 29-werkgroep is een onafhankelijk lichaam waarin alle Europese toezichthouders voor de bescherming van persoonsgegevens zijn vertegenwoordigd. De werkgroep heeft onder andere tot taak de Europese Commissie te adviseren over kwesties met betrekking tot de bescherming van gegevens en alle vraagstukken te bestuderen over de toepassing van de Richtlijn op nationaal niveau teneinde bij te dragen aan een uniforme toepassing van de Richtlijn. De praktijk heeft uitgewezen dat alle Communautaire besluiten die tot nu toe op dit gebied werden genomen, zijn gebaseerd op criteria die in dit document zijn vastgelegd als basis voor de analyse van de situatie in een bepaald land.

In het document van de werkgroep wordt een functionele benadering van deze materie ontwikkeld, waarbij de conclusies niet worden gebaseerd op de aard van de bestaande voorschriften, maar op de praktische resultaten die in een bepaald land werden bereikt. Daarbij wordt uitgegaan van het feit dat voorschriften voor gegevensbescherming alleen bijdragen tot de bescherming van personen als deze voorschriften in de praktijk worden opgevolgd. Wil een analyse van passende bescherming zinvol zijn, dan moet deze dus twee basiselementen omvatten: de inhoud van de betreffende voorschriften en de methoden waarmee de effectieve naleving ervan wordt gewaarborgd.

---

[13] Zie Artikel 76, lid 2 WBP en Artikel 25, lid 2 van de Richtlijn.
[14] Brief van de Minister van Justitie aan het Parlement van 9 maart 2000; Tweede Kamer, vergaderjaar 1999-2000, 27 043, nr. 1.
[15] Document van de Artikel 29-werkgroep 'Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikel 25 en 26 van de EU-Richtlijn betreffende Gegevensbescherming', WP 12.

Uitgaande van de Richtlijn en rekening houdend met de bepalingen van andere internationale teksten, definieert de werkgroep een "kern" van "inhoudelijke" principes voor gegevensbescherming en vereisten voor "procedures/handhaving". De Minister van Justitie heeft dezelfde criteria gehanteerd in zijn brief aan de Tweede Kamer van maart 2000, als toelichting hoe het begrip "passende bescherming" moet worden geïnterpreteerd.

De volgende inhoudelijke basisprincipes zouden moeten worden opgenomen in bestaande wettelijke voorschriften:

- Het principe van specificiteit: de gegevens mogen alleen voor een specifiek doeleinde worden verwerkt en mogen daarna alleen worden gebruikt of verder worden doorgegeven voorzover dat niet strijdig is met het doel van de doorgifte.
- Het principe van kwaliteit en evenredigheid: gegevens moeten nauwkeurig zijn en waar nodig actueel worden gehouden. De gegevens moeten passend, relevant en niet excessief zijn in verhouding tot het doel waarvoor ze worden doorgegeven of verder worden verwerkt.
- Het principe van transparantie: personen moeten worden geïnformeerd over het doel van de verwerking en de identiteit van de verantwoordelijke in het derde land en overige informatie voor zover die nodig is om een eerlijke gegevensverwerking te waarborgen.
- Het principe van beveiliging: de verantwoordelijke moet technische en organisatorische maatregelen nemen die zijn toegesneden op de risico's die de verwerking met zich meebrengt.
- Recht op toegang, rectificatie en verzet: de betrokkene moet het recht hebben kopieën te verkrijgen van alle verwerkte gegevens die op hem/haar betrekking hebben, evenals het recht onjuiste gegevens te rectificeren. In bepaalde omstandigheden moet hij/zij ook in staat worden gesteld zich te verzetten tegen de verwerking van gegevens die op hem/haar betrekking hebben.
- Beperking van verdere doorgifte aan derden die geen partij zijn in het contract: verdere doorgifte van de persoonsgegevens door de ontvanger van de oorspronkelijke gegevens mag alleen worden toegestaan als de tweede ontvanger (de ontvanger van de verdere doorgifte) voorschriften naleeft die een passend beschermingsniveau bieden.

Bij specifieke vormen van verwerking moet ook rekening worden gehouden met de volgende principes:

- Bijzondere gegevens: als het gaat om bijzonder gegevens[16], moeten aanvullende waarborgen worden geboden.
- Het recht van verzet bij gegevensverwerking ten behoeve van direct marketing: als gegevens worden doorgegeven ten behoeve van direct marketing, moet de betrokkene in elk willekeurig stadium van de doorgifte het recht hebben aan te geven dat zijn/haar gegevens niet voor dergelijke doeleinden mogen worden gebruikt.
- Geautomatiseerde individuele besluiten: als de doorgifte tot doel heeft het nemen van een geautomatiseerd besluit zoals bedoeld in artikel 15 van de Richtlijn, dan moet de persoon het recht hebben in kennis te worden gesteld van de logica die aan dat besluit ten grondslag ligt en moeten overige maatregelen worden genomen om de gerechtvaardigde belangen van de persoon te beschermen.

Deze principes moeten worden gelezen en geïnterpreteerd in het licht van de Europese Richtlijn.

[16] Voor een definitie van bijzondere gegevens, zie Artikel 8 van de Richtlijn en Artikel 16 WBP.

Er worden drie criteria gegeven om de effectiviteit te beoordelen van de voorschriften voor gegevensbescherming:

- Goed niveau van naleving van de voorschriften: sommige elementen zoals het niveau van bewustzijn van verantwoordelijken en betrokkenen en het bestaan van effectieve, afschrikkende sancties spelen een belangrijke rol bij het bereiken van een goed niveau van naleving van de voorschriften.
- Verlening van bijstand aan afzonderlijke betrokkenen: een individu moet zijn/haar rechten snel en effectief kunnen doen gelden, hetgeen geen onoverkomelijke kosten met zich mee mag brengen. Hiertoe moet een institutioneel mechanisme in een of andere vorm beschikbaar zijn dat onafhankelijke behandeling van klachten mogelijk maakt. In Europa wordt deze functie vervuld door onafhankelijke toezichthouders zoals het CBP, maar in derde landen zijn ook andere systemen toelaatbaar, mits ondersteuning en hulp aan de betrokkenen wordt gewaarborgd.
- Passende schadeloosstelling voor getroffen partijen: er moeten passende procedures beschikbaar zijn om schadeloosstelling te bieden aan getroffen partijen als niet aan de voorschriften wordt voldaan. Dit is een essentieel element, dat een procedure van onafhankelijke beoordeling of arbitrage moet omvatten en dat het mogelijk maakt passende schadevergoedingen uit te keren en sancties te treffen.

Deze inhoudelijke principes en vereisten voor procedures en handhaving moeten worden beschouwd als minimumeisen waaraan de bescherming moet voldoen voordat deze in alle gevallen als passend kan worden aangemerkt. Zoals we later zullen zien spelen deze principes ook een belangrijke rol bij de beoordeling van de aanwezigheid van “passende waarborgen” in het kader van een vergunningaanvraag.
Een dergelijke lijst van minimumeisen biedt natuurlijk geen pasklare oplossing voor elke situatie. In sommige gevallen zullen er eisen aan moeten worden toegevoegd en in andere gevallen kan het zelfs mogelijk zijn enkele vereisten niet toe te passen. Het risico dat de doorgifte met zich meebrengt voor de betrokkene is een belangrijke factor in het vaststellen van de exacte eisenpakket voor een bepaald geval.

Het document van de artikel 29-werkgroep behandelt in het bijzonder de toepassing van de voornoemde benadering op zelfregulering in de industrie. Dat is vooral van belang omdat zowel de Richtlijn als de WBP regels van het beroepsleven en de veiligheidsmaatregelen die in dat land worden nageleefd, noemen bij de omstandigheden waarmee bij een specifieke doorgifte rekening moet worden gehouden.
De conclusies van dit deel van het document kunnen als volgt worden samengevat:

- Zelfregulering moet worden beoordeeld aan de hand van de hierboven aangegeven criteria (inhoudelijke principes en vereisten voor procedures/handhaving).
- Voordat een instrument voor zelfregulering kan worden beschouwd als een valide onderdeel van “passende bescherming”, moet het bindend zijn voor alle leden aan wie persoonsgegevens worden doorgegeven en moet het passende waarborgen bieden als de gegevens worden doorgegeven aan niet-leden.
- Het instrument moet transparant zijn en moet op hoofdlijnen de inhoud van alle basisprincipes van gegevensbescherming omvatten.
- Het instrument moet mechanismen omvatten waarmee een goed niveau van algemene naleving effectief wordt gewaarborgd. Dat kan bijvoorbeeld worden bereikt middels een stelsel van afschrikkende sancties en strafmaatregelen, of door middel van verplichte externe audits.
- Het instrument moet ondersteuning en hulp bieden aan individuele betrokkenen die worden geconfronteerd met een probleem met betrekking tot de verwerking van hun

persoonsgegevens. Er moet dan ook een gemakkelijk toegankelijk, onpartijdig en onafhankelijk lichaam beschikbaar zijn dat klachten van betrokkenen kan behandelen en kan oordelen over eventuele overtredingen.
- Het instrument moet passende genoegdoening waarborgen als de voorschriften niet worden nageleefd. Een betrokkene moet een oplossing van zijn/haar probleem worden geboden en passende schadevergoeding, voor zover relevant.

Uit het voorafgaande kan worden geconcludeerd dat de aard van de voorschriften waarin de basisprincipes zijn vervat niet de beslissende factor is, maar het feit dat de betreffende voorschriften bindend moeten zijn en moeten voldoen aan de vereisten voor procedures en handhaving.

2.1.2. Wie beslist in specifieke gevallen over een passend karakter?

Voordat een afzonderlijke doorgifte plaatsvindt, moet een beslissing worden genomen over het al dan niet bestaan van een passend beschermingsniveau voor dat specifieke geval. Volgens artikel 76, lid 2 WBP moet een beslissing worden genomen waarbij rekening wordt gehouden met de omstandigheden van elk afzonderlijk geval. De memorie van toelichting benadrukt het feit dat de verantwoordelijke[17] zelf degene is die in de eerste plaats beoordeelt of er sprake is van een passend beschermingsniveau voor een specifieke doorgifte.
De Minister van Justitie heeft deze visie bevestigd tijdens de bespreking in de Eerste Kamer, in antwoord op de vraag of een onderneming zelfstandig een besluit kan nemen over het beschermingsniveau van een land. In zijn antwoord wees hij erop dat een onderneming in de eerste plaats daarover zelf een oordeel kan vormen, maar dat een rechter vanzelfsprekend deze beslissing kan herzien. De Minister wees er ook op dat het in dergelijke gevallen raadzaam is contact op te nemen met het CBP of het Ministerie van Justitie.

Net als de andere bepalingen van de WBP is artikel 76 een materiële bepaling die per geval moet worden toegepast en geïnterpreteerd. In het kader van de WBP is de verantwoordelijke verantwoordelijk voor alle besluiten die betrekking hebben op de verwerking; hij kan ook aansprakelijk worden gesteld voor verlies of schade als de voorschriften van de WBP[18] niet worden nageleefd.
Een van de voornaamste elementen waarmee de verantwoordelijke rekening moet houden is het bestaan van een Communautair besluit of een ministeriële regeling of beschikking over het beschermingsniveau in het land waarnaar hij/zij gegevens wil doorgeven. Als er een positief besluit van de Europese Commissie bestaat met betrekking tot dat derde land, heeft de verantwoordelijke zekerheid over het rechtmatige karakter van de doorgifte, mits wordt voldaan aan eventuele voorwaarden die de Commissie in haar besluit daaraan heeft gesteld.

Als er op Communautair niveau geen beslissing is genomen, moet de verantwoordelijke de specifieke omstandigheden van het geval in beschouwing nemen (zoals omschreven in artikel 76, lid 2 WBP), de specifieke risico's en de specifieke situatie in het betreffende land beoordelen, waarbij hij rekening houdt met de criteria en functionele benadering die in paragraaf 2.1.1. zijn uiteengezet.
Dat houdt met name in dat voor een bepaalde doorgifte de verantwoordelijke niet noodzakelijkerwijs het beschermingsniveau van de algemene wetgeving van het derde land

[17] Pagina 193 van de memorie van toelichting. Dezelfde passage staat op pagina 55 van de Richtlijnen die gepubliceerd zijn door de Minister van Justitie.
[18] Zie Artikel 49 WBP, lid 3.

beoordeelt, maar van de specifieke bindende voorschriften die op de betreffende doorgifte van toepassing zijn (zoals bijvoorbeeld sectoriële rechtsregels) en van de mechanismen voor handhaving/procedures, evenals het bestaan van publieke onafhankelijke lichamen of instanties die belast zijn met toezicht op naleving van deze voorschriften, ondersteuning en hulp aan betrokkenen en waar nodig schadevergoeding.
Als de verantwoordelijke specifieke stappen moet nemen om de bescherming van de persoonsgegevens in die specifieke omstandigheden te waarborgen, bijvoorbeeld door een contract te ondertekenen met de ontvangende partij in dat derde land, kan men niet van passende bescherming spreken. In die situatie neemt de verantwoordelijke stappen om voor passende waarborgen te zorgen, op basis waarvan de Minister van Justitie[19] mogelijk een vergunning kan verlenen.

De memorie van toelichting[20] bij de WBP geeft aan dat de verantwoordelijke zich in geval van twijfel tot het CBP kan wenden voor nadere informatie. De verantwoordelijke kan ook andere informatiebronnen raadplegen over wetgeving voor de bescherming van persoonsgegevens in andere landen[21].
In dergelijke gevallen is het beleid van het CBP voornamelijk gericht op het verstrekken van algemene informatie. De beoordeling van een concreet beschermingsniveau in een specifiek geval moet door de verantwoordelijke zelf worden uitgevoerd, degene die juridisch verantwoordelijk is voor een dergelijke beslissing. Het CBP voert alleen beoordelingen van specifieke gevallen uit als er een zwaarwegend belang geldt dat een dergelijke beoordeling rechtvaardigt; als er bijvoorbeeld grote risico's aan de doorgifte zijn verbonden, als er aanzienlijke belangen op het spel staan of als betrokkenen een klacht hebben ingediend.

Het is voor de verantwoordelijken af te raden de doorgifte te laten doorgaan, tenzij de omstandigheden van het specifieke geval duidelijk aangeven dat in het derde land een passend beschermingsniveau wordt geboden. Bij twijfel moet een doorgifte niet op basis van een dergelijk besluit worden uitgevoerd; de doorgifte kan toch juridisch toelaatbaar zijn op basis van een van de uitzonderingen van artikel 77, lid 1 of een vergunning van de Minister van Justitie volgens artikel 77, lid 2 WBP. Deze mechanismen worden in detail besproken in paragraaf 2.2 en 2.3.

2.1.3. Wanneer en hoe beslist de Europese Commissie over een beschermingsniveau?

Artikel 25, lid 6 van de Richtlijn geeft de Europese Commissie de bevoegdheid een besluit te nemen over het al dan niet passende karakter van het beschermingsniveau. Daartoe moet de Commissie een specifieke procedure volgen die in artikel 31 van de Richtlijn is uiteengezet. De Commissie kan positief beslissen op basis van het nationale recht in dat land, of van de internationale verplichtingen die dat land is aangegaan.
Deze laatste mogelijkheid is vooral interessant aangezien deze niet alleen verwijst naar het bestaan van internationale conventies, verdragen of andere instrumenten van publiek internationaal recht, maar ook naar specifieke internationale afspraken die worden gemaakt na onderhandelingen die de Commissie kan aangaan teneinde een situatie recht te zetten die is ontstaan na een negatieve beslissing[22].

[19] Zie voor meer informatie paragraaf 2.3 van dit document.
[20] Pagina 193.
[21] Zoals de websites van de Europese Unie of de Raad van Europa en de rapporten die gepubliceerd zijn door organisaties als EPIC of Privacy Laws and Business.
[22] Zie Artikel 25, paragrafen 4, 5 en 6 van de Richtlijn.

De praktijk van de afgelopen jaren (in het bijzonder met betrekking tot de Safe Harbour-regeling die verder in dit document wordt besproken) heeft uitgewezen dat de Commissie kan besluiten onderhandelingen aan te gaan zonder een formele negatieve beslissing over een beschermingsniveau te nemen, als het duidelijk is dat de omstandigheden inderdaad aanleiding zouden kunnen geven tot een negatieve beslissing. Dit voorbeeld geeft aan dat de Commissie zal proberen het nemen van een negatieve beslissing te vermijden vanwege de politieke consequenties die dat kan hebben.

Bij de procedure voor de beslissing van de Commissie is ook de artikel 29-werkgroep betrokken, die bestaat uit de nationale toezichthouders voor de bescherming van persoonsgegevens en het Artikel 31-comité, dat uit vertegenwoordigers van de Lidstaten bestaat. Doorgaans geeft de Artikel 29-werkgroep eerst haar mening, die vervolgens door het Artikel 31-comité wordt meegewogen bij de stemming over voorgestelde maatregelen van de Europese Commissie. De Europese Commissie houdt rekening met de meningen die door beide groepen naar voren worden gebracht, maar heeft het recht daarvan af te wijken in haar definitieve beslissing.
Artikel 31 van de Richtlijn biedt aanvullende waarborgen in dergelijke gevallen. Als de Europese Commissie besluit maatregelen te nemen die niet in overeenstemming zijn met de mening van het Artikel 31-comité, dan moet de Raad van de Europese Unie daarvan op de hoogte worden gesteld. De Raad mag desgewenst een afwijkende beslissing nemen, als een gekwalificeerde meerderheid daarvoor kiest.
Het Europees Parlement speelt ook een rol in deze procedure, omdat het parlement kan controleren of de Europese Commissie haar bevoegdheid niet te buiten is gegaan en of zij overeenkomstig de bestaande procedurele voorschriften heeft gehandeld.

Volgens de Richtlijn kan de Commissie een positief of een negatief besluit nemen. Vanwege de politieke consequenties van een negatieve beslissing valt het echter te verwachten dat de Commissie terughoudend zal zijn in het nemen van negatieve beslissingen. Tot nu toe heeft de Commissie in alle gevallen positief beslist.
Het toepassingsgebied van een beslissing kan variëren: de beslissing kan bijvoorbeeld voor een heel land gelden (zoals het geval is voor beslissingen over Zwitserland en Hongarije), voor een groep verantwoordelijken die een specifiek stelsel volgen (zoals voor de Safe Harbour-regeling geldt) of voor een bepaald deel van de wetgeving (hetgeen voor Canada geldt). Met andere woorden, een beslissing van de Commissie kan gevolgen hebben voor een heel land of voor een specifieke sector of groep in dat land.

De laatste alinea van artikel 25, lid 6 van de Richtlijn stelt dat Lidstaten de nodige maatregelen moeten nemen om zich naar het besluit van de Commissie te voegen. Dat houdt met name in dat de Lidstaten alle bestaande obstakels moeten wegnemen die kunnen voortkomen uit bestaande nationale wetgeving of andere wettelijke instrumenten die het vrije verkeer van persoonsgegevens met het betreffende land kunnen belemmeren[23]. De beslissingen van de Commissie zijn met onmiddellijke ingang van kracht[24].
Artikel 78, lid 2 WBP verklaart dat de beslissing van de Europese Commissie of de Raad op nationaal niveau wordt vastgelegd door een Ministeriële regeling of beschikking van de Minister van Justitie. Het doel van deze maatregelen is adequate publiciteit te verlenen aan Communautaire besluiten op nationaal niveau om zodoende juridische zekerheid te bieden.

[23] Zoals vermeld in de brief van de Minister van Justitie aan de Tweede Kamer van 9 maart 2000 aangaande de toepassing van Artikel 25 en 26 van de Europese Richtlijn, pagina 4. Tweede Kamer, vergaderjaar 1999-2000, 27 043, nr. 1.
[24] Zie Artikel 31, lid 2, van de Richtlijn.

Om de bestaande beslissingen van de Commissie bij het publiek onder de aandacht te brengen, worden deze ook gepubliceerd op de website van het College bescherming persoonsgegevens (CBP) [25]. Tot nu toe heeft de Commissie slechts vier maal een beslissing genomen, met betrekking tot Zwitserland, Hongarije, het Amerikaanse Safe Harbour-systeem[26] en het beschermingsniveau dat de Canadese Personal Information Protection and Electronic Documents Act[27] biedt. In hoofdstuk 3 van dit document wordt aandacht besteed aan het Safe Harbour-systeem.

Een algemene beslissing over het beschermingsniveau in een bepaald land op algemeen of sectorieel niveau kan alleen op Communautair niveau worden genomen. Als een dergelijke beslissing wordt genomen, dan is deze juridisch bindend voor de Lidstaten en voor alle verantwoordelijken binnen de EU.
Uit de gegeven verklaringen kan echter worden afgeleid dat de besluitvorming over een beschermingsniveau een complex en tijdrovend proces is waarbij diverse partijen betrokken zijn en die eerst een grondige analyse vergt van het wettelijke kader en de specifieke omstandigheden in een land. Dit proces is nog complexer en tijdrovender als het onderhandelingen vereist met het derde land teneinde tot een specifieke regeling te komen, zoals het geval was met de Verenigde Staten. Het is dan ook niet te verwachten dat op korte termijn beslissingen worden genomen over alle landen ter wereld[28].

Dat betekent in de praktijk dat voorlopig zeker niet kan worden geconcludeerd dat het uitblijven van een positieve beslissing van de Commissie inhoudt dat het beschermingsniveau in een bepaald land niet passend zou zijn[29].

2.1.4. Conclusie

Voor elke specifieke doorgifte moet een verantwoordelijke bepalen welk beschermingsniveau aanwezig is voor dat specifieke geval, op basis van een bestaande beslissing van de Commissie of, wanneer een dergelijke beslissing niet genomen is, op basis van de omstandigheden van dat geval.
Bij een dergelijke beoordeling moet rekening worden gehouden met de criteria die in paragraaf 2.1.1 zijn genoemd.

- Als vraag 1 Is er sprake van een passend beschermingsniveau? bevestigend kan worden beantwoord, dan kan de doorgifte plaatsvinden. De naleving van alle andere bepalingen van de WBP moet worden gewaarborgd.
- Als vraag 1 Is er sprake van een passend beschermingsniveau? ontkennend moet worden beantwoord, dan is doorgifte niet toegestaan volgens artikel 76 WBP. Zie paragraaf 2.2 en 2.3 om te bepalen of een oplossing kan worden gevonden ingevolge artikel 77 WBP.

[25] www.cbpweb.nl
[26] Besluiten van 26 juli 2000, gepubliceerd in het Publicatieblad van de Europese Gemeenschappen L 215, 25 augustus 2000.
[27] Besluit van 20 december 2001, gepubliceerd in het Publicatieblad van de Europese Gemeenschappen L 2, 4 januari 2002.
[28] Deze passage wordt gestaafd door de tekst van overweging 4 van de preambule van het Commissiebesluit van juni 2001 over contractuele bepalingen inzake doorgiftes tussen verantwoordelijken: “De Commissie kan op korte en ook op middellange termijn waarschijnlijk slechts voor een beperkt aantal landen een passend beschermingsniveau vaststellen op grond van artikel 25, lid 6”.
[29] Zoals eveneens vermeld in de brief van de Minister aan de Tweede Kamer van 9 maart 2000, pagina 7.

De Minister van Justitie heeft in zijn brief aan de Tweede Kamer van maart 2000[30] aangegeven dat in gevallen waarin het CBP na bestudering van de zaak concludeert dat het beschermingsniveau voor een bepaalde doorgifte naar een derde land niet passend is, de Minister daarvan op de hoogte moet worden gesteld. De wetgever heeft besloten dat, met het oog op de daarmee samenhangende gevolgen en de politieke implicaties, het wenselijk is de eindverantwoordelijkheid bij de Minister te leggen; hij kan beslissen welke maatregelen noodzakelijk zijn en de Europese Commissie daarover informeren.

2.2. Is het mogelijk gebruik te maken van een van de uitzonderingen van artikel 77.1?

Artikel 77, lid 1 WBP is de nationale implementatie van artikel 26 van de Richtlijn. Het basisidee achter dit artikel is dat zelfs in situaties waarin er geen passend beschermingsniveau is dat doorgifte volgens artikel 76 van de WBP mogelijk maakt, deze doorgifte toch rechtmatig kan plaatsvinden als gebruik kan worden gemaakt van een van de uitzonderingen die in dit artikel limitatief worden opgesomd.
Het artikel bevat een overzicht van alternatieve criteria. Als wordt voldaan aan de voorwaarden voor een van de uitzonderingen die in dit artikel worden genoemd, kan de doorgifte naar dat land worden uitgevoerd. Het spreekt voor zich dat in dergelijke gevallen ook moet worden voldaan aan alle overige vereisten/verplichtingen van de WBP die binnen de EU van toepassing zijn[31].

Zoals de Minister van Justitie in zijn brief aan de Tweede Kamer van maart 2000 al aangaf, moet het overzicht van uitzonderingen van artikel 77, lid 11 streng en restrictief worden geïnterpreteerd[32]. Een belangrijk element bij de interpretatie is het woord “noodzakelijk” dat in de verwoording van de meeste uitzonderingen wordt gebruikt.
In de volgende paragrafen wordt elke uitzondering afzonderlijk besproken en wordt een leidraad gegeven voor de interpretatie ervan. Deze leidraad omvat alle elementen van interpretatie uit de memorie van toelichting bij de WBP, de Richtlijn en van de Minister van Justitie en het document van de artikel 29-werkgroep (WP 12) dat in de vorige paragraaf werd genoemd.

2.2.1. Ondubbelzinnige toestemming van de betrokkene

De eerste uitzondering betreft gevallen waarbij de betrokkene zijn/haar ondubbelzinnige toestemming heeft gegeven voor de doorgifte. Voor de juiste interpretatie van deze uitzondering moet rekening worden gehouden met de volgende elementen:

- Toestemming is volgens de definitie van artikel 1, sub i WBP elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.
- De toestemming moet specifiek worden gegeven voor de doorgifte, niet voor verwerking in het algemeen.
- De vereiste van informatie aan de betrokkene is vooral van belang aangezien het in dit geval inhoudt dat de betrokkene zich bewust moet zijn van of bewust moet worden gemaakt van de bijzondere risico’s van de doorgifte en van het beschermingsniveau in het land waarnaar zijn/haar gegevens worden doorgegeven. De toestemming is alleen geldig als de betrokkene afdoende geïnformeerd is. Als de relevante informatie niet wordt gegeven, geldt deze uitzondering niet.

[30] Pagina 15 van de brief.
[31] Zie memorie van toelichting bij de WBP, pagina 194.
[32] Pagina 5 van de brief.

- Het is niet afdoende dat de betrokkene geen bezwaar maakt tegen de beoogde doorgifte nadat hij/zij is daarover is geïnformeerd ('opt out'-constructie). Dat is geen duidelijke wilsuiting van de betrokkene.
- Omdat de toestemming ondubbelzinnig moet zijn, maakt elke twijfel over het feit of toestemming al dan niet is verleend de uitzondering ongeldig.

Deze uitzondering is vooral nuttig in situaties waarin rechtstreeks contact bestaat tussen de verantwoordelijke en de betrokkene, aangezien in dergelijke situaties de verantwoordelijke gemakkelijk de nodige informatie kan verstrekken en de vereiste ondubbelzinnige toestemming kan verkrijgen.
Deze uitzondering is lastiger toe te passen als de beoogde doorgifte de gegevens van grotere aantallen betrokkenen omvat. In zo'n geval moet de informatie volledig en op een passende manier aan alle betrokkenen worden verstrekt en moet toestemming worden verkregen van ieder van hen om de doorgifte mogelijk te maken.
Naast het feit dat dit een tijdrovende en kostbare operatie kan zijn (bijvoorbeeld omdat de betrokkenen zich op verschillende locaties bevinden) heeft het gebruik van toestemming in degelijke gevallen andere praktische bezwaren, zoals:

- Wat moet de verantwoordelijke doen als een deel van de betrokkenen toestemming verleent en een ander deel niet? Aangezien de toestemming vrijwillig moet worden gegeven, moet de betrokkenen duidelijk worden gemaakt dat ze vrij zijn om "ja" of "nee" te zeggen tegen de beoogde doorgifte, zonder dat dit negatieve consequenties heeft. Dat is vooral van belang in een arbeidsrelatie, waar een betrokkene zich "verplicht" zal voelen "ja" te zeggen tegen een beoogde doorgifte door de werkgever als de betrokkene niet weet welke gevolgen het heeft om "nee" te zeggen.
- Wat doet de verantwoordelijke als sommige betrokkenen in een later stadium besluiten hun toestemming in te trekken? Men moet niet vergeten dat betrokkenen (of indien van toepassing hun wettelijke vertegenwoordigers) vrij zijn op elk willekeurig tijdstip hun toestemming in te trekken[33]. Het besluit de toestemming in te trekken heeft geen terugwerkende kracht, maar verwerking van de gegevens van die betrokkene moet vanaf dat moment worden gestaakt.

Vanwege de hierboven aangegeven redenen is het niet aan te raden van deze uitzondering gebruik te maken in gevallen met meerdere betrokkenen of grotere aantallen betrokkenen en waarbij de beoogde doorgifte alleen nuttig is als deze voor de gegevens van alle betrokkenen geldt. Een voorbeeld is een werkgever in Europa die besluit de gegevens van alle werknemers in een database buiten de EU onder te brengen, en alle werknemers moeten een toestemmingsformulier ondertekenen.

Ook dient opgemerkt dat de Artikel 29-werkgroep het gebruik van toestemming met betrekking tot arbeid heeft besproken in een document van september 2001[34]. De werkgroep is van mening dat gebruikmaking van toestemming in dit verband zou moeten worden beperkt tot gevallen waarin de werknemer daadwerkelijk de vrije keuze heeft en ook daarna de toestemming zonder nadelige consequenties kan intrekken. Zelfs als men wel op deze toestemming vertrouwt, moet deze geldig zijn en moet de werkgever nog altijd voldoen aan de andere eisen van de Richtlijn, waaronder artikel 6 en artikel 15 over geautomatiseerde beslissingen. Bovendien moet de werknemer over de verwerking worden geïnformeerd volgens de eisen van artikelen 10 en 11.

[33] Zoals vermeld in Artikel 5, lid 2, WBP.
[34] Advies 8/2001 over de verwerking van persoonsgegevens in het kader van de arbeidsverhouding, aangenomen op 13 september 2001, 5062/01/EN/Final, WP 48.

In het bijzonder verklaart de Artikel 29-werkgroep in de passage over de doorgifte van gegevens van werknemers naar derde landen, dat het de voorkeur verdient te vertrouwen op passende bescherming in het land van bestemming in plaats van te vertrouwen op de in artikel 26 genoemde uitzonderingen, zoals toestemming van de werknemer. Als men op toestemming vertrouwt, moet deze ondubbelzinnig en vrijwillig worden gegeven. Het is voor werkgevers niet aan te raden uitsluitend te vertrouwen op toestemming, behalve in gevallen waarin er geen problemen ontstaan als die toestemming naderhand wordt ingetrokken.

2.2.2. De doorgifte is noodzakelijk voor de uitvoering van een overeenkomst of precontractuele maatregelen

De tweede uitzondering verwijst naar omstandigheden waarbij de doorgifte van persoonsgegevens naar een derde land noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke of het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene. Voor een juiste interpretatie van deze uitzondering moet rekening worden gehouden met de volgende elementen:

- De betreffende doorgifte moet noodzakelijk zijn. Met andere woorden, deze uitzondering geldt niet als een doorgifte nuttig zou zijn of de uitvoering van een overeenkomst zou vergemakkelijken, maar niet echt noodzakelijk aangezien er een manier bestaat waarop de overeenkomst kan worden uitgevoerd terwijl de gegevens binnen de EU blijven.
- De uitzondering verwijst naar een overeenkomst waarin de betrokkene een partij is, of naar precontractuele maatregelen waar de betrokkene om heeft verzocht.
- De uitzondering is strikt beperkt tot de gegevens die voor een bepaald doel nodig zijn. Als aanvullende, niet-essentiële gegevens worden doorgegeven of als het doel van de doorgifte niet de uitvoering van een overeenkomst dient maar een ander doel (bijvoorbeeld follow-up marketing), dan geldt de uitzondering niet.

Een kenmerkend voorbeeld van een toepassing van deze uitzondering is een geval waarbij de betrokkene een overeenkomst aangaat met een reisbureau om voor hem/haar een reis naar een derde land te boeken. In dat geval zal het voor de uitvoering van de overeenkomst nodig zijn gegevens over de betrokkene te verzenden naar de luchtvaartmaatschappij en naar hotels in het derde land ten behoeve van tickets en hotelreserveringen.
Een ander voorbeeld dat in de memorie van toelichting wordt genoemd is een geval waarbij een betaling wordt verricht voor de uitvoering van een overeenkomst, waarbij het niet mogelijk is vooraf te weten via welke landen de bankoverschrijving wordt uitgevoerd. De betrokkene vraagt de bank de betaling voor hem/haar uit te voeren en daar zijn zijn/haar gegevens voor nodig.
Een geval van precontractuele maatregelen die door de betrokkene worden geïnitieerd is bijvoorbeeld een verzoek door de betrokkene om informatie over een bepaalde dienst, om te kunnen beslissen of hij/zij al dan niet een contractuele verplichting met deze onderneming in het derde land wil aangaan. Deze uitzondering is niet van toepassing als de gegevens werden doorgegeven als gevolg van direct-marketingactiviteiten van de verantwoordelijke.

2.2.3. De doorgifte is noodzakelijk voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten overeenkomst

De derde uitzondering betreft gevallen waarbij de doorgifte van gegevens naar een derde land noodzakelijk is voor de sluiting of uitvoering van een overeenkomst tussen de verantwoordelijke en een derde, in het belang van de betrokkene. Voor de juiste interpretatie van deze uitzondering moet rekening worden gehouden met de volgende elementen:

- Deze uitzondering verwijst naar een overeenkomst waarin de betrokkene geen partij is, maar die in zijn/haar belang wordt gesloten. De overeenkomst moet tot doel hebben iets te bereiken in het belang van de betrokkene.
- Deze uitzondering kan nooit de wettelijke grondslag vormen voor een doorgifte van persoonsgegevens naar een derde land ten behoeve van direct marketing, aangezien een dergelijke doorgifte niet in het belang is van de betrokkene, maar in het belang van degene die de betrokkene benadert voor direct marketing met gebruikmaking van de persoonsgegevens van de betrokkene.
- Net als in het voorgaande geval wordt de toepassing van deze uitzondering beperkt door de "proef van noodzakelijkheid": alle doorgegeven persoonsgegevens moeten noodzakelijk zijn voor de uitvoering van de overeenkomst.

Een voorbeeld van een doorgifte die onder deze uitzondering valt is een geval van herverzekering bij maatschappijen buiten de EU. Als een betrokkene een verzekering afsluit met een Nederlandse verzekeringsmaatschappij, is het mogelijk dat deze maatschappij vanwege het hoge verzekerde bedrag een herverzekeringscontract afsluit met een derde. Het kan nodig zijn persoonsgegevens over de betrokkene door te geven aan de herverzekeringsmaatschappij, die buiten de EU kan zijn gevestigd. In dit geval kan de uitzondering van toepassing zijn, want het gaat om een overeenkomst tussen de verzekeringsmaatschappij in Nederland en de herverzekeringsmaatschappij buiten de EU, die wordt gesloten in het belang van de betrokkene (als extra waarborg voor zijn/haar verzekering) die met betrekking tot deze overeenkomst dus een derde partij is.
Een ander voorbeeld is een geval waarbij de betrokkene de begunstigde is van een internationale bankoverschrijving. In dat geval zou het noodzakelijk zijn persoonsgegevens over de betrokkene door te geven naar het derde land dat de betaling uitvoert als onderdeel van een overeenkomst waarin de betrokkene geen partij is, maar die in zijn/haar belang wordt uitgevoerd. De overeenkomst wordt in feite uitgevoerd tussen de verantwoordelijke die de gegevens doorgeeft en de bank.

2.2.4. De doorgifte is noodzakelijk vanwege een zwaarwegend algemeen belang, of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht

De vierde uitzondering omvat twee soorten situaties:

1. Gevallen waarbij de doorgifte nodig is vanwege een zwaarwegend algemeen belang. In dat geval vindt de doorgifte niet plaats in het belang van de betrokkene, maar omdat daar een algemeen belang mee is gediend. Deze uitzondering kan van toepassing zijn op beperkte doorgiftes tussen overheidsinstellingen, hoewel ervoor moet worden gewaakt dat deze bepaling niet al te ruim wordt opgevat. Een algemeen belang is op zich geen afdoende rechtvaardiging voor de doorgifte, er moet een zwaarwegend algemeen belang mee gediend zijn. Overweging 58 van de Richtlijn geeft aan dat doorgiftes tussen administraties van belastingdiensten of douane of tussen sociale-zekerheidsinstanties doorgaans onder deze uitzondering zullen vallen. Doorgiftes tussen toezichthoudende autoriteiten in de financiële sector kunnen wellicht ook onder deze uitzondering vallen.

2. Gevallen waarbij de gegevens moeten worden doorgegeven voor de vaststelling, uitvoering of verdediging in rechte van enig recht. Dat kan bijvoorbeeld het geval zijn als de persoonsgegevens moeten worden doorgegeven naar een instantie voor kredietbeoordeling buiten de EU voorafgaand aan een gerechtelijke procedure. Deze uitzondering betreft doorgiftes die plaatsvinden in het kader van een internationale

rechtszaak of gerechtelijke procedure, in het bijzonder doorgiftes die nodig zijn voor de vaststelling, uitvoering of verdediging van juridische aanspraken.

2.2.5. De doorgifte is noodzakelijk ter bescherming van een vitaal belang van de betrokkene

Deze vijfde uitzondering betreft doorgiftes die noodzakelijk zijn ter bescherming van vitale belangen van de betrokkene. Daarbij wordt opgemerkt dat in overweging 31 van de Richtlijn het begrip "vitaal belang" zeer nauw wordt omschreven als een belang "dat voor de betrokkene van levensbelang is". Doorgaans worden daardoor financiële belangen, eigendomsbelangen of familiebelangen uitgesloten. Ook hier moet de test van noodzakelijkheid worden toegepast.

Een duidelijk voorbeeld van een dergelijke doorgifte is de urgente doorgifte van een medisch dossier naar een derde land waar een toerist, die eerder in de EU onder medische behandeling was, een ongeval heeft gehad of ernstig ziek is geworden. In zulke gevallen, gezien de urgentie van de situatie en de toestand van de patiënt, zou het onmogelijk zijn toestemming te verkrijgen van de betrokkene.

2.2.6. Doorgifte vanuit een register dat door het publiek kan worden geraadpleegd

De laatste uitzondering betreft gevallen waarbij de doorgifte wordt uitgevoerd vanuit een openbaar register dat bij wettelijk voorschrift is ingesteld of vanuit een register dat bedoeld is om te worden geraadpleegd, door het algemene publiek of door een persoon die zich op een gerechtvaardigd belang kan beroepen, voor zover in het betreffende geval is voldaan aan de wettelijke voorwaarden voor raadpleging.

De bedoeling van deze uitzondering is dat, indien een register kan worden geraadpleegd door het publiek of door personen die een gerechtvaardigd belang kunnen aantonen, het feit dat een dergelijke persoon zich in een derde land bevindt en het raadplegen derhalve een doorgifte van persoonsgegevens inhoudt, geen belemmering vormt voor de doorgifte van de gegevens aan die persoon.
Uit overweging 58 van de Richtlijn blijkt duidelijk dat niet moet worden toegestaan dat het gehele register of complete gegevenscategorieën uit dat register worden doorgegeven als gevolg van deze uitzondering. In het licht van deze beperkingen moet deze uitzondering niet worden beschouwd als een algemene uitzondering voor de doorgifte van gegevens uit openbare registers. Het zal bijvoorbeeld duidelijk zijn dat de doorgifte van grote hoeveelheden gegevens uit openbare registers voor commerciële doeleinden of het op kenmerk selecteren van openbare gegevens met het doel profielen op te stellen van bepaalde personen of groepen (data mining), niet mag plaatsvinden op grond van deze uitzondering.

De verwoording van deze uitzondering in de Richtlijn verwijst naar "registers die bedoeld zijn om te worden geraadpleegd door het publiek". In dat opzicht is het van toepassing op registers zoals het register van voertuigenkentekens of het handelsregister.

2.2.7. Conclusie

- Als vraag 2 *Is het mogelijk gebruik te maken van een van de uitzonderingen van artikel 77.1?* bevestigend kan worden beantwoord, dan kan de doorgifte plaatsvinden. De naleving van alle andere bepalingen van de WBP moet worden gewaarborgd.
- Als vraag 2 *Is het mogelijk gebruik te maken van een van de uitzonderingen van artikel 77.1?* ontkennend moet worden beantwoord, dan is doorgifte op grond van artikel 77, lid 1 WBP niet toegestaan. Zie paragraaf 2.3 om te bepalen of een oplossing kan worden gevonden ingevolge artikel 77, lid 2 WBP.

In zijn brief aan de Tweede Kamer van maart 2000 heeft de Minister van Justitie aangegeven dat in gevallen waar geen van deze uitzonderingsgronden van toepassing is, de doorgifte onrechtmatig is. Het CBP kan een bestuursrechtelijke dwangmaatregel nemen als dat nodig is om een dergelijke doorgifte tegen te houden[35].

2.3. Is het mogelijk een vergunning voor de doorgifte te verkrijgen van de Minister van Justitie (artikel 77.2)?

Artikel 77, lid 2 WBP verklaart dat de Minister van Justitie na raadpleging van het CBP een vergunning mag afgeven voor een doorgifte van persoonsgegevens of een categorie doorgiftes aan een niet-lidstaat die geen passend beschermingsniveau waarborgt.
Als het noodzakelijk wordt geacht de individuele privacy en fundamentele rechten en vrijheden van personen te beschermen en uitoefening van daaraan verbonden rechten te waarborgen, kunnen gedetailleerde voorschriften aan de uitgifte van deze vergunning worden verbonden.
Met dit artikel wordt het tweede lid van artikel 26 van de Richtlijn vertaald naar het Nederlands recht. Deze bepaling geldt voor situaties waarin een verantwoordelijke gegevens wil doorgeven naar een derde land dat geen passend beschermingsniveau waarborgt en waarbij het niet mogelijk of wenselijk is gebruik te maken van een van de uitzonderingen die in de voorgaande paragraaf zijn besproken. In dat geval kan de Lidstaat een dergelijke doorgifte toestaan als de verantwoordelijke voor aanvullende waarborgen zorgt met betrekking tot de bescherming van de privacy en fundamentele rechten en vrijheden van personen en met betrekking tot de uitoefening van daaraan verbonden rechten. Deze waarborgen kunnen met name voortvloeien uit passende contractuele bepalingen.

De Minister van Justitie is verplicht het advies van het CBP in te winnen voordat hij een vergunning uitgeeft. Volgens de tekst van de memorie van toelichting bij de WBP[36] speelt het advies van de CBP in dit verband een belangrijke rol; het draagt bij aan de kwaliteit van de besluitvorming over vergunningen, vanwege de deskundigheid en ervaring van het CBP op dit gebied.

Een verantwoordelijke hoeft niet voor elke afzonderlijke doorgifte een vergunning aan te vragen. Het is mogelijk een vergunning voor een categorie van doorgiftes aan te vragen, met andere woorden, een duidelijk omschreven verzameling van doorgiftes met gemeenschappelijke elementen waarbij dezelfde omstandigheden een rol spelen. Een vergunning kan alleen worden verleend op basis van specifieke en duidelijk omschreven

[35] Pagina 15 van de brief.
[36] Pagina 195.

omstandigheden en waarborgen die worden ingesteld om specifieke risico's af te schermen en waarbij het toepassingsgebied van de vergunning te allen tijde kan worden bepaald.
Een vergunning van de Minister van Justitie voor een specifieke doorgifte of een verzameling doorgiftes biedt een hoge graad van juridische zekerheid aan de verantwoordelijke die persoonsgegevens naar een derde land wil doorgeven.

2.3.1. Wat is een "passende waarborg"?

De tekst van artikel 77 WBP geeft niet aan welke maatregelen een verantwoordelijke kan aanvoeren om een vergunning van de Minister te verkrijgen. De memorie van toelichting[37] bij dit artikel bevat echter met betrekking tot de specifieke voorschriften die daaraan kunnen worden verbonden, een tekst die vergelijkbaar is met de tekst van de Richtlijn: de voorschriften die aan de vergunning zijn verbonden, kunnen worden gerelateerd aan contractuele bepalingen die de verantwoordelijke heeft opgenomen in een overeenkomst met de persoon aan wie de persoonsgegevens worden doorgegeven.
Artikel 26 van de Richtlijn bepaalt dat de passende waarborgen die de verantwoordelijke moet aanvoeren in gevallen waarin persoonsgegevens moeten worden doorgegeven naar een derde land dat geen passend beschermingsniveau biedt, in het bijzonder kunnen voortvloeien uit passende contractuele bepalingen. In overweging 59 van de Richtlijn wordt de term "contractuele bepalingen" niet gebruikt; er wordt verwezen naar "bijzondere maatregelen [die] kunnen worden getroffen om het ontoereikende beschermingsniveau in een derde land te verhelpen". Artikel 26, lid 4 van de Richtlijn geeft de Commissie, overeenkomstig de procedure die in artikel 31 is uiteengezet, de bevoegdheid te besluiten dat passende waarborgen zoals bedoeld in artikel 26, lid 2 worden geboden door passende contractuele bepalingen.

In beide gevallen is het duidelijk dat de wetgever contractuele bepalingen beschouwt als de meest voor de hand liggende manier om passende waarborgen te bieden, maar daarbij worden andere instrumenten niet uitgesloten. Daarbij kan men denken aan diverse mogelijkheden waarbij zowel de exporteur als de importeur verschillende rollen kunnen spelen, of waar ook andere partijen bij kunnen worden betrokken (bijvoorbeeld een externe auditor, het CBP) met bilaterale of unilaterale verplichtingen. Het nakomen van de verplichtingen die middels een bindend instrument zijn overeengekomen, kan dan de basis vormen voor de toekenning van een vergunning.

Vanuit het oogpunt van bescherming van persoonsgegevens is de aard of denominatie van het betreffende instrument niet relevant, voorzover het instrument op zich, of in combinatie met ondersteunende contractuele bepalingen, het gewenste effect kan bereiken: het bieden van passende waarborgen voor de doorgifte. Een wereldwijd privacybeleid van een onderneming bijvoorbeeld, is op zich niet afdoende omdat het als zodanig niet bindend is en unilateraal door de onderneming kan worden gewijzigd. De situatie verandert echter als een aantal institutionele waarborgen aan het beleid wordt toegevoegd, zoals contracten die het beleid ondersteunen, het beleid afdoende in de publiciteit brengen of het beleid te deponeren bij het CBP etc. Dergelijke vraagstukken moeten van geval tot geval worden geanalyseerd door het CBP, waarbij rekening wordt gehouden met de principes die door de werkgroep zijn vastgelegd met betrekking tot zelfregulering[38].

---

[37] Pagina 195: Deze voorschriften kunnen betrekking hebben op contractuele bepalingen die de verantwoordelijke opneemt in een overeenkomst met degene aan wie de gegevens worden doorgegeven.
[38] Zie voor informatie het document van de Artikel 29-werkgroep van 24 juli 1998 of de samenvatting in paragraaf 2.1.1 van dit document.

Ten behoeve van de leesbaarheid van dit document wordt in de volgende paragrafen de term "contractuele oplossingen" gebruikt, waarmee wordt verwezen naar elk instrument, al dan niet in de vorm van contractuele bepalingen, dat dezelfde juridische effecten kan bewerkstelligen, gepresenteerd door een verantwoordelijke in het kader van een aanvraag voor een vergunning van de Minister van Justitie volgens artikel 77, lid 2 WBP.
Elk instrument dat door verantwoordelijke wordt gepresenteerd als basis voor het verkrijgen van een vergunning, wordt door het CBP en de Minister bestudeerd aan de hand van de criteria die in de volgende paragraaf van dit beleidsdocument zijn uiteengezet.

2.3.2. Vereisten voor contractuele oplossingen

De belangrijkste functie van contractuele oplossingen is in dit verband bevredigende compensatie te bieden voor de afwezigheid van een passend algemeen beschermingsniveau, door opname van de ontbrekende essentiële elementen van de bescherming voor een bepaalde specifieke situatie[39]. De bepalingen van een contractuele oplossing moeten in detail worden uiteengezet en op correcte wijze worden toegepast op de betreffende doorgifte.

Het uitgangspunt voor de interpretatie van het begrip "passend beschermingsniveau" zoals dat in artikel 77, lid 2 WBP wordt gebruikt is het begrip "passende bescherming", dat in paragraaf 2.1.1 van dit document uitgebreid werd besproken. Zoals al werd aangegeven, omvat dit begrip een verzameling basisprincipes voor gegevensbescherming tezamen met bepaalde voorwaarden waaraan moet worden voldaan om hun effectiviteit te waarborgen. Een eerste vereiste van een contractuele oplossing is dan ook dat deze moet resulteren in de verplichting voor de partijen bij de doorgifte te waarborgen dat de volledige verzameling principes voor gegevensbescherming, zoals omschreven in paragraaf 2.1.1, van toepassing is op de verwerking van de gegevens die aan het derde land worden doorgegeven. De contractuele oplossing moet een omschrijving in detail omvatten van de wijze waarop de ontvanger van de gegevens (die in contractuele overeenkomsten vaak de importeur van de gegevens wordt genoemd) de principes moet toepassen. De criteria die in paragraaf 2.1.1. zijn beschreven met betrekking tot de effectiviteit van een systeem voor gegevensbescherming, moeten ook worden toegepast bij de beoordeling van de effectiviteit van een contractuele oplossing. Het is een kwestie van middelen vinden om de afwezigheid van mechanismen voor toezicht en handhaving te compenseren en om hulp, ondersteuning en uiteindelijk schadeloosstelling te kunnen bieden aan de betrokkene die wellicht geen partij in het contract is.

De mate van autonomie die de ontvanger van de gegevens in het derde land heeft om de gegevens na de doorgifte te verwerken, bepaalt in grote mate de risico's die inherent zijn aan de doorgifte. In een doorgifte tussen een verantwoordelijke in de EU en een bewerker buiten de EU zijn de risico's beperkter, aangezien de bewerker alleen kan handelen naar de instructies van de verantwoordelijke en niet de vrijheid heeft om beslissingen te nemen over de verwerking en, wat belangrijker is, omdat de wet van het land van de verantwoordelijke van toepassing blijft op de verwerking.
Dat is het gevolg van de manier waarop het toepassingsgebied van de Richtlijn (en dus ook van de WBP) is gedefinieerd, in beide gevallen in artikel 4. De controle over de gegevens die door de bewerker buiten de EU worden verwerkt wordt uitgeoefend door een lichaam dat in

[39] In het document WP 12 van de Artikel 29-werkgroep is een heel hoofdstuk gewijd aan contractuele bepalingen. Deze paragraaf is van die tekst afgeleid.

een EU-lidstaat is gevestigd en de wet van het betreffende EU-land blijft van toepassing op de verwerking in het derde land, waardoor de verantwoordelijke volgens die wet aansprakelijk blijft voor eventuele schade die door een onrechtmatige verwerking wordt veroorzaakt[40]. Voorzover de verantwoordelijke die de gegevens doorgeeft de controle behoudt over de verwerking die in het derde land wordt uitgevoerd, is het risico voor de betrokkene beperkter, aangezien hij eventuele claims kan richten aan een verantwoordelijke binnen de EU en verzoeken tot schadeloosstelling kan richten aan een wettelijke of toezichthoudende autoriteit binnen de EU.

Vaak wordt aangenomen dat de betrokkene en de verantwoordelijke binnen de EU zich in hetzelfde land bevinden en dat de wet op de gegevensbescherming van het land van de betrokkene dus op de verwerking van toepassing is. Dat is in de praktijk echter niet altijd het geval, aangezien gegevens binnen de EU gecentraliseerd kunnen worden beheerd door één verantwoordelijke, die de gegevens doorgeeft aan een verantwoordelijke/bewerker in een derde land. In elk geval garandeert het feit dat de wetgeving voor gegevensbescherming van de EU van toepassing is, de betrokkene een hoog en geharmoniseerd beschermingsniveau en geeft het hem/haar de mogelijkheid eventuele klachten of verzoeken in te dienen bij de toezichthouder in zijn/haar eigen land, die de zaak vervolgens kan doorverwijzen naar de overeenkomstige toezichthoudende autoriteit in het land van de verantwoordelijke. Dat vloeit voort uit een verplichting van de Europese toezichthoudende autoriteiten met elkaar samen te werken volgens artikel 28, lid 6 van de Richtlijn[41]. Vanwege alle bovengenoemde redenen hoeven contractuele oplossingen voor een doorgifte tussen een verantwoordelijke in de EU en een bewerker buiten de EU minder gedetailleerd te zijn dan in het geval van een doorgifte van een verantwoordelijke naar een andere verantwoordelijke buiten de EU[42].

Bij contractuele oplossingen tussen een verantwoordelijke in de EU en een verantwoordelijke buiten de EU is de situatie complexer, aangezien er geen EU-wet van toepassing is nadat de doorgifte heeft plaatsgevonden. Er moeten andere, meer geavanceerde mechanismen worden ingevoerd om de betrokkene een passende juridische oplossing te bieden. Aangezien de betrokkene als zodanig geen partij is in de overeenkomst, moet in de overeenkomst een clausule ten gunste van derde partijen worden opgenomen, waarmee met betrekking tot de overeenkomst bepaalde rechten worden toegekend aan de betrokkene. Dit systeem is op dit moment toelaatbaar in de rechtsstelsels van alle EU-lidstaten.
De contractuele oplossing moet verder passende bepalingen omvatten met betrekking tot de aansprakelijkheid en verantwoordelijkheid van de partijen in de overeenkomst. In dat opzicht, gezien de praktische en juridische obstakels waarmee een betrokkene wordt geconfronteerd als hij/zij schadevergoeding probeert te verkrijgen van een partij buiten de EU, moet elke contractuele oplossing teneinde passende waarborgen te bieden, garanderen dat de betrokkene recht heeft op compensatie van de partij van de verantwoordelijke die in het rechtsgebied van de EU is gevestigd. Dat kan worden bereikt door een clausule van gezamenlijke en hoofdelijke aansprakelijkheid op te nemen waaraan de partijen in de overeenkomst gebonden zijn.

[40] Zie Artikel 23 van de Richtlijn.
[41] Zie ook Artikel 61, lid 6 WBP.
[42] Dit feit wordt tevens benadrukt in overweging 8 van de preambule van het Commissiebesluit over standaard contractuele bepalingen van juni 2001: “Deze beschikking betreft niet de doorgifte van persoonsgegevens door voor de verwerking verantwoordelijken die in de Gemeenschap zijn gevestigd aan ontvangers buiten het grondgebied van de Gemeenschap die slechts als bewerkers optreden. Deze doorgiften vereisen niet dezelfde waarborgen,omdat de bewerker uitsluitend namens de voor de verwerking verantwoordelijke optreedt”.

Een bijkomende moeilijkheid bij dergelijke doorgiftes is het feit dat de importeur van de gegevens is gevestigd in een land buiten de EU, hetgeen toezicht door de verantwoordelijke of een toezichthoudende autoriteit in de EU aanzienlijk bemoeilijkt. Dit probleem moet door de contractuele oplossingen worden ondervangen, door de importeur te verplichten samen te werken in gevallen waarin de verantwoordelijke of de toezichthoudende autoriteit van mening is dat een onderzoek of audit op de locatie van de importeur van de gegevens nodig is.

2.3.3. Kunnen contractuele oplossingen in alle gevallen worden gebruikt?

Contractuele oplossingen kunnen in sommige situaties een goede oplossing bieden, maar er zijn ook situaties denkbaar waar het niet mogelijk is met een overeenkomst de nodige passende waarborgen te bieden.
Dat is vooral het geval in minder democratische landen, waar de macht van overheidsinstanties om informatie op te vragen verder strekt dan toegestaan is volgens internationaal aanvaarde normen voor de bescherming van de mensenrechten. In zulke gevallen heeft het opnemen van bepalingen in een contractuele oplossing ter beperking van de bevoegdheden van de verantwoordelijke/bewerker in het derde land in het verstrekken van deze informatie aan de overheid geen wettelijk effect, aangezien de bestaande wettelijke eisen in het betreffende land vaak voorrang hebben op contracten waaraan de importeur van de gegevens is gebonden.
Landen waar de verplichtingen om informatie beschikbaar te stellen aan overheidsinstanties verder strekken dan nodig is om te voldoen aan de behoeften van een democratische maatschappij en met betrekking tot de openbare orde zoals aangegeven in artikel 13, lid 1 van de Richtlijn, zijn geen veilige bestemmingen voor doorgiftes op basis van contractuele oplossingen.

Zoals al eerder werd aangegeven, moeten contractuele oplossingen nauwkeurig worden omschreven en aangepast aan de specifieke omstandigheden van de betreffende doorgifte. Een overeenkomst is dan ook vooral geschikt voor situaties waarbij doorgiftes vergelijkbaar en herhalend van aard zijn. De lastige aspecten met betrekking tot supervisie houden in dat een contractuele oplossing waarschijnlijk het meest effectief is als de partijen grote organisaties zijn die toch al publiekelijk in de belangstelling staan en die aan strenge regelgeving onderhevig zijn. Voor grote internationale netwerken zoals die bestaan voor creditcardtransacties en reserveringen voor vliegtickets gelden beide kenmerken; dat zijn dan ook goede voorbeelden van situaties waarin overeenkomsten bij uitstek geschikt kunnen zijn[43].
Op vergelijkbare wijze geldt dat waar partijen in de doorgifte partners zijn of tot hetzelfde moederbedrijf behoren, de mogelijkheden om nalatigheid in de naleving van de overeenkomst te onderzoeken veel groter zijn, vanwege de sterke banden tussen de ontvanger in het derde land en de partij in de EU. Doorgiftes binnen ondernemingen zijn daarmee ook een gebied met goede mogelijkheden voor de ontwikkeling van effectieve contractuele oplossingen.

2.3.4. Het gebruik van modelcontracten die door de Europese Commissie zijn goedgekeurd

Artikel 26, lid 4 van de Richtlijn geeft de Europese Commissie de bevoegdheid te beslissen dat bepaalde contractuele bepalingen al dan niet passende waarborgen bieden zoals bedoeld in

[43] In gevallen die contractuele oplossingen behoeven. Zoals in paragraaf 2.2. is toegelicht, kunnen deze bedrijven in sommige gevallen en onder de genoemde omstandigheden van Artikel 77, lid 1 WBP, gebruik maken van de uitzonderingen van de WBP en hebben derhalve in deze gevallen geen contract nodig, alhoewel het hun vrij staat voor deze oplossing te kiezen.

artikel 26, lid 2. Voor dergelijke beslissingen geldt dezelfde procedure als voor een beoordeling van passende bescherming in een derde land, hetgeen inhoudt dat zowel de Artikel 29-werkgroep als het Artikel 31-comité betrokken zijn bij de voorbereiding van een dergelijke beslissing.

De afgelopen jaren heeft een aantal internationaal erkende organisaties zoals de IKK (Internationale Kamer van Koophandel) en de CBI (Confederation of British Industries) contact gehad met de Artikel 29-werkgroep en de Europese Commissie over modelcontracten die de organisaties hadden opgesteld. Deze contacten hebben geleid tot de formulering van adviezen die de werkgroep aan de organisaties kenbaar heeft gemaakt, maar dit heeft nog niet geleid tot bekrachtiging in de vorm van een Commissiebesluit over teksten die aan de Commissie zijn voorgelegd.
Omdat men daarnaast vond dat de beschikbaarheid van modelcontracten grensoverschrijdend gegevensverkeer aanzienlijk zou vergemakkelijken, besloot de Commissie zelf een aantal clausules op te stellen, waarbij zij gebruik maakte van de deskundigheid van de artikel 29-werkgroep en het Artikel 31-comité en van commentaar van buitenaf. Dit initiatief heeft geleid tot een eerste Commissiebesluit van juni 2001[44], voor doorgiftes tussen twee verantwoordelijken. Een verzameling contractuele bepalingen voor doorgiftes tussen verantwoordelijken in de EU en bewerkers in derde landen werd op 27 december 2001 aangenomen[45].

De modelcontracten die door de Europese Commissie zijn goedgekeurd, kunnen worden gebruikt door een verantwoordelijke die onder het toepassingsgebied van de WBP valt als basis om een vergunning te verkrijgen ingevolge artikel 77, lid 2 WBP. De WBP omvat geen bepalingen waarmee verantwoordelijken die de clausules van het Commissiebesluit toepassen, worden vrijgesteld van de vereiste een vergunning aan te vragen en daarom geldt deze vereiste ook in deze gevallen. In het Commissiebesluit van juni 2001[46] wordt duidelijk aangegeven dat het besluit geen afbreuk doet aan de mogelijkheden van Lidstaten om op nationaal niveau toestemmingen te verlenen overeenkomstig nationale voorschriften waarmee artikel 26, lid 2 van de Richtlijn wordt geïmplementeerd; in de WBP is dat artikel 77, lid 2. De benodigde procedures en de tijdsinvestering voor het verkrijgen van een vergunning kunnen echter aanzienlijk worden vereenvoudigd en verkort omdat de rol van de nationale overheden sterk wordt beperkt door het Commissiebesluit. Dit wordt in de navolgende paragrafen nader toegelicht.

2.3.4.1. Hoofdpunten van de door de Europese Commissie goedgekeurde modelcontracten

- Het Commissiebesluit van juni 2001 is alleen van toepassing op de doorgifte van persoonsgegevens tussen een verantwoordelijke in de EU en verantwoordelijke buiten de EU. Doorgiftes aan bewerkers vallen niet onder dit instrument. Het Commissiebesluit van

[44] Publicatieblad van de Europese Gemeenschappen, L 181, 4 juli 2001. Op de website van de Europese Commissie worden vaak gestelde vragen (FAQ) over het gebruik van de standaard contractuele bepalingen van een antwoord voorzien: http://www.europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm
[45] Beschikking van de Commissie van 27 december 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar in derde landen gevestigde bewerkers krachtens Richtlijn 95/46/EG, Publicatieblad van de Europese Gemeenschappen, L 6, 10 januari 2002.
[46] Overweging 6.

december 2001 is alleen van toepassing op de doorgifte door een verantwoordelijke aan een bewerker buiten de EU[47].

- De modelcontracten hebben alleen betrekking op gegevensbescherming. Het staat de exporteur van de gegevens (de verantwoordelijke in de EU) en de importeur van de gegevens (de verantwoordelijke of bewerker in het derde land) vrij andere clausules over zakelijke kwesties op te nemen, zoals wederzijdse ondersteuning bij geschillen met een betrokkene of een toezichthoudende autoriteit die zij relevant vinden voor het contract, zolang deze niet rechtstreeks of indirect strijdig zijn met de modelcontracten[48] of inbreuk maken op grondrechten of vrijheden van de betrokkenen. In alle gevallen moeten de modelcontracten volledig worden nageleefd, willen zij juridisch gezien tot passende waarborgen leiden voor de doorgifte van persoonsgegevens zoals dat door de Richtlijn wordt vereist[49].

- De modelcontracten bevatten bepalingen voor vraagstukken zoals de verplichtingen van de exporteur en de importeur, de clausule voor handelen in het belang van derden (de betrokkene), de gezamenlijke en hoofdelijke aansprakelijkheid van de partijen in de overeenkomst, samenwerking van partijen met de toezichthoudende autoriteiten, bemiddeling en jurisdictie bij geschillen tussen de partijen, beëindiging van de clausules, toepasselijk recht en de verplichting van de partijen de voorwaarden van de clausules niet te wijzigen.

- De details van de doorgifte en in het bijzonder de categorieën persoonsgegevens en de doeleinden waarvoor zij worden doorgegeven, moeten door de partijen worden gespecificeerd in bijlage 1 bij het contract dat een integraal onderdeel van de clausules vormt.

2.3.4.2. De rol van het College bescherming persoonsgegevens met betrekking tot de modelcontracten

Zoals in het begin van paragraaf 2.3 werd aangegeven, moet onderscheid worden gemaakt tussen de rol van Minister van Justitie en van het College bescherming persoonsgegevens (CBP) met betrekking tot het toewijzen van vergunningen.
De Minister heeft de bevoegdheid een definitief besluit te nemen met betrekking tot een aanvraag voor een vergunning, waarbij hij rekening houdt met het advies van het CBP. Het College heeft een adviserende rol voor de Minister en fungeert tegelijkertijd als toezichthoudende autoriteit voor de desbetreffende verwerkingen, niet alleen op het moment dat het besluit over de vergunning wordt genomen, maar ook daarna.
Met betrekking tot de modelcontracten is de adviserende rol van het CBP over de vergunning beperkt, maar de bevoegdheden van het CBP als toezichthoudende autoriteit over alle andere bepalingen van de WBP blijven onverminderd van toepassing.

[47] Zie Artikel 2 van het Commissiebesluit van december 2001.
[48] Zie overweging 5 van het Commissiebesluit van juni 2001, overweging 4 van het Commissiebesluit van december 2001.
[49] Zie Frequently asked questions on the Commission Decision 2001/497/EC: Kunnen bedrijven de standaard contractuele bepalingen opnemen in een breder contract en specifieke bepalingen toevoegen? op de website van de Europese Commissie.

Een doorgifte van persoonsgegevens naar een derde land is een verwerking in de zin van de WBP, hetgeen inhoudt dat alle andere vereisten van de WBP van toepassing zijn naast de bepalingen van hoofdstuk 11.
De contractuele bepalingen van de Commissie hebben tot doel te garanderen dat bij de doorgifte van gegevens naar een derde land, de verantwoordelijke daarvoor passende waarborgen biedt op basis van het contract. Commissiebesluit[50] houden voor Lidstaten in dat zij niet kunnen weigeren de in het besluit omschreven clausules te erkennen, als die worden gebruikt overeenkomstig de tekst van het besluit zodat passende waarborgen worden geboden. De bevoegdheden van de nationale toezichthoudende autoriteiten om de naleving van alle andere bepalingen van de nationale wet te beoordelen, in dit geval de WBP, worden niet beperkt door dit besluit.

Als verantwoordelijken gebruik maken van de modelcontracten van de Commissie, dan is het CBP en/of de Minister vrij toelichting te vragen omtrent aspecten die van invloed kunnen zijn op naleving van de overige bepalingen van de WBP met betrekking tot de verwerkingen. Dit betreft met name problemen die zich kunnen voordoen naar aanleiding van informatie die door de contractpartijen wordt verstrekt in bijlage 1 van het contract, dat integraal onderdeel vormt van het contract en dat verplicht moet worden ingevuld door de partijen. Dit is duidelijk aangegeven in de tekst van overweging 7 van het Commissiebesluit van juni 2001, die als volgt luidt: “Deze beschikking stelt slechts vast dat de in de bijlage opgenomen modelcontractbepalingen door een in de Gemeenschap gevestigde voor de verwerking verantwoordelijke kunnen worden gebruikt om voldoende waarborgen in de zin van artikel 26, lid 2 van Richtlijn 95/46/EG te bieden. De doorgifte van persoonsgegevens naar derde landen is een verwerking in een lidstaat, waarvan de rechtmatigheid wordt bepaald door het nationale recht. De toezichthoudende autoriteiten van de lidstaten dienen in de uitoefening van hun taken en bevoegdheden overeenkomstig artikel 28 van Richtlijn 95/46/EG bevoegd te blijven om te beoordelen of de gegevensexporteur zich houdt aan de nationale wetsvoorschriften tot uitvoering van Richtlijn 95/46/EG en met name aan specifieke regels betreffende de verplichting om informatie te verstrekken krachtens die richtlijn”[51]. Deze overweging benadrukt het feit dat de toezichthoudende autoriteiten in het bijzonder kunnen controleren of de verantwoordelijke de betrokkene afdoende heeft geïnformeerd over de uit te voeren doorgifte naar een derde land zonder dat daarvoor passende bescherming wordt geboden.

Zoals reeds werd aangegeven, willen partijen in het contract mogelijk extra clausules in het contract opnemen in aanvulling op een modelcontract. Dat is alleen mogelijk als deze clausules niet rechtstreeks of indirect strijdig zijn met de modelcontracten, of inbreuk maken op grondrechten of vrijheden van de betrokkenen. Bij de beoordeling van een aanvraag voor een vergunning, zullen het CBP en/of de Minister ook moeten beoordelen of met de toevoeging van aanvullende clausules deze vereisten worden gerespecteerd. Daarbij moet worden onderstreept dat de clausules alleen de juridische status bieden die daaraan middels het Commissiebesluit worden toegekend als de clausules volledig worden nagevolgd. Als de inhoud van het contract wordt beïnvloed door deze aanvullingen, zal het CBP in zijn advies de consequenties van deze aanvullingen evalueren en de Minister daarover adviseren.

Het is denkbaar dat de partijen de tekst van sommige clausules van het Commissiebesluit zouden willen aanpassen of wijzigen. Clausule 11 van de modelcontracten van de Commissie

[50] Overweging 6 van het Commissiebesluit van juni 2001, overweging 5 van het Commissiebesluit van december 2001.
[51] Zie ook overweging 6 van het Commissiebesluit van december 2001.

voor doorgiftes tussen twee verantwoordelijken en clausule 20 van de modelcontracten voor doorgifte van een verantwoordelijke aan een bewerker verbieden de partijen de tekst van de clausules te wijzigen of aan te passen.
Het aanbrengen van amendementen heeft dan ook gevolgen voor de juridische status die de Commissie aan de clausules heeft verleend. De partijen kunnen er echter voor kiezen de clausules aan te passen aan de specifieke omstandigheden voor de overdracht, waarna op grond van deze "nieuwe" clausules een aanvraag voor een vergunning kan worden ingediend bij de Minister. In dergelijke gevallen zal het CBP de clausules beoordelen zonder gebonden te zijn door de gevolgen van het Commissiebesluit. Als de clausules echter de vereisten die in paragraaf 2.3.2 zijn beschreven respecteren, kan het CBP concluderen dat de clausules afdoende bescherming bieden, zodat een positief advies aan de Minister kan worden uitgebracht.

Artikel 4 van de Commissiebesluiten van juni 2001 en van december 2001 geeft de toezichthoudende autoriteiten ook de bevoegdheid gegevensverkeer naar derde landen te verbieden of te onderbreken teneinde individuen te beschermen met betrekking tot de verwerking van hun persoonsgegevens, in gevallen waarbij:

- wordt vastgesteld dat het recht dat op de gegevensimporteur van toepassing is hem vereisten oplegt waarmee van de toepasselijke regels betreffende gegevensbescherming moet worden afgeweken,die verder gaan dan de beperkingen die in een democratische samenleving noodzakelijk zijn als bedoeld in artikel 13 van Richtlijn 95/46/EG,indien die vereisten in aanzienlijke mate afbreuk dreigen te doen aan de door de modelcontractbepalingen geboden waarborgen,of
- een bevoegde autoriteit heeft vastgesteld dat de gegevensimporteur de contractbepalingen niet is nagekomen, of
- het in aanzienlijke mate waarschijnlijk is dat de in de bijlage opgenomen modelcontractbepalingen niet worden of niet zullen worden nageleefd en bijverdere doorgifte het risico bestaat dat de betrokkenen ernstige schade wordt berokkend.

Het is te verwachten dat deze clausule niet vaak zal worden gebruikt, aangezien deze alleen voor uitzonderlijke gevallen is bedoeld. Zoals in artikel 3, lid 3 van dit besluit is bepaald, wordt de Europese Commissie ingelicht over eventueel gebruik van deze clausule door een Lidstaat, waarna de ontvangen informatie wordt doorgegeven aan de andere Lidstaten. De Commissie kan passende maatregelen nemen overeenkomstig de procedure van artikel 31, lid 2 van de Richtlijn.

2.3.5. Procedure voor de toekenning van een vergunning

Om de procedure voor de toekenning van vergunningen sneller en meer gebruikersvriendelijk te maken, worden de aanvraagformulieren voor een vergunning rechtstreeks bij het CBP ingediend, die er advies over uitbrengt en dan het hele dossier aan de Minister van Justitie voorlegt. Om dezelfde redenen hebben het CBP en het Ministerie van Justitie overeenkomst bereikt over de hoofdlijnen van dit document; ze zijn tot een gemeenschappelijk begrip in deze materie gekomen op basis waarvan deze gevallen op consistente en goed afgestemde wijze kunnen worden afgehandeld.

De verantwoordelijke is doorgaans degene die de aanvraag indient. De wet verbiedt echter niet dat een vertegenwoordiger van een groep verantwoordelijken met gemeenschappelijke kenmerken een aanvraag indient, zolang de betreffende aanvraag een volledige lijst met namen van de daarbij betrokken verantwoordelijken bevat en de doorgiftes van de diverse verantwoordelijken kunnen worden aangeduid als een categorie doorgiftes, een nauwkeurig

omschreven groep doorgiftes met gemeenschappelijke elementen waarbij dezelfde omstandigheden een rol spelen.

Aanvragers van een vergunning moeten een formulier invullen, dat als een van de bijlagen bij dit document is gevoegd. Behalve het formulier moet de aanvrager het CBP een kopie sturen van het instrument dat door de partijen zal worden gebruikt om passende waarborgen te bieden en dat daardoor de grondslag vormt voor de toekenning van de vergunning. De partijen hoeven niet de volledige tekst van een dergelijk instrument of instrumenten toe te sturen; alleen de relevante delen of artikelen moeten worden bijgevoegd. De aanvrager is verantwoordelijk voor de selectie van de teksten en moet een verklaring ondertekenen waarin wordt aangegeven dat alle relevante documentatie tezamen met het aanvraagformulier werden ingediend.

Op basis van de informatie op het formulier maakt het CBP een eerste selectie van de aanvragen in verschillende categorieën. Deze verdeling heeft rechtstreekse gevolgen voor de manier waarop de aanvraag wordt beoordeeld en daardoor voor de tijd die de procedure voor de toekenning in beslag neemt.

De volgende categorieën worden onderscheiden:

2.3.5.1. Aanvragers die gebruikmaken van de modelcontracten met enkele toevoegingen

In dit geval is de beoordeling door het CBP gericht op de toegevoegde clausules, waarbij wordt vastgesteld of de toevoegingen rechtstreeks of indirect strijdig zijn met de modelcontracten of inbreuk maken op fundamentele rechten of vrijheden van de betrokkenen. Als het CBP tot de conclusie komt dat de toevoegingen bij de modelcontracten niet overeenstemmen met het Commissiebesluit, wordt de aanvrager in kennis gesteld van deze voorlopige conclusie. De aanvrager wordt dan in de gelegenheid gesteld zijn/haar aanvraag te heroverwegen en de tekst van de clausules aan te passen, binnen een periode die in de brief van het CBP wordt aangegeven. Als deze aanvullende stap nodig is, duurt de procedure onvermijdelijk een aantal weken langer voordat een advies aan de Minister wordt uitgebracht.

2.3.5.2. Aanvragers die gebruikmaken van de modelcontracten met wijzigingen of door henzelf opgestelde contractuele oplossingen

In dit geval voert het CBP een uitgebreidere beoordeling uit die meer tijd in beslag zal nemen dan de hierboven beschreven procedures. Het CBP informeert aanvragers die onder deze categorie vallen over de tijd die de procedure in beslag neemt voordat een advies aan de Minister wordt uitgebracht over het dossier.

De beoordeling van het CBP richt zich op de vereisten waaraan de contractuele oplossingen moeten voldoen, zoals aangegeven in paragraaf 2.3.2. van dit document.

De manier waarop de modelcontracten van de Commissie worden gebruikt (met of zonder toevoegingen of wijzigingen, met toevoegingen maar zonder wijzigingen, of met wijzigingen) heeft rechtstreeks invloed op de procedure waarmee de CBP de clausules beoordeelt en advies uitbrengt aan de Minister.
Het staat de partijen vrij hun eigen contractuele bepalingen of oplossingen te formuleren. In dat geval beoordeelt het CBP deze overeenkomstig de vereisten die in paragraaf 2.3.2. zijn aangegeven.

2.3.6. Wat gebeurt er nadat een beslissing is genomen over een aanvraag?

Als de Minister na ontvangst van het advies van het CBP besluit de aanvrager een vergunning te verlenen, stelt hij de Europese Commissie daarvan in kennis[52]. Zoals aangegeven in artikel 26, lid 3 van de Richtlijn moeten ook alle andere Lidstaten worden geïnformeerd over toegekende vergunningen.
Dit artikel bepaalt ook dat in gevallen waarin een Lidstaat of de Commissie op rechtmatige grond met betrekking tot de bescherming van de privacy van personen de toekenning aanvecht, de Commissie passende maatregelen moet nemen overeenkomstig de procedure van artikel 31, waarna de Lidstaten passende maatregelen moeten nemen om dit besluit na te leven. In de praktijk kan dat betekenen dat de Minister in dergelijke gevallen de vergunning intrekt of de voorwaarden wijzigt; ook daarvan moet de Europese Commissie in kennis gesteld worden[53].

Er kunnen andere redenen zijn die de intrekking of wijziging van een vergunning door de Minister rechtvaardigen. Zoals aangegeven in de memorie van toelichting bij de WBP[54], kan de Europese Commissie bijvoorbeeld van mening zijn dat het land waarnaar de persoonsgegevens worden doorgegeven geen passend beschermingsniveau biedt[55]. Het feit dat de Europese Commissie het beschermingsniveau in een bepaald land ontoereikend vindt, heeft in principe geen gevolgen voor een besluit dat met betrekking tot een vergunning voor doorgifte naar dat land is genomen, aangezien dat besluit is gebaseerd op passende waarborgen die door de verantwoordelijke worden geboden ter compensatie van het ontbreken van een passend beschermingsniveau in een derde land. Het negatieve besluit van de Commissie kan echter zijn gebaseerd op nieuwe feiten over de situatie in het derde land, die nieuw licht kunnen werpen op de overwegingen op basis waarvan de vergunning werd verleend.

[52] Artikel 78, lid 1, onder b, WBP.
[53] Artikel 78, lid 1, onder c, WBP.
[54] Pagina 196.
[55] Artikel 78, lid 2, onder a, WBP stelt dat de Minister een ministeriële regeling of beschikking zal uitvaardigen, wanneer dit volgt uit een besluit van de Commissie of Raad om doorgiftes naar een bepaald land buiten de EU te verbieden.

Een vergelijkbare situatie kan zich voordoen in uitzonderingsgevallen waarin het CBP op basis van artikel 4 van het Commissiebesluit over contracten, besluit het gegevensverkeer naar een bepaald land te verbieden of te onderbreken. Indien de Minister tot het oordeel komt dat een derde land geen passend beschermingsniveau moet hij de Europese Commissie daarvan in kennis stellen.[56]

Situaties waarin een vergunning wordt ingetrokken of opgeschort zijn zeer uitzonderlijk. Over het algemeen biedt dit instrument aanzienlijk meer rechtszekerheid dan een doorgifte naar een land waarvoor geen Communautair besluit over het beschermingsniveau bestaat op basis van artikel 76, lid 2 of artikel 77, lid 1.

[56] Artikel 78, lid 1, onder a, WBP

3. Een interessante beschikking van de Commissie: de Safe Harbour-regeling

Tot nu toe heeft de Commissie slechts vier beslissingen genomen met betrekking tot het beschermingsniveau in een derde land: de beschikkingen over Zwitserland, Hongarije en de Safe Harbour-regeling in de Verenigde Staten, die gedateerd zijn op 26 juli 2000[57]. De beschikking over Canada is genomen op 20 december 2001[58].
De beschikkingen over Zwitserland en Hongarije waren nauwelijks controversieel, aangezien in beide landen uitgebreide wetgeving bestaat voor de bescherming van gegevens. Beide landen hebben een onafhankelijke toezichthoudende autoriteit en beide hebben ze het Verdrag van de Raad van Europa ondertekend, geratificeerd en effectief geïmplementeerd[59].
Met betrekking tot de Verenigde Staten is de zaak minder eenvoudig. In artikel 25 bepaalt de Richtlijn dat de Europese Commissie, nadat zij heeft bevonden dat een land geen passend beschermingsniveau biedt, onderhandelingen kan openen met dat land met het doel tot een oplossing te komen voor die situatie.
Er is geen officieel besluit genomen waarin is bepaald dat het beschermingsniveau in de Verenigde Staten niet passend zou zijn. Velen waren echter van mening dat het bestaande juridische kader in Amerika, dat bestaat uit sectoriële wetgeving en procedures voor zelfregulering, op zich niet afdoende was.

Technisch gesproken hebben er geen onderhandelingen plaatsgevonden tussen de Europese Commissie en het Amerikaanse Department of Commerce over de Safe Harbour-regeling. De Europese Commissie kan alleen op basis van een mandaat van de Raad internationale onderhandelingen openen om tot internationale afspraken te komen.
In dit geval werd een dialoog of discussie gevoerd tussen beide partijen om standpunten uit te wisselen en om overeenstemming te bereiken over een mogelijke regeling die afdoende waarborgen zou bieden aan degenen die persoonsgegevens doorgeven aan ondernemingen die aan de beoogde regeling zouden deelnemen bij doorgifte.

Deze dialoog heeft meer dan twee jaar in beslag genomen en zowel de artikel 29-werkgroep als het Artikel 31-comité waren daar van het begin tot het eind bij betrokken. Na een aantal adviezen van de artikel 29-werkgroep[60] over kwesties die maatregelen van Amerikaanse zijde vereisten, heeft het Artikel 31-comité een unaniem positief standpunt ingenomen tijdens de bijeenkomst in mei 2000. Het officiële besluit van de Commissie werd in juli 2000 genomen.

De Safe Harbour-regeling is tamelijk complex en bestaat uit zeven principes die moeten worden gerespecteerd door de ondernemingen die aan de regeling deelnemen, evenals vijftien veelgestelde vragen en een verzameling bijlagen met diverse documenten.
Een interessant aspect van het Commissiebesluit is dat het alleen betrekking heeft op die ondernemingen die de Safe Harbour-principes aanhangen; met andere woorden, het is geen besluit dat van toepassing is op een heel land of een hele sector of bepaalde sectoren in een land, maar op een groep ondernemingen die vrijwillig heeft besloten een bepaald systeem te

[57] Publicatieblad van de Europese Gemeenschappen, L 215, Deel 43, 25 augustus 2000.
[58] Besluit van 20 december 2001, gepubliceerd in het Publicatieblad van de Europese Gemeenschappen L 2, 4 januari 2002.
[59] Publicatieblad van de Europese Gemeenschappen, L 215, Deel 43, 25 augustus 2000.
[60] Zie opinie 4/2000 van 16 mei 2000, opinie 3/2000 van 16 maart 2000, opinie 7/99 van december 1999, werkdocument van 7 juli 1999, opinie 4/99 van 7 juni 1999, opinie 2/99 van 3 mei 1999 en opinie 1/99 van 26 januari 1999.

volgen. De inschrijving daarvoor is daadwerkelijk vrijwillig: de ondernemingen doen alleen mee als ze dat willen. De voorschriften zijn echter bindend voor degenen die besluiten zich aan te melden.
Om verantwoordelijken in de EU te laten weten of een Amerikaanse onderneming kan worden beschouwd als een organisatie met een passend beschermingsniveau zoals bedoeld in dit besluit, beheert het Amerikaanse Department of Commerce een lijst van organisaties die zich voor de Safe Harbour-regeling hebben aangemeld. De lijst geeft ook duidelijk aan welke ondernemingen eventueel hun status als "veilige haven" hebben verloren, bijvoorbeeld omdat ze zich niet aan de regels hebben gehouden. De lijst kan door iedereen worden opgevraagd via de website van het Department of Commerce[61].

Wat de handhaving van de regeling betreft, vele Safe Harbour-ondernemingen laten hun naleving jaarlijks controleren door een onafhankelijke instantie, maar daartoe zijn ze niet verplicht. Er zijn regels aan de hand waarvan een onderneming zelf moet controleren of aan de voorschriften wordt voldaan. Daarna is de handhaving voornamelijk geregeld via alternatieve mechanismen voor de beslechting van geschillen. Onafhankelijke instanties uit de private sector zullen eventuele klachten onderzoeken en proberen een oplossing te vinden. Als een Safe Harbour-onderneming zich niet neerlegt bij de bevindingen van deze instanties, wordt de zaak doorverwezen naar de Federal Trade Commission of het Department of Transportation, afhankelijk van de betreffende sector, die wettelijk bevoegd zijn om naleving af te dwingen. Ernstige gevallen van overtreding hebben tot gevolg dat de betreffende onderneming van de lijst van de Department of Commerce wordt geschrapt.

De Europese toezichthoudende autoriteiten voor de bescherming van persoonsgegevens spelen ook een belangrijke rol als handhavingsinstituten voor organisaties die deelnemen aan de Safe Harbour-regeling, door middel van het zogenaamde Safe Harbour-panel. Meer informatie over dit panel vindt u op:
http://forum.europa.eu.int/Public/irc/secureida/safeharbor/home

Actuele informatie over de Safe Harbour-regeling en de actuele lijst van ondernemingen die het systeem toepassen vindt u op: http://www.export.gov/safeharbor/

[61] http://www.export.gov/safeharbor/

4. Praktijkvoorbeelden

In dit hoofdstuk volgt nu een aantal voorbeelden van de wijze waarop Hoofdstuk 11 WBP kan worden toegepast. Het iBazar-voorbeeld komt uit de praktijk.

4.1. iBazar – eBay

Een aantal maanden voordat de WBP van kracht werd, in juli 2001, werd het College bescherming persoonsgegevens om advies gevraagd ten aanzien van een omstreden zaak. Het ging daarbij om een voorgenomen doorgifte van klantgegevens aan de VS[62]. Het toenmalige advies van het CBP was gebaseerd op de tekst van de Richtlijn.

4.1.1. Feiten

iBazar, exploitant van veilingwebsites in diverse EU-landen, is overgenomen door het Amerikaanse bedrijf eBay. Om de overgang van de klanten van iBazar zo eenvoudig mogelijk te houden, wil eBay de klantgegevens van iBazar Nederland overbrengen naar de VS. Het voorstel van eBay is om de doorgifte te laten plaatsvinden, tenzij de klant hier bezwaar tegen maakt ('opt-out'-principe); de gegevens kunnen in de VS echter pas gebruikt worden nadat de klant hiervoor toestemming heeft gegeven ('opt-in'-principe).
De raadsman van iBazar noemt in zijn brief aan het CBP nog twee uitzonderingen die naar zijn mening eveneens als grond kunnen dienen om tot doorgifte over te gaan: enerzijds is de doorgifte noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke; anderzijds is de doorgifte noodzakelijk voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst.

4.1.2. Zoeken naar een oplossing

4.1.2.1. Is er sprake van passende bescherming?

Het besluit van de Europese Commissie over het Safe Harbour-regeling van juli 2000 houdt in, dat de aanmerking "passend beschermingsniveau" voorbehouden is aan bedrijven die zich bij deze regeling hebben aangesloten. Aangezien eBay zich niet bij deze regeling heeft aangesloten, is een passend beschermingsniveau geen rechtsgrond voor doorgifte.

4.1.2.2. Is een van de uitzonderingen van toepassing?

De raadsman van iBazar voerde drie mogelijke rechtsgronden aan voor de doorgifte:

- De eerste optie voor de voorgenomen doorgifte van gegevens is het verkrijgen van ondubbelzinnige toestemming van de betrokkene. De definitie van toestemming stelt dat het daarbij moet gaan om een vrije wilsuiting. Daarvan is in dit geval geen sprake, omdat het bedrijf gebruikmaakt van een 'opt-out'-constructie: het bedrijf neemt dus aan dat klanten hun toestemming verlenen indien zij geen expliciete afwijzing te kennen geven.
- De tweede optie heeft betrekking op het feit dat de doorgifte noodzakelijk is voor de uitvoering van een contract tussen de betrokkene en de verantwoordelijke. In het onderhavige geval bestaat er geen overeenkomst tussen de consument en eBay en zijn er

[62] Nadere informatie en de briefwisseling met de onderneming in kwestie, in het Nederlands en het Engels, is te vinden op: www.cbpweb.nl

evenmin aanwijzingen dat de voorgenomen doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de consument en iBazar.
- De derde optie heeft te maken met een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst. Deze uitzondering bevat de strikte voorwaarde dat de overeenkomst gesloten moet worden in het belang van de betrokkene. In dit geval is hiervan echter geen sprake, omdat de overname van iBazar door eBay berust op de commerciële belangen van de partijen in genoemde overeenkomst.

4.1.3. Conclusie

Tijdens de behandeling van deze zaak was een vergunning nog geen optie, omdat de WBP nog niet van kracht was.
Het bedrijf had twee mogelijkheden:
- eBay zou zich kunnen aansluiten bij het Safe Harbour-systeem, waardoor het de garantie van een passend beschermingsniveau kan bieden.
- eBay zou een 'opt-in'-constructie (toestemming) kunnen gebruiken voor alle klanten voordat de doorgifte plaatsvindt. Uit onderzoek van het CBP is gebleken dat eBay een dergelijke procedure heeft toegepast voor de doorgifte van klantgegevens van iBazar Frankrijk naar de VS[63].

eBay heeft de aanbeveling van het CBP inmiddels opgevolgd en voorafgaand aan de doorgifte een 'opt-in'-constructie ingevoerd voor alle klanten.

4.2. Doorgifte van een Nederlandse verantwoordelijke aan een bewerker in India

4.2.1. Feiten

Een Nederlands bedrijf met ongeveer 5.000 klanten besluit om te gaan samenwerken met een bewerker buiten de Europese Unie. Het bedrijf wil op die manier de kosten van gegevensverwerking voor zijn klantendatabase terugdringen en vindt in India een bedrijf dat over de juiste ervaring beschikt.

4.2.2. Zoeken naar een oplossing

4.2.2.1. Is er sprake van passende bescherming?

Er is geen besluit van de Europese Commissie en/of Ministeriële beschikking met betrekking tot het beschermingsniveau in India. Na diverse onderzoeken over gegevensbescherming te hebben geraadpleegd, komt de verantwoordelijke tot de conclusie dat in dit derde land noch algemene, noch sectoriële wetgeving van kracht is ten aanzien van gegevensbescherming.

4.2.2.2. Is een van de uitzonderingen van toepassing?

De verantwoordelijke neemt de lijst met uitzonderingen door in Artikel 76, lid 1 WBP. Drie van de hierin opgenomen uitzonderingen zouden in dit geval van toepassing kunnen zijn:
- ondubbelzinnige toesteming van de betrokkenen: het is in principe mogelijk om alle klanten te vragen toestemming te verlenen voor de doorgifte naar India. Dit is echter geen praktische oplossing, omdat dit met 5.000 klanten tot een erg kostbare en tijdrovende

[63] Bij de procedure die door iBazar Frankrijk is gebruikt, moest de gebruiker de volgende schriftelijke mededeling doen: "J'accepte : que mes coordonnées personnelles ainsi que mes informations de facturation soient transférées et traitées aux Etats-Unis" ("Ik aanvaard dat mijn persoons- en factureringsgegevens doorgegeven worden naar en gebruikt worden in de Verenigde Staten").

procedure zou leiden. Bovendien is er het risico dat een deel van de klanten geen toestemming geeft voor de doorgifte.
- de doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkenen en de verantwoordelijke: deze uitzondering is in dit geval niet van toepassing, omdat de doorgifte niet nodig is om dat doel te bereiken. De enige reden die het bedrijf heeft voor deze doorgifte is kostenbesparing.
- de doorgifte is noodzakelijk voor de sluiting of uitvoering van een in het belang van de betrokkenen tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst: deze uitzondering is hier niet van toepassing, omdat het contract met de bewerker niet wordt gesloten in het belang van de betrokkenen, maar in het belang van de verantwoordelijke.

4.2.2.3. Is het mogelijk om een vergunning te krijgen voor de doorgifte van gegevens?

Conform de verplichting in Artikel 14, lid 2 WBP dienen de verantwoordelijke en de bewerker hun respectievelijke verplichtingen vast te leggen in een overeenkomst. Naast de punten in Artikel 14 WBP zou dit contract bepalingen kunnen bevatten die voorzien in passende waarborgen voor de doorgifte (zie paragrafen 2.3.1. en 2.3.2.). Een dergelijke overeenkomst kan dienen als basis voor een vergunningaanvraag.
De Europese Commissie heeft op 27 december 2001 haar goedkeuring verleend aan een aantal modelcontracten tussen verantwoordelijken en bewerkers. Het is aan de partijen zelf om te bepalen of zij de modelcontracten van de Commissie gebruiken (hetgeen leidt tot een versnelling en vereenvoudiging van de aanvraagprocedure), dan wel hun eigen contracten opstellen.

4.3.2. Conclusie

Bij deze zaak is in het beoogde derde land geen sprake van een passend beschermingsniveau. Een van de uitzonderingen die de WBP aangeeft, toestemming, zou van toepassing kunnen zijn; deze oplossing is echter niet bepaald praktisch.
Een mogelijkheid is om een vergunning van de Minister van Justitie aan te vragen op basis van het contract tussen de verantwoordelijke en de bewerker.

4.3. Een doorgifte van een Nederlandse openbare instelling naar een openbare instelling in een derde land

4.3.1. Feiten

Een Nederlandse openbare instelling heeft belangstelling voor een uitwisseling van persoonsgegevens met een andere openbare instelling in een derde land, X, met betrekking tot Nederlandse burgers die naar dat land zijn geëmigreerd.
Land X is een democratisch, ontwikkeld land met een goed werkend rechtsstelsel en passende middelen voor schadeloosstelling van betrokkenen.

4.3.2. Zoeken naar een oplossing

4.3.2.1. Is er sprake van passende bescherming?

Er is vooralsnog geen besluit van de Commissie over het beschermingsniveau in land X. Na het CBP te hebben geraadpleegd, krijgt de Nederlandse verantwoordelijke te horen dat de Commissie binnen afzienbare tijd tot een positief besluit zal komen. Dit besluit zal echter direct verband houden met wetgeving die uitsluitend van toepassing is op de particuliere sector in X.

De verantwoordelijke ontdekt dat er een internationaal verdrag bestaat tussen het Nederlandse Ministerie en het Ministerie in X. Dit verdrag bevat een heel hoofdstuk over gegevensbescherming waarin de basisprincipes ten aanzien van inhoud en de vereisten voor procedures en handhaving (zie paragraaf 2.1.1.) in voldoende mate zijn omschreven.
De verantwoordelijke concludeert dat er sprake is van een passend beschermingsniveau voor de genoemde doorgifte.

4.4. Doorgifte van een Nederlands bedrijf naar een internationale database

4.4.1. Feiten

De Nederlandse verantwoordelijke van een wereldwijd opererende multinational besluit om personeelsgegevens beschikbaar te maken voor al haar dochterondernemingen. Hiervoor wordt een database geïnstalleerd in Amsterdam. Alle dochterondernemingen hebben toegang tot de database en kunnen persoonsgegevens verzenden, inzien of downloaden. In de praktijk betekent dit dat tussen de database in Nederland en elk van de landen in kwestie gegevens worden verzonden en ontvangen. In geografische zin worden dus persoonsgegevens vanuit Nederland verplaatst naar diverse derde landen.

4.4.2. Zoeken naar een oplossing

4.4.2.1. Is er sprake van passende bescherming?

De multinational heeft dochterondernemingen verspreid over de hele wereld. Voor landen in de Europese Unie levert dat geen beperkingen op, evenmin als voor landen waarover een Communautair besluit is genomen.
De Amerikaanse dochteronderneming heeft besloten de Safe Harbour-principes niet te onderschrijven. Hetzelfde probleem doet zich voor ten aanzien van de dochterondernemingen in landen waar geen of of slechts zeer beperkte regelgeving voor gegevensbescherming van kracht is.
Voor deze zaak zou een nauwkeurige beoordeling moeten worden uitgevoerd van het beschermingsniveau in een groot aantal landen. Ten minste kan worden vastgesteld dat de doorgifte betrekking heeft op een aanzienlijk aantal landen zonder passende bescherming.

4.4.2.2. Is een van de uitzonderingen van toepassing?

Hier is sprake van dezelfde situatie als in paragraaf 4.1.2.2. Toestemming zou een rechtsgrond inhouden voor doorgifte, maar betekent wel dat van alle werknemers in de hele wereld toestemming moet worden verkregen. Aangezien het toestemmingsformulier dient te vermelden dat werknemers de vrije keuze hebben om al of niet met de doorgifte in te stemmen, bestaat er een aanzienlijk risico dat een aantal werknemers geen toestemming verleent, dan wel deze toestemming later weer intrekt. Het nut van de database wordt hiermee twijfelachtig.
Zoals in paragraaf 4.1.2.2. al is aangegeven, bieden de overige uitzonderingen geen rechtsgrond voor doorgifte.

4.4.2.3. Is het mogelijk om een vergunning te krijgen voor de doorgifte van gegevens?

De verantwoordelijke zou een contractuele oplossing kunnen overwegen, waarbij alle dochterondernemingen zich verplichten de principes in de overeenkomst te zullen naleven. Deze contractuele oplossing zou met verschillende instrumenten kunnen worden gerealiseerd, die afzonderlijk of in combinatie met aanvullende contractuele regelingen passende bescherming zouden moeten bieden voor doorgifte.

De Nederlandse verantwoordelijke dient een vergunning aan te vragen op basis van de gekozen contractuele oplossing.

4.4.3. Conclusie

In een situatie waarin doorgifte van persoonsgegevens van een groot aantal betrokkenen naar meerdere landen moet gaan plaatsvinden, zou de meest praktische oplossing zijn om voor contractuele oplossingen te kiezen en de vergunningaanvraag aan de Minister hierop te baseren.
Wanneer de wetgeving over gegevensbescherming van meerdere landen van toepassing is op bepaalde aspecten van de verwerking, dienen de procedures te worden gevolgd zoals vastgelegd in de wetgeving van de landen in kwestie. Het verdient aanbeveling om in een dergelijke situatie gebruik te maken van de modelcontracten van de Europese Commissie, omdat dan de procedure voor de EU-landen zo min mogelijk vertraging oploopt.

4.5. Doorgifte van een Nederlands bedrijf naar een "minder democratisch" derde land

4.5.1. Feiten

Een Nederlands bedrijf heeft belangstelling voor een doorgifte van persoonsgegevens om deze te laten verwerken in een derde land, "Bananenrepubliek" genaamd, omdat de kosten voor verwerking daar erg laag zijn. In dit land heeft een onlangs een militaire staatsgreep plaatsgevonden, waardoor het politieke klimaat onstabiel is geworden. Volgens de laatste berichten hebben de politie en het leger de macht in handen.

4.5.2. Zoeken naar een oplossing

4.5.2.1. Is er sprake van passende bescherming?

De verantwoordelijke stelt vast dat er geen Communautair besluit bestaat ten aanzien van "Bananenrepubliek". In dit derde land is zeer uitgebreide wetgeving voor gegevensbescherming van kracht, waarin alle basisprincipes van de Europese gegevensbescherming vertegenwoordigd zijn. Uit een analyse van de vereisten voor procedures/handhaving in de huidige situatie komt naar voren dat de situatie in het land onbevredigend is. Op dat moment is in dat land dus geen sprake van passende bescherming.

4.5.2.2. Is een van de uitzonderingen van toepassing?

De enige mogelijke uitzondering die de verantwoordelijke in dit geval kan overwegen, is toestemming te vragen aan de betrokkenen. Naast de praktische problemen die in de voorgaande paragraaf worden beschreven, realiseert de verantwoordelijke zich dat aan de betrokkenen moet worden gemeld dat de gegevens worden overgedragen aan "Bananenrepubliek". Het is zeer onwaarschijnlijk dat de betrokkenen bereid zullen zijn onder de genoemde omstandigheden toestemming te verlenen.

4.5.2.3. Is het mogelijk een vergunning aan te vragen voor de doorgifte?

De verantwoordelijke zou kunnen overwegen om een vergunningaanvraag in te dienen op basis van de contractuele regelingen die met de bewerker in het derde land zijn getroffen.
De situatie in "Bananenrepubliek" zou in de praktijk echter betekenen dat de bewerker, zelfs wanneer deze van goede wil is en bereid de contractuele regelingen na te leven, hiertoe niet in staat zal zijn. In de contractuele regelingen zouden bepalingen kunnen worden opgenomen die de mogelijkheden van de bewerker om gegevens aan de staat te verstrekken, beperken. Dit zou echter geen wettelijke gevolgen hebben, omdat de bestaande wettelijke eisen en feitelijke

omstandigheden van het land in kwestie prevaleren boven contracten waaraan de gegevensimporteur onderhevig is.
Zoals de Europese toezichthoudende autoriteiten voor de bescherming van persoonsgegevens hebben vastgesteld, zijn landen waar de verplichting om informatie aan de staat te verstrekken verder gaat dan de behoeften van een democratische maatschappij en redenen van openbare orde, als bedoeld in Artikel 13, lid 1 van de Richtlijn, geen veilige bestemming voor een doorgifte op basis van contractuele oplossingen.

4.5.3. Conclusie

Doorgifte van persoonsgegevens naar "Bananenrepubliek" zou in de huidige situatie een onaanvaardbaar risico inhouden voor de betrokkenen. Wanneer de verantwoordelijke een verzoek tot doorgifte zou indienen, zou het CBP de Minister een negatief advies geven. Zoals vermeld in Artikel 78 WBP kan de Minister de Commissie van de Europese Gemeenschappen in kennis stellen van het feit dat, naar zijn oordeel, dit derde land geen waarborgen voor een passend beschermingsniveau biedt in de zin van artikel 76, lid 1.

4.6. Doorgifte van een Nederlandse financiële instelling aan diverse financiële instellingen buiten de Europese Unie

4.6.1. Feiten

Een Nederlandse financiële instelling wil persoonsgegevens gaan uitwisselen met andere financiële instellingen buiten de Europese Unie in het kader van een programma ter preventie en opsporing van fraude.

4.6.2. Zoeken naar een oplossing

4.6.2.1. Is er sprake van passende bescherming?

De financiële instelling heeft over de hele wereld dochterondernemingen. Voor landen in de Europese Unie levert dat geen beperkingen op, evenmin als voor landen waarover een Communautair besluit is genomen.
De Amerikaanse dochteronderneming heeft besloten om de Safe Harbour-principes niet te onderschrijven of is hiertoe niet in staat. Hetzelfde probleem doet zich voor ten aanzien van de dochterondernemingen in landen waar geen of of slechts zeer beperkte regelgeving voor gegevensbescherming van kracht is.
Voor deze zaak zou een nauwkeurige beoordeling moeten worden uitgevoerd van het beschermingsniveau in een groot aantal landen. Ten minste kan worden vastgesteld dat de doorgifte betrekking heeft op een aanzienlijk aantal landen zonder passende bescherming.

4.6.2.2. Is een van de uitzonderingen van toepassing?

Op het eerste gezicht lijkt de uitzondering uit Artikel 77, lid 1, onder d (doorgifte noodzakelijk op grond van een zwaarwegend algemeen belang, of voor de vaststelling, uitoefening of verdediging in rechte van enig recht) van toepassing te zijn.
In de praktijk is het echter minder eenvoudig. Het eerste gedeelte van deze uitzondering heeft volgens de interpretatie van de Werkgroep alleen betrekking op bepaalde vormen van beperkte overdracht tussen overheden. Niet elk algemeen belang is op zich afdoende rechtvaardiging voor doorgifte; er moet sprake zijn van een zwaarwegend algemeen belang.
Het tweede deel van deze uitzondering, de doorgifte van gegevens voor de vaststelling, uitoefening of verdediging in rechte van enig recht, is evenmin een grond voor doorgifte van persoonsgegevens ten behoeve van algemene maatregelen voor fraudepreventie en -

opsporing, zelfs wanneer als gevolg van de genomen maatregelen een aantal fraudegevallen aan het licht komt en tot gerechtelijke vervolging wordt overgegaan.

4.6.2.3. Is het mogelijk om een vergunning te krijgen voor de doorgifte van gegevens?

De verantwoordelijke zou een contractuele oplossing kunnen overwegen, waarin alle dochterondernemingen zich verplichten de principes in de overeenkomst te zullen naleven. Deze contractuele oplossing zou met verschillende instrumenten kunnen worden gerealiseerd, die afzonderlijk of in combinatie met aanvullende contractuele regelingen passende bescherming zouden moeten bieden voor doorgifte.
De Nederlandse verantwoordelijke dient een vergunning aan te vragen op basis van de gekozen contractuele oplossing.

4.6.3. Conclusie

In een situatie waarin doorgifte van persoonsgegevens van een groot aantal betrokkenen naar meerdere landen moet gaan plaatsvinden, zou de meest praktische oplossing zijn om voor contractuele oplossingen te kiezen en hierop de vergunningaanvraag bij de Minister te baseren.
Wanneer de wetgeving over gegevensbescherming van meerdere landen van toepassing is op bepaalde aspecten van de bewerking, dienen de procedures te worden opgevolgd zoals vastgelegd in de wetgeving van de landen in kwestie. Het verdient aanbeveling om in een dergelijke situatie gebruik te maken van de modelcontracten van de Europese Commissie, omdat dan de procedure in de desbetreffende EU-landen zo weinig mogelijk vertraging oploopt.

Bijlagen:

- verplicht door vergunningaanvragers te gebruiken formulier.

- door de Europese Commissie goedgekeurde contracten voor de doorgifte tussen verantwoordelijken (Commissiebesluit juni 2001): http://www.europa.eu.int/comm/internal_market/en/dataprot/news/index.htm

- door de Europese Commissie goedgekeurde contracten voor doorgiftes tussen verantwoordelijken en bewerkers (Commissiebesluit december 2001): http://europa.eu.int/eur-lex/en/dat/2002/l_006/l_00620020110en00520062.pdf

- Commissiebesluiten ten aanzien van Zwitserland, Hongarije en de VS, 26 juli 2000: http://www.europa.eu.int/comm/internal_market/en/dataprot/news/index.htm

- Commisiebesluit ten aanzien van Canada, 20 december 2001: http://europa.eu.int/eur-lex/en/dat/2002/l_002/l_00220020104en00130016.pdf

Aanvraagformulier voor een vergunning zoals omschreven in Artikel 77.2 WBP (verplicht te gebruiken)

Dit aanvraagformulier dient door de aanvrager worden ingevuld en ondertekend.

Ter attentie van de Minister van Justitie p/a College bescherming persoonsgegevens – Prins Clauslaan 20 – 2509 AJ Den Haag

Gegevens van de bij de doorgifte betrokken partijen

Gegevensexporteur

Gegevensexporteur is …(omschrijf kort de activiteiten die betrekking hebben op de doorgifte), gevestigd in …(vul land in).

Gegevensimporteur

Gegevensimporteur is …(omschrijf kort de activiteiten die betrekking hebben op de doorgifte), gevestigd in …(vul land in).

Betrokkenen

De door te geven persoonsgegevens hebben betrekking op de volgende categorieën van betrokkenen (noem categorieën). Indien van toepassing dient onderscheid te worden gemaakt op basis van de aard van de gegevens.

Doel van de doorgifte

De doorgifte is noodzakelijk om de volgende redenen (noem redenen). Indien van toepassing dient onderscheid te worden gemaakt op basis van de aard van de gegevens.

Gegevenscategorieën

De door te geven persoonsgegevens vallen in de volgende gegevenscategorieën (noem categorieën)

Bijzondere gegevens (indien van toepassing)

De door te geven persoonsgegevens vallen in de volgende categorieën van bijzondere gegevens gegevens (noem categorieën)

Ontvangers

De door te geven persoonsgegevens mogen uitsluitend worden verstrekt aan de volgende ontvangers(categorieën) (noem ontvangers(categorieën)). Indien van toepassing dient onderscheid te worden gemaakt op basis van de aard van de gegevens.

Bewaartermijn

De door te geven persoonsgegevens mogen niet langer dan (noem termijn) worden bewaard. Indien van toepassing dient onderscheid te worden gemaakt op basis van de aard van de gegevens.

Contactpersoon

Vul voor de exporteur en de importeur de naam en contactgevens in van een contactpersoon ten behoeve van verdere communicatie met het CBP.

Basis voor de vergunning

Welk instrument is door de partijen gebruikt om “passende waarborgen” voor de voorgenomen doorgifte te garanderen? (Noem instrument. Een kopie van de relevante onderdelen van het instrument dient als bijlage bij dit formulier te worden gevoegd)

Hebt u de door de Europese Commissie goedgekeurde modelcontracten gebruikt? (Kruis aan wat van toepassing is) Ja □ Nee □ Indien het vorige antwoord bevestigend was, beantwoord dan ook de volgende vragen:

- Vul de volledige referentie in van het door u gebruikte modelcontract van de Europese Commissie.

- Zijn er bepalingen aan het bestaande modelcontract toegevoegd? Ja □ Nee □
  Zo ja, geef dan aan welke.

- Zijn er bepalingen van het modelcontract gewijzigd? Ja □ Nee □
  Zo ja, geef dan aan welke.

Hebt u nog andere bestaande contracten gebruikt die niet door de Europese Commissie zijn goedgekeurd, zoals contracten van ICC, CBI, Raad van Europa 1992…? Ja □ Nee □
Zo ja, geef dan aan welke.

Aanvullende informatie *(niet verplicht)*

Heeft u, of één van de aan u geaffilieerde ondernemingen, toestemming gevraagd in andere lidstaten van de EU voor een vergelijkbare doorgifte op basis van dit of een vergelijkbaar instrument?

Ja □ Nee □

Zo ja, geef s.v.p. aan in welke lidstaten.

Gebruik deze ruimte voor overige informatie die betrekking heeft op deze doorgifte.

Handtekening

Gegevensexporteur

De exporteur verklaart hierbij dat alle relevante documentatie voor de beoordeling van de toereikendheid van de geboden waarborgen als bijlage bij dit formulier zijn toegezonden aan het CBP.

Naam:

Datum:

Bevoegde handtekening: