EUROPESE COMMISSIE
DIRECTORAAT-GENERAAL XV
INTERNE MARKT EN FINANCIËLE DIENSTEN
Vrij verkeer van informatie, vennootschapsrecht en financiële informatie
Vrij verkeer van informatie, gegevensbescherming en internationale aspecten daarvan

DG XV D/5025/98
WP 12

Groep voor de bescherming van personen
in verband met de verwerking van persoonsgegevens

Werkdocument

Doorgifte van persoonsgegevens naar derde landen : toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming

Goedgekeurd door de groep op 24 juli 1998

Inhoud

Inleiding

Dit document heeft tot doel de tot dusver uitgevoerde werkzaamheden van de Groep voor de bescherming van persoonsgegevens, die overeenkomstig artikel 29 van de richtlijn gegevensbescherming[1] werd opgericht, samen te brengen en zo de standpunten over alle vraagstukken die centraal staan bij de persoonsgegevensstromen naar derde landen in het kader van de toepassing van de richtlijn gegevensbescherming van de EU (95/46/EG), op een rij te zetten. Bij de opstelling van het document is uitgegaan van de regeling voor de doorgifte van persoonsgegevens naar derde landen, zoals vastgelegd in de artikelen 25 en 26 van de richtlijn. (De tekst van deze artikelen is opgenomen in bijlage 2).

In artikel 25, lid 1, is het beginsel vastgelegd dat lidstaten alleen persoonsgegevens doorgeven als het betrokken derde land een passend beschermingsniveau waarborgt. In lid 2 is bepaald dat het "passend karakter" per geval wordt beoordeeld "met inachtneming van alle omstandigheden die op de doorgifte van gegevens of op een categorie gegevensdoorgiften van invloed zijn". Lid 6 stelt dat de Commissie kan constateren dat bepaalde landen waarborgen voor een passend beschermingsniveau bieden. In **hoofdstuk 1** van dit document wordt verder ingegaan op dit centrale begrip, het passend beschermingsniveau. Er wordt getracht te verklaren wat met "passend" wordt bedoeld en er wordt een kader geschetst voor de beoordeling van het passende beschermingsniveau in specifieke gevallen.

In de hoofdstukken 2 en 3 wordt de toepassing van deze aanpak verder behandeld. In **hoofdstuk 2** wordt ingegaan op doorgiften naar landen die Verdrag nr. 108 van de Raad van Europa hebben geratificeerd, terwijl in **hoofdstuk 3** de verschillende vraagstukken aan bod komen die zich voordoen als de bescherming van doorgegeven gegevens niet voortvloeit uit wetgeving, maar voornamelijk of geheel uit zelfreguleringsmechanismen.

Bij het ontbreken van een passend beschermingsniveau in de zin van artikel 25, lid 2, wordt door artikel 26, lid 2, van de richtlijn voorzien in de mogelijkheid *ad hoc*-oplossingen - met name van contractuele aard - toe te passen. Hierdoor kunnen dan toch voldoende waarborgen worden geboden om de doorgifte te doen plaatshebben. In **hoofdstuk 4** van dit document wordt bestudeerd in welke omstandigheden *ad hoc*-oplossingen van contractuele aard passend zijn en zijn enkele aanbevelingen opgenomen met betrekking tot de vorm en inhoud van dergelijke oplossingen.

---

[1] Zie **WP 4 (5020/97)** "Eerste richtsnoeren voor de doorgifte van persoonsgegevens naar derde landen - Voorstel inzake een methode voor de beoordeling van het passend karakter van het beschermingsniveau", een discussiedocument dat op 26 juni 1997 door de Groep werd aangenomen.
WP 7 (5057/97) Werkdocument: "Beoordeling van zelfregulering: wanneer komt zelfregulering door de industrie het beschermingsniveau van gegevens in geval van overdracht naar een derde land ten goede?", dat op 14 januari 1998 door de Grroep werd aangenomen.
WP 9 (5005/97) Werkdocument: "Voorlopig standpunt inzake het gebruik van contractuele bepalingen in het kader van de overdracht van persoonsgegevens naar derde landen", dat op 22 april 1998 door de Groep werd goedgekeurd.

In **hoofdstuk 5** wordt dan ingegaan op de derde en laatste mogelijkheid waarin door de richtlijn wordt voorzien: het beperkt aantal gevallen, zoals genoemd in artikel 26, lid 1, waarin in de praktijk van het vereiste van een passend beschermingsniveau mag worden afgeweken. De precieze draagwijdte van deze afwijkingen wordt bestudeerd en er worden voorbeelden gegeven van gevallen waarin een beroep kan worden gedaan op dit artikel en gevallen waarin dat niet mogelijk is.

Hoofdstuk 6 tot slot bevat enkele opmerkingen over procedurele vraagstukken die zich in verband met de beoordeling van het beschermingsniveau (passend of niet passend) en de totstandbrenging van een coherente communautaire aanpak van deze vraagstukken voordoen.

Bijlage I bevat een reeks voorbeelden die bedoeld zijn om aan te tonen hoe de in dit document uiteengezette aanpak in de praktijk kan worden toegepast.

HOOFDSTUK 1: BEOORDELEN OF HET BESCHERMINGSNIVEAU "PASSEND" IS

(1) Wanneer is het beschermingsniveau "passend"?

De gegevensbescherming heeft tot doel een bescherming te garanderen aan de persoon over wie gegevens worden verwerkt. Dit wordt doorgaans bewerkstelligd door middel van een combinatie van rechten van de betrokkene enerzijds en plichten van degene die de gegevens verwerkt of voor de verwerking verantwoordelijk is anderzijds. De in Richtlijn 95/46/EG neergelegde rechten en plichten gaan terug op de in het Verdrag nr. 108 van de Raad van Europa (1981) vervatte rechten en plichten, welke nauw aansluiten bij de beginselen van de OESO-richtsnoeren (1980) of van de richtsnoeren van de Verenigde Naties (1990). Hieruit kan worden afgeleid dat over de inhoud van de gegevensbeschermingsvoorschriften een ruime consensus bestaat die zich tot ver buiten de vijftien EU-lidstaten uitstrekt.

De gegevensbeschermingsvoorschriften dragen evenwel alleen dan aan de bescherming van personen bij, wanneer zij in de praktijk effectief worden toegepast. Daarom moet niet alleen worden gekeken naar de inhoud van de voorschriften die van toepassing zijn op naar een derde land doorgegeven persoonsgegevens, maar ook naar de mechanismen waarmee de doelmatigheid ervan wordt gegarandeerd. In Europa zijn de gegevensbeschermingsvoorschriften traditioneel verankerd in wetten, zodat schendingen kunnen worden bestraft en schadeloosstelling kan worden gevorderd. Daarnaast voorzien deze wetten doorgaans in aanvullende procedurele mechanismen, zoals de instelling van toezichthoudende autoriteiten bij wie ook klachten kunnen worden ingediend. Deze procedurele aspecten zijn in Richtlijn 95/46/EG terug te vinden in de bepalingen betreffende aansprakelijkheid, sancties, rechtsmiddelen, toezichthoudende autoriteiten en kennisgeving. Buiten de Gemeenschap komen dergelijke procedurele mechanismen, die moeten garanderen dat de voorschriften hun beslag krijgen, veel minder vaak voor. Zo worden de partijen bij Verdrag nr. 108 opgeroepen de beginselen van de gegevensbescherming in hun wetgeving op te nemen, maar worden er geen aanvullende mechanismen zoals een toezichthoudende autoriteit verlangd. Zo ook verlangen de OESO-richtsnoeren enkel dat de beginselen in het nationale recht “in acht worden genomen” en garanderen zij dus op procedureel vlak geenszins dat de richtsnoeren daadwerkelijk in een doelmatige bescherming resulteren. De VN-richtsnoeren, die van latere datum zijn, bevatten wél bepalingen over toezicht en sancties, hetgeen duidt op het groeiende besef dat er op wereldniveau moet worden toegezien op een goede handhaving van de gegevensbeschermingsvoorschriften.

Zo is duidelijk dat een zinvolle analyse van een passend beschermingsniveau twee fundamentele elementen moet omvatten: de inhoud van de toepasselijke voorschriften en de middelen om de handhaving ervan te garanderen.

Met Richtlijn 95/46/EG als uitgangspunt en met de overige internationale regelingen voor ogen zou een lijst van basisbeginselen moeten kunnen worden vastgesteld voor de “inhoud” van de gegevensbeschermingsregels en voor de “procedurele/handhavingsvereisten”, welke beginselen dan als minimumvereisten voor een passend beschermingsniveau kunnen worden beschouwd. Het moet hierbij niet

gaan om een onveranderlijke lijst, want in een aantal gevallen zal hij moeten worden aangevuld, terwijl in andere gevallen van bepaalde vereisten zal moeten worden afgezien. De omvang van het risico van de doorgifte voor de betrokkene is een belangrijke factor om uit te maken welke vereisten in een concreet geval moeten worden gesteld. De samenstelling van een basislijst van minimumvereisten blijft desondanks een nuttig uitgangspunt voor elke analyse.

(i) Beginselen betreffende de inhoud

De navolgende beginselen worden in overweging gegeven:

1) **specificiteit** - gegevens moeten met een specifiek doel worden verwerkt en mogen vervolgens enkel worden gebruikt en doorgegeven als dat niet onverenigbaar is met het doel van de doorgifte. De enige uitzonderingen op deze regel zijn de in een democratische samenleving noodzakelijke gevallen, zoals bedoeld in artikel 13 van de richtlijn[2].

2) **kwaliteit en evenredigheid van de gegevens** - de gegevens moeten correct en, zo nodig, geactualiseerd zijn. Zij moeten passend en relevant zijn en mogen gelet op het doel van de doorgifte of van de verdere verwerking niet excessief zijn.

3) **transparantie** - aan natuurlijke personen moet informatie worden verstrekt over het doel van de verwerking en de identiteit van de voor de verwerking verantwoordelijke in het derde land, alsmede alle verdere informatie die nodig is om een eerlijke verwerking te garanderen. Uitzonderingen hierop zijn enkel mogelijk binnen de grenzen van de artikelen 11, lid 2,[3] en 13 van de richtlijn.

4) **beveiliging** - de voor de verwerking verantwoordelijke moet technische en organisatorische beveiligingsmaatregelen treffen die in overeenstemming zijn met de risico's van de verwerking. Eenieder die onder het gezag van de voor de verwerking verantwoordelijke staat, met inbegrip van een in opdracht werkende verwerker, mag enkel volgens zijn instructies gegevens verwerken.

5) **recht van toegang, rectificatie en verzet** - de betrokken persoon moet recht hebben op een kopie van alle hem betreffende gegevens die worden verwerkt alsmede recht op rectificatie wanneer deze gegevens onjuist blijken. In bepaalde situaties moet de betrokkene zich ook tegen verwerking van zijn gegevens kunnen verzetten. Uitzonderingen op deze rechten zijn alleen mogelijk in overeenstemming met artikel 13 van de richtlijn.

---

[2] Overeenkomstig artikel 13 is een beperking van het "specifiteitsbeginsel" mogelijk, indien deze noodzakelijk is ter vrijwaring van de veiligheid van de Staat, de landsverdediging, de openbare veiligheid, het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of schendingen van de beroepscodes voor gereglementeerde beroepen, een belangrijk economisch en financieel belang of de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

[3] In artikel 11, lid 2, is bepaald dat, wanneer de gegevens niet bij de betrokkene zijn verkregen, de informatie niet aan de betrokkenne hoeft te worden verstrekt, indien dit onmogelijk blijkt of onevenredig veel moeite kost of indien de registratie of verstrekking bij wet is voorgeschreven.

6) **beperking van doorgifte naar anderen** - verdere doorgifte van persoonsgegevens door de ontvanger van de oorspronkelijke doorgifte mag slechts worden toegestaan wanneer de regels die een passend beschermingsniveau garanderen ook van toepassing zijn op de tweede ontvanger (d.w.z. de ontvanger van de verdere doorgifte). Hiervan kan enkel worden afgeweken binnen de grenzen van artikel 26, lid 1, van de richtlijn. (In hoofdstuk 5 wordt verder op deze afwijkingen ingegaan).

Hieronder volgen enkele voorbeelden van beginselen die ook op bepaalde soorten verwerkingen van toepassing zijn:

1) **gevoelige gegevens** - wanneer het gaat om "gevoelige" categorieën gegevens (opgesomd in artikel 8 van de richtlijn[4]) moeten extra beveiligingsmaatregelen worden genomen, zoals het vereiste dat de betrokkene uitdrukkelijk met de verwerking instemt.

2) **direct marketing** - als gegevens voor direct-marketingdoeleinden worden doorgegeven, dan moet de betrokkene te allen tijde bezwaar kunnen maken tegen het gebruik van zijn persoonsgegevens voor dergelijke doeleinden.

3) **geautomatiseerde individuele besluiten** - heeft de doorgifte een geautomatiseerd individueel besluit in de zin van artikel 15 van de richtlijn tot doel, dan moet de betrokkene het recht hebben in kennis te worden gesteld van de argumenten die aan dit besluit ten grondslag liggen en dienen andere maatregelen te worden genomen om zijn rechtmatige belangen te beschermen.

(ii) Procedurele/handhavingsmechanismen

In Europa bestaat een ruime consensus dat de gegevensbeschermingsbeginselen in wetteksten moeten zijn verankerd en dat een systeem van "extern toezicht", in de vorm van een onafhankelijke autoriteit, noodzakelijk is om de naleving van de gegevensbeschermingsregels te garanderen. Elders in de wereld ligt dat vaak anders.
Als uitgangspunt voor de beoordeling van het passend karakter van de bescherming moeten de doelstellingen worden geïdentificeerd die aan het procedureel gegevensbeschermingssysteem ten grondslag liggen; op basis hiervan moet dan worden uitgemaakt of de verscheidene in derde landen geldende gerechtelijke en buitengerechtelijke mechanismen aan deze doelstellingen beantwoorden.

Een gegevensbeschermingssysteem heeft in wezen drieërlei doel:

1) Een **goede naleving** van de voorschriften verzekeren**.** (Geen enkel systeem garandeert volledige naleving, maar sommige systemen zijn beter dan andere). De kwaliteit van een systeem kan doorgaans worden afgeleid uit de mate waarin degenen die voor de verwerking verantwoordelijk zijn besef hebben van hun plichten en de mate

[4] Gegevens waaruit de raciale of ethnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, gegevens die de gezondheid en het seksuele leven betreffen en gegevens inzake overtredingen, strafrechtelijke veroordelingen of veiligheidsmaatregelen.

waarin de betrokkenen op de hoogte zijn van hun rechten en de hen ter beschikking staande middelen om deze te doen gelden. Doeltreffende, afschrikkende sancties kunnen van groot belang zijn om de handhaving van de voorschriften te garanderen; hetzelfde geldt natuurlijk voor een directe controle door de autoriteiten, auditors of onafhankelijke gegevensbeschermingscontroleurs.

2) **Bijstand verlenen** aan de betrokkenen bij de uitoefening van hun rechten. Eenieder moet zijn rechten snel, doeltreffend en zonder hoge kosten kunnen doen gelden. Dit vooronderstelt een institutioneel mechanisme voor onafhankelijk onderzoek van de klachten.

3) Een **passende schadeloosstelling** verzekeren aan de ten gevolge van schending van de voorschriften gelaedeerde partij. Dit is van het grootste belang en vereist onder meer een onafhankelijke scheidsrechterlijke instelling die schadevergoedingen mogelijk maakt en zo nodig sancties kan opleggen.

HOOFDSTUK 2: TOEPASSING VAN DE AANPAK OP LANDEN DIE VERDRAG NR. 108 VAN DE RAAD VAN EUROPA GERATIFICEERD HEBBEN

Naast de richtlijn is Verdrag nr. 108 het enige instrument in het internationale recht dat de bescherming van gegevens betreft. Het merendeel van de verdragspartijen zijn tevens lidstaat van de Europese Unie (alle 15 EU-lidstaten hebben het verdrag inmiddels geratificeerd) of zijn - zoals Noorwegen en IJsland - op grond van de overeenkomst betreffende de Europese Economische Ruimte door de richtlijn gebonden. Het verdrag werd evenwel ook geratificeerd door Slovenië, Hongarije en Zwitserland, waarschijnlijk binnenkort gevolgd door andere derde landen, met name daar landen die geen lid zijn van de Raad van Europa zich bij het verdrag kunnen aansluiten. Het is dus nuttig, en niet alleen vanuit zuiver academisch oogpunt, om te onderzoeken of de landen die het verdrag hebben geratificeerd kunnen worden aangemerkt als landen met een passend beschermingsniveau in de zin van artikel 25 van de richtlijn.

Als uitgangspunt is het niettemin nuttig de tekst van het verdrag zelf te analyseren in het licht van de theoretische beschrijving van het begrip "passend beschermingsniveau" in hoofdstuk 1 van dit document.

Wat de inhoud van de basisbeginselen betreft, kan worden gezegd dat het verdrag aan de eerste vijf van de zes "minimumvereisten" voldoet[5]. De overeenkomst bevat ook het vereiste dat in het geval van gevoelige gegevens passende waarborgen moeten worden gegeven, die voor een goede bescherming bij dit soort gegevens onontbeerlijk zijn.

Wat in het verdrag op inhoudelijk vlak essentieel ontbreekt, zijn beperkingen voor de doorgifte naar landen die geen partij zijn bij het verdrag. Dit betekent dat een land dat partij is bij Verdrag nr. 108 als "tussenstation" kan dienen voor het doorgeven van gegevens vanuit de Gemeenschap naar een ander derde land waar het beschermingsniveau totaal ontoereikend is.

Het tweede aspect van het "passende beschermingsniveau" betreft de procedurele mechanismen die de handhaving van de basisbeginselen moeten garanderen. Het verdrag schrijft voor dat de beginselen in het nationale recht moeten worden opgenomen en dat passende sancties en rechtsmiddelen moeten worden vastgesteld voor gevallen van schending van de beginselen. Dit zou moeten volstaan om te garanderen dat de voorschriften genoegzaam worden nageleefd en dat voor de betrokkenen in geval van schending van de voorschriften beroep bij de rechter openstaat (doelstellingen 1 en 3 van een handhavingsmechanisme). Het verdrag verplicht de verdragspartijen evenwel niet institutionele mechanismen in te voeren voor onafhankelijk onderzoek van klachten, hoewel in de praktijk de landen die het verdrag hebben geratificeerd dat meestal wel hebben gedaan. Dit is een zwak punt van het

[5] Enige twijfel is mogelijk wat het "transparantiebeginsel" betreft. Artikel 8, onder a), van het Verdrag voorziet niet echt in de *actieve* verplichting tot informatieverstrekking, die de essentie van de artikelen 10 en 11 van de richtlijn uitmaakt. Bovendien bevat het verdrag geen specifieke bepalingen betreffende de mogelijkheid bezwaar te maken tegen het gebruik van de gegevens voor direct marketing noch bepalingen met betrekking tot geautomatiseerde individuele besluiten ("profiling").

verdrag: wanneer dit soort institutionele mechanismen ontbreekt, bestaat het risico dat de betrokkenen in bepaalde gevallen geen adequate garantie van bijstand voor de uitoefening van hun rechten hebben (doelstelling 2).

Deze korte analyse lijkt erop te wijzen dat van de doorgifte van persoonsgegevens naar landen die Verdrag nr. 108 hebben geratificeerd mag worden aangenomen dat zij op grond van artikel 25, lid 1, van de richtlijn toelaatbaar is, op voorwaarde:

- dat ook het betrokken land over passende institutionele mechanismen beschikt om op de naleving toe te zien, betrokkenen bij te staan en verhaalmogelijkheden te verschaffen (zoals een onafhankelijke toezichthoudende autoriteit met passende bevoegdheden) en
- dat het de eindbestemming van de doorgifte is en niet een tussenstation voor verdere doorgifte, tenzij de gegevens verder worden doorgegeven aan een EU-land of een andere bestemming die een passend beschermingsniveau biedt[6].

Dit is natuurlijk een sterk vereenvoudigde en oppervlakkige analyse van het verdrag. Het is dan ook niet uitgesloten dat zich bij concrete gegevensdoorgiften naar derde landen die partij zijn bij het verdrag, nieuwe problemen voordoen die hier niet zijn behandeld.

[6] Verdrag nr. 108 wordt momenteel opnieuw bestudeerd, wat kan leiden tot wijzigingen die bedoeld zijn deze en andere problemen op te lossen.

HOOFDSTUK 3: TOEPASSING VAN DE AANPAK OP ZELFREGULERING DOOR DE INDUSTRIE

Inleiding

Artikel 25, lid 2, van de richtlijn betreffende gegevensbescherming (95/46/EG) bepaalt dat het door een derde land geboden beschermingsniveau moet worden beoordeeld met inachtneming van *alle omstandigheden* die op de doorgifte van gegevens of op een categorie gegevensdoorgiften van invloed zijn. Hierbij wordt niet alleen specifiek naar rechtsregels verwezen, maar ook naar "de beroepscodes en de veiligheidsmaatregelen die in die landen worden nageleefd".

Er moet dus ook rekening worden gehouden met niet in de wet verankerde voorschriften die in het betrokken derde land van kracht kunnen zijn, op voorwaarde dat deze *worden nageleefd*. Dit is de context waarin de rol van zelfregulering door de industrie moet worden onderzocht.

Wat is zelfregulering?

De term "zelfregulering" heeft niet voor iedereen dezelfde betekenis. In dit document moet onder *code voor zelfregulering* (of elk ander instrument dat daartoe strekt) worden verstaan: een verzameling van regels tot bescherming van gegevens, die van toepassing is op meerdere tot eenzelfde beroepsgroep of sector behorende verantwoordelijken voor de verwerking van persoonsgegevens, en waarvan de inhoud hoofdzakelijk door de leden van die beroepsgroep of sector is vastgelegd.

Dit is een brede definitie die – in het ene uiterste - een vrijblijvende code voor de bescherming van gegevens, opgesteld door een kleine brancheorganisatie met slechts enkele leden, kan omvatten alsook - in het andere uiterste - de gedetailleerde codes inzake beroepsethiek die gelden voor volledige beroepsgroepen, zoals artsen en bankiers, en vaak bijna rechtskracht hebben.

Is de organisatie die de code heeft opgesteld, representatief voor de sector?

Zoals ook verder in dit hoofdstuk wordt betoogd, is een belangrijke maatstaf voor de waarde van een code de afdwingbaarheid van de regels. De vraag naar de representativiteit van de organisatie die de code heeft opgesteld, is hier waarschijnlijk ondergeschikt aan het gewicht dat zij in de schaal kan werpen om bijvoorbeeld haar leden wegens niet-naleving van de code een sanctie op te leggen. Er zijn evenwel andere redenen waarom codes die voor een volledige sector of beroepsgroep gelden en in zeer ruime kring toepassing vinden, beter geschikt zijn als instrument voor gegevensbescherming dan codes van kleine groepen van ondernemingen binnen een sector. In de eerste plaats komt een versnipperde sector die gekenmerkt wordt door verschillende rivaliserende organisaties met elk hun eigen code voor gegevens-bescherming, verwarrend over op de consument. Door het naast elkaar bestaan van meerdere, onderling verschillende codes ontstaat een algemeen beeld dat voor de betrokkene te weinig transparant is. Het tweede punt is dat, met name in sectoren zoals direct marketing, waar het heel gebruikelijk is dat bedrijven in dezelfde sector

persoonsgegevens uitwisselen, situaties kunnen ontstaan waarbij het bedrijf dat persoonsgegevens verstrekt aan een andere code voor gegevensbescherming is onderworpen dan het bedrijf dat ze ontvangt. Dit leidt tot onzekerheid over de toe te passen regels en kan ook het onderzoek naar en de regeling van klachten van betrokkenen in verband met hun gegevens bemoeilijken.

Beoordeling van zelfregulering: de juiste invalshoek

Gezien het grote aantal instrumenten dat onder het begrip *zelfregulering* valt, is het duidelijk dat er een onderscheid moet worden gemaakt tussen de verschillende vormen van zelfregulering met betrekking tot de reële impact die zij hebben op het niveau van gegevensbescherming bij doorgifte naar een derde land.

Elke verzameling van regels voor de bescherming van gegevens (of zij nu als zelfregulering dan wel als regulering wordt geclassificeerd) moet in de eerste plaats worden beoordeeld op basis van de krachtlijnen die zijn uitgetekend in hoofdstuk 1 van dit document. Fundamenteel bij deze benadering is dat niet alleen de inhoud van het instrument (dat een aantal basisbeginselen moet omvatten) onder de loep wordt genomen, maar ook de doeltreffendheid waarmee het:

- een goede algemene naleving garandeert;
- de betrokkenen ondersteuning biedt;
- en, wat van cruciaal belang is, passende verhaalmogelijkheden biedt (inclusief zonodig schadeloosstelling).

Beoordeling van de inhoud van een zelfreguleringsinstrument

Dit is een relatief gemakkelijke opdracht. Zaak is dat het instrument beantwoordt aan de noodzakelijke 'inhoudelijke beginselen' van hoofstuk 1. Het gaat hier om een objectieve beoordeling van de inhoud van de code en niet van de wijze waarop zij werd opgesteld. Dat een sector of beroepsgroep bij het vaststellen van die inhoud zelf de grootste rol heeft gespeeld, is als zodanig niet relevant, hoewel de kans uiteraard groter is dat de vereiste basisbeginselen inzake gegevensbescherming nadrukkelijker in de code aanwezig zullen zijn als met de standpunten van de betrokkenen en de consumentenverenigingen rekening is gehouden.
Een cruciale factor is de transparantie van de code. De voorschriften moeten duidelijk verwoord zijn en aan de hand van concrete voorbeelden worden geïllustreerd.
Bovendien moet worden verboden dat gegevens worden verstrekt aan bedrijven die niet onder de code vallen, tenzij anderszins in een adequate beveiliging is voorzien.

Beoordeling van de doeltreffendheid van een zelfreguleringsinstrument

Moeilijker wordt het als een bepaalde code of een specifiek instrument voor zelfregulering op zijn doeltreffendheid moet worden beoordeeld, omdat dit inzicht vereist in de manier waarop en de middelen waarmee de naleving van de code wordt gegarandeerd en overtredingen van de code worden aangepakt. Een code voor zelfregulering kan niet als passende bescherming worden aangemerkt als zij niet aan alle drie functionele criteria inzake een passend beschermingsniveau voldoet.

Goede naleving

Een code voor een sector of beroepsgroep wordt in de regel opgesteld door een voor die sector of beroepsgroep representatieve organisatie, op wier leden zij dan van toepassing wordt. De naleving van een code hangt veelal af van de mate waarin deze leden weet hebben van het bestaan en de inhoud van de code, van de stappen die worden ondernomen om haar transparant te maken voor de consument - zodat ook de marktkrachten effectief kunnen bijdragen tot de naleving ervan -, van het bestaan van externe controlesystemen (zoals een verplichte audit van de naleving van de code op gezette tijden) en, misschien wel het belangrijkste, van het type en de handhaving van de sancties om de naleving van de code af te dwingen.
Deze overwegingen werpen de volgende belangrijke vragen op:

- hoe zorgt de representatieve organisatie ervoor dat haar leden weten dat de code bestaat?
- verlangt de representatieve organisatie van haar leden het bewijs dat zij de code toepassen? Hoe vaak?
- wordt dit bewijs door het lid zelf geleverd of door een externe persoon/instantie (zoals een erkend controleur)?
- stelt de representatieve organisatie een onderzoek in als haar een inbreuk op de code wordt gemeld of het vermoeden daarvan bestaat?
- is naleving van de code een voorwaarde om lid te worden van de representatieve organisatie of heeft de code een zuiver "vrijblijvend" karakter?
- over welke disciplinaire maatregelen beschikt de representatieve organisatie om een bewezen inbreuk door een lid te bestraffen (uitsluiting of andere)?
- kan een persoon of bedrijf in een beroep of sector actief blijven, ook na uitsluiting uit de desbetreffende representatieve organisatie?
- is de naleving van de code ook op andere wijze afdwingbaar, bijvoorbeeld langs juridische weg of via arbitrage? In sommige landen hebben beroepscodes kracht van wet. In bepaalde omstandigheden zou de naleving van een code voor een specifieke sector ook op basis van een algemene wet inzake eerlijke handelspraktijken of zelfs inzake mededinging kunnen worden afgedwongen.

Bij de verschillende soorten sancties die worden toegepast, is het belangrijk een onderscheid te maken tussen "remediërende" sancties, waarbij van een nalatige houder alleen maar wordt geëist dat hij zich aan de code conformeert, en sancties die de niet-naleving van de code door de houder daadwerkelijk bestraffen. Het blijkt dat alleen deze "bestraffende" sancties het toekomstige gedrag van een voor de verwerking verantwoordelijke kunnen beïnvloeden, omdat zij hem in zekere mate stimuleren om de code te blijven naleven.

Daarom vormt het onbreken van krachtige ontmoedigende en bestraffende sancties een grote handicap voor een code. Het is immers niet duidelijk hoe zonder dergelijke sancties kan worden gegarandeerd dat de regels in het algemeen degelijk worden nageleefd, tenzij er een rigoureus extern controlesysteem wordt opgezet (zoals een openbare of particuliere instantie die bij niet-naleving van de code de bevoegdheid heeft om op te treden, of een verplichte externe audit op gezette tijden).

Bijstand aan de betrokkene

Een basisvoorwaarde voor een passend en doeltreffend gegevensbeschermingssysteem is dat een betrokkene die een probleem heeft in verband met zijn persoonsgegevens, niet aan zijn lot wordt overgelaten, maar op een of andere vorm van geïnstitutionaliseerde ondersteuning kan rekenen. Deze ondersteunende instantie moet idealiter onpartijdig en onafhankelijk zijn en over de nodige bevoegdheden beschikken om alle mogelijke klachten van betrokkenen te onderzoeken. Wat zelfregulering betreft, rijzen hier de volgende vragen:

- bestaat er een systeem om klachten van betrokkenen te onderzoeken?
- hoe worden de betrokkenen op de hoogte gesteld van het bestaan van een dergelijk systeem en van de uitspraken met betrekking tot individuele klachten?
- zijn er kosten voor de betrokkene?
- wie voert het onderzoek uit? Beschikt deze instantie over de nodige bevoegdheden?
- wie oordeelt over vermeende inbreuken op de code? Is deze instantie onafhankelijk en onpartijdig?

De onpartijdigheid van de arbiter of scheidsrechter bij een vermeende inbreuk op een code is een cruciaal element. Het is vanzelfsprekend dat deze onafhankelijk moet zijn van degene die voor de verwerking verantwoordelijk is. Onafhankelijkheid op zich volstaat echter niet om onpartijdigheid te garanderen. In het ideale geval behoort de arbiter ook tot een andere beroepsgroep of sector dan de voor de verwerking verantwoordelijke die van inbreuk op de code wordt beschuldigd, om alle belangenverstrengeling te vermijden. Is dit niet mogelijk, dan kan de neutraliteit worden verzekerd door in het arbitragecollege niet alleen vertegenwoordigers van de sector maar ook (een gelijk aantal) vertegenwoordigers van de consument op te nemen.

Passende schadeloosstelling

Als blijkt dat de zelfreguleringscode niet is gerespecteerd, moet de benadeelde verhaal kunnen zoeken. Op die manier moet het probleem worden verholpen (bv. verbetering of verwijdering van onjuiste gegevens of stopzetting van onrechtmatige verwerking van gegevens) en ervoor worden gezorgd dat de betrokkene, als hij schade heeft geleden, op passende wijze wordt vergoed. Er zij op gewezen dat “schade” in de zin van de richtlijn betreffende gegevensbescherming niet alleen lichamelijke en financiële schade omvat, maar ook alle psychologische of morele schade die de betrokkene heeft geleden (in het Amerikaanse en Britse recht omschreven als “distress” of leed).

Vele van de hierboven (“*Goede naleving*”) vermelde vragen over sancties zijn ook hier relevant. Er werd al betoogd dat sancties een dubbele functie hebben, namelijk een bestraffende (om zo de nalatige houder én ook anderen te stimuleren de regels te respecteren) en een remediërende (die een inbreuk ongedaan maakt). Hier gaat het in eerste instantie om de tweede functie, waarbij de volgende bijkomende vragen rijzen:

- kan worden nagegaan of een lid dat handelt in strijd met de code, zich heeft geconformeerd en de misstand heeft rechtgezet?

- kunnen individuele personen zich voor schadeloosstelling op de code beroepen, en zo ja, hoe?
- staat inbreuk op de code gelijk met niet-naleving van een overeenkomst, is de code onder het publiekrecht afdwingbaar (bv. op basis van de regels voor de bescherming van de consument of de regels inzake oneerlijke mededinging) en kan de bevoegde (scheids)rechter op basis hiervan schadevergoeding toekennen?

Conclusies

- Zelfregulering moet worden beoordeeld aan de hand van de objectieve en functionele criteria in hoofdstuk 1.
- Een zelfreguleringsinstrument kan pas als een volwaardige component van een systeem voor een "passend beschermingsniveau" worden beschouwd, als het bindend is voor alle leden aan wie persoonsgegevens worden doorgegeven, en voorziet in adequate beveiliging bij verstrekking van gegevens aan niet-leden.
- Het instrument moet transparant zijn en de basisbeginselen voor gegevensbescherming in acht nemen.
- Het instrument moet dusdanig zijn opgezet dat het in het algemeen een goede naleving van de regels garandeert. Dit is bijvoorbeeld mogelijk via een systeem van afschrikkende maatregelen en sancties of met verplichte externe audits.
- Het instrument moet ondersteuning bieden aan betrokkenen die een probleem hebben in verband met de verwerking van hun persoonsgegevens. Daarom moet een laagdrempelig, onpartijdig en onafhankelijk orgaan worden gecreëerd waar betrokkenen een klacht kunnen indienen en waar uitspraak wordt gedaan over inbreuken op de code.
- Het instrument moet bij niet-naleving van de code in passende verhaalmogelijkheden voorzien, zodat de misstand kan worden rechtgezet en zonodig schadevergoeding kan worden toegekend.

HOOFDSTUK 4: DE ROL VAN CONTRACTUELE BEPALINGEN

1. Inleiding

Overeenkomstig artikel 25, lid 1, van de richtlijn gegevensbescherming (95/46/EG) mogen persoonsgegevens in beginsel alleen naar een derde land worden doorgegeven indien dat derde land een passend beschermingsniveau waarborgt. Doel van dit hoofdstuk is de door artikel 26, lid 2, geboden mogelijkheid van afwijkingen van het in artikel 25 genoemde "passende bescherming"-beginsel te onderzoeken. Krachtens deze bepaling kan een lidstaat toestemming geven voor een doorgifte of een categorie doorgiften van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt, "indien de voor de verwerking verantwoordelijke voldoende waarborgen biedt ten aanzien van de bescherming van de persoonlijke levenssfeer, de fundamentele rechten en vrijheden van personen, alsmede ten aanzien van de uitoefening van de daaraan verbonden rechten". Verder wordt bepaald dat "deze waarborgen met name kunnen voortvloeien uit passende contractuele bepalingen". Artikel 26, lid 4, verleent de Commissie tevens de bevoegdheid om volgens de in artikel 31 beschreven procedure te besluiten dat bepaalde modelcontractbepalingen voldoende waarborgen bieden overeenkomstig artikel 26, lid 2.

Het idee om contracten te gebruiken als een middel om de internationale doorgifte van persoonsgegevens te reguleren, is uiteraard geen uitvinding van de richtlijn. Al in 1992 hebben de Raad van Europa, de Internationale Kamer van Koophandel en de Europese Commissie gezamenlijk het initiatief genomen voor een studie over dit onderwerp[7]. Recenter heeft een toenemend aantal deskundigen en commentatoren, wellicht geïnspireerd door de uitdrukkelijke verwijzing in de richtlijn, in studies en artikelen commentaar geleverd op het gebruik van contracten. Contracten zijn steeds ook gebruikt in de 'echte wereld' voor het oplossen van problemen inzake gegevensbescherming die voortvloeien uit de uitvoer van persoonsgegevens uit bepaalde EU-lidstaten. In Frankrijk wordt er sinds eind jaren tachtig op grote schaal gebruik van gemaakt. In Duitsland heeft het recente voorbeeld van de 'Bahncard'-zaak, waarbij de Citibank betrokken was, nogal wat publiciteit gekregen[8].

2. Het gebruik van contracten als grondslag voor intracommunautaire gegevensstromen

Alvorens na te gaan aan welke voorwaarden contractuele bepalingen in het kader van gegevensstromen naar derde landen moeten voldoen, is het belangrijk het verschil tussen een situatie waarbij derde landen betrokken zijn en een intracommunautaire situatie duidelijk te maken. In het laatstgenoemde geval is een overeenkomst een instrument om de verdeling van de aansprakelijkheid inzake gegevensbescherming vast te stellen en te regelen wanneer meer dan een persoon of instantie betrokken is bij de

---

[7] "Modelcontract om een gelijkwaardige gegevensbescherming te waarborgen in het kader van grensoverschrijdende gegevensstromen, met toelichting", een gezamenlijk door de Raad van Europa, de Commissie van de Europese Gemeenschappen en de Internationale Kamer van Koophandel uitgevoerde studie, Straatsburg, 2 november 1992.

[8] Zie de uiteenzetting van Alexander Dix over deze zaak op de *International Data Protection and Privacy Commissioners' Conference*, september 1996, Ottawa.

verwerking van de gegevens in kwestie. Volgens de richtlijn moet één persoon of instantie, namelijk de "voor de verwerking verantwoordelijke", de hoofdaansprakelijkheid voor de naleving van de essentiële beginselen inzake gegevensbescherming voor zijn rekening nemen. De tweede persoon of instantie, de "verwerker", is alleen verantwoordelijk voor de beveiliging van de gegevens. Een persoon of instantie wordt geacht de "voor de verwerking verantwoordelijke" te zijn indien hij/zij beslissingsrecht heeft over doel en wijze van gegevensverwerking, terwijl de "verwerker" gewoon de persoon of instantie is die de gegevensverwerking materieel uitvoert. De verhouding tussen beide wordt geregeld door artikel 17, lid 3, van de richtlijn, dat bepaalt:

"De uitvoering van verwerkingen door een verwerker moet worden geregeld in een overeenkomst of een rechtsakte die de verwerker bindt jegens de voor de verwerking verantwoordelijke en waarin met name wordt bepaald dat
- de verwerker slechts handelt in opdracht van de voor de verwerking verantwoordelijke;
- de in lid 1 bedoelde verplichtingen (de materiële bepalingen inzake gegevensbeveiliging), zoals gedefinieerd door de wetgeving van de lidstaat waarin de verwerker is gevestigd, eveneens op deze persoon rusten".

Dit is een uitwerking van het in artikel 16 neergelegde algemene principe dat eenieder die handelt onder het gezag van de voor de verwerking verantwoordelijke, met inbegrip van de verwerker zelf, persoonsgegevens uitsluitend in opdracht van de voor de verwerking verantwoordelijke mag verwerken (behoudens op grond van wettelijke verplichtingen).
Wanneer persoonsgegevens naar derde landen worden doorgegeven, zal daarbij normaliter eveneens meer dan een partij betrokken zijn. Hier draait het om de verhouding tussen de persoon of instantie die de gegevens doorgeeft (de "overdrager") en de persoon of instantie in het derde land die de gegevens in ontvangst neemt (de "ontvanger"). Ook in dit kader moet de overeenkomst erop gericht zijn te regelen hoe de aansprakelijkheid voor de inachtneming van de gegevensbescherming over de beide partijen wordt verdeeld. De overeenkomst moet echter meer doen: het moet de betrokkene bijkomende waarborgen bieden die noodzakelijk zijn omdat de ontvanger in het derde land niet onderworpen is aan een afdwingbaar geheel van voorschriften inzake gegevensbescherming die een passend beschermingsniveau bieden.

3. Doel van een contractuele oplossing

In het kader van de doorgifte naar derde landen vormt een overeenkomst derhalve een middel aan de hand waarvan de verantwoordelijke voor de verwerking passende garanties kan bieden wanneer gegevens buiten de Gemeenschap (en dus buiten de bescherming van de richtlijn en het hele kader van het Gemeenschapsrecht[9]) worden doorgegeven naar een derde land waar het algemene beschermingsniveau niet voldoende hoog is. Wil een contractuele bepaling deze functie kunnen vervullen, dan moet zij in afdoende mate een tegenwicht bieden voor het ontbreken van een algemeen

[9] De uitoefening door een persoon van zijn rechten op het gebied van gegevensbescherming wordt in de Gemeenschap vergemakkelijkt door het algemeen juridisch kader, bijvoorbeeld het verdrag van Straatsburg (1977) inzake het verzenden van verzoeken om rechtsbijstand.

passend beschermingsniveau door in elk concreet geval bescherming te bieden op de belangrijkste punten waaraan in dat geval iets schort.

4. De specifieke voorwaarden voor een contractuele oplossing

Het uitgangspunt voor de interpretatie van de uitdrukking 'voldoende waarborgen', zoals die in artikel 26, lid 2, is gebruikt, is het begrip 'passend beschermingsniveau', dat reeds in Hoofdstuk 1 is toegelicht. Dit is gebaseerd op een aantal grondbeginselen inzake gegevensbescherming, waaraan bepaalde voorwaarden zijn verbonden om de doeltreffendheid ervan te garanderen.

(i) De materiële voorschriften inzake gegevensbescherming

De eerste voorwaarde voor een contractuele oplossing is derhalve dat deze aan de partijen bij de doorgifte de verplichting moet opleggen om te waarborgen dat de in Hoofdstuk 1 opgesomde basisbeginselen inzake gegevensbescherming in hun geheel van toepassing zijn op de verwerking van de naar een derde land doorgegeven gegevens. Deze basisbeginselen zijn:

- het specificiteitsbeginsel
- het kwaliteits- en evenredigheidsbeginsel
- het transparantiebeginsel
- het beveiligingsbeginsel
- het recht van toegang, rectificatie en verzet
- beperking van doorgifte naar anderen die geen partij zijn bij het contract[10].

Voorts moeten in bepaalde situaties bijkomende beginselen worden toegepast betreffende gevoelige gegevens, direct marketing en geautomatiseerde individuele besluiten.

De overeenkomst moet in detail aangeven op welke wijze de ontvanger van de doorgegeven gegevens deze beginselen (d.w.z. doel, gegevenscategorieën, duur van bewaring, beveiligingsmaatregelen enz. moeten worden aangegeven) dient toe te passen. In andere omstandigheden, bijvoorbeeld wanneer de bescherming in een derde land voortvloeit uit een algemene gegevensbeschermingswet die vergelijkbaar is met de richtlijn, zullen allicht andere regelingen gelden die verduidelijken hoe de voorschriften inzake gegevensbescherming in de praktijk functioneren (gedragscodes, kennisgeving, adviesfunctie van de toezichthoudende autoriteit). In een contractuele context is dit niet het geval. Detailgegevens zijn dan ook absoluut noodzakelijk wanneer de doorgifte op basis van een overeenkomst geschiedt.

(ii) De materiële voorschriften doeltreffend maken

[10] Verdere doorgiften van de persoonsgegevens van de ontvanger naar een derde mag niet worden toegestaan, tenzij een methode wordt gevonden om deze derde er contractueel toe te verplichten dezelfde waarborgen inzake gegevensbescherming te bieden.

In Hoofdstuk 1 worden drie criteria vermeld waaraan de doeltreffendheid van een systeem van gegevensbescherming dient te worden getoetst. Deze criteria zijn de mate waarin het systeem erin slaagt:

- een **goede naleving** van de voorschriften te verzekeren;
- **bijstand** te verlenen **aan de betrokkenen** bij de uitoefening van hun rechten;
- een **passende schadeloosstelling** te verzekeren aan de ten gevolge van schending van de voorschriften gelaedeerde partij.

Dezelfde criteria moeten gelden bij de beoordeling van de doeltreffendheid van een contractuele oplossing. Dit is een zware, maar niet onmogelijke opgave. Het komt er op aan middelen te vinden die het ontbreken van algemene bekendheid en handhavingsmaatregelen kunnen compenseren en die bijstand en uiteindelijk schadeloosstelling kunnen verzekeren aan een betrokkene die geen partij is bij het contract.

Elk van deze vraagstukken moet grondig worden onderzocht. Voor het gemak van de analyse worden zij in omgekeerde volgorde behandeld.

Verzekeren van schadeloosstelling aan een betrokkene

Een betrokkene een verhaalmogelijkheid bieden (d.w.z. een recht om een onafhankelijke scheidsrechter uitspraak te laten doen over een klacht en in voorkomende gevallen schadeloosstelling te verkrijgen) door middel van een overeenkomst tussen een 'overdrager' van gegevens en een 'ontvanger' is geen eenvoudige zaak. Veel zal afhangen van de aard van het contractenrecht dat gekozen is als de nationale wetgeving waaronder de overeenkomst valt. Naar verwachting zal de toepasselijke wet over het algemeen die zijn van de lidstaat waarin de partij die de gegevens doorgeeft, is gevestigd. Het contractenrecht van sommige lidstaten maakt het mogelijk aan derden rechten te verlenen, maar in andere lidstaten is dit niet het geval.

In de regel zal de rechtszekerheid voor de betrokkene echter toenemen naarmate de vrijheid van de ontvanger om doel, middelen en voorwaarden waaronder hij de doorgegeven gegevens verwerkt, meer wordt beperkt. Aangezien het hier gaat om situaties waarin onvoldoende algemene bescherming voorhanden is, verdient het de voorkeur dat in de overeenkomst wordt bepaald dat de ontvanger ten aanzien van de doorgegeven gegevens of de wijze waarop deze vervolgens worden verwerkt, geen zelfstandige beslissingsvrijheid heeft. De ontvanger mag uitsluitend volgens de instructies van de overdrager handelen, en ofschoon de gegevens materieel buiten de EU zijn gebracht, blijft het beslissingsrecht over de gegevens berusten bij de in de Gemeenschap gevestigde persoon of instantie die de gegevens heeft doorgegeven. De overdrager blijft aldus de voor de verwerking verantwoordelijke, terwijl de ontvanger niet meer dan een in onderaanneming werkende verwerker is. Aangezien in dergelijke gevallen de zeggenschap over de gegevens wordt uitgeoefend door een persoon of instantie die in een EU-lidstaat is gevestigd, blijft het recht van de betrokken lidstaat van toepassing op de verwerking die in het derde land plaatsvindt[11], en blijft de overdrager de voor de verwerking verantwoordelijke overeenkomstig het recht van die

[11] Op grond van artikel 4, lid 1, onder a), van Richtlijn 95/46/EG.

lidstaat aansprakelijk voor alle eventuele schade die het gevolg zou zijn van een onrechtmatige verwerking[12].

Dit soort regeling is vergelijkbaar met die welke is toegepast in de "Interterritoriale overeenkomst", waarmee de eerdergenoemde zaak Citibank 'Bahncard' werd opgelost. Daarbij werden in de overeenkomst in detail de regels voor gegevensverwerking vastgelegd, met name die inzake gegevensbeveiliging, en werd elk ander gebruik van de gegevens door de ontvanger uitgesloten. De Duitse wet werd van toepassing verklaard op gegevensverwerking in het derde land en aldus werd de betrokkenen een verhaalmogelijkheid gegarandeerd[13].

Er zullen zich uiteraard gevallen voordoen waarin dit soort oplossing niet bruikbaar is. Het is zeer wel mogelijk dat de ontvanger niet zonder meer een gegevensverwerkingsdienst verleent aan de in de EU gevestigde verantwoordelijke voor de gegevens. Zo kan de ontvanger bijvoorbeeld de gegevens hebben gekocht of gehuurd om ze voor eigen rekening en eigen doeleinden te gebruiken. Onder die omstandigheden moet de ontvanger een zekere vrijheid hebben om de gegevens naar eigen inzicht te gebruiken en zo in feite zelf een 'voor de verwerking verantwoordelijke' worden.

In dit soort gevallen kan niet worden teruggegrepen op de doorlopende automatische toepasselijkheid van het recht van een lidstaat en op de doorlopende aansprakelijkheid van de overdrager van de gegevens voor eventuele schade. Andere, complexere regelingen moeten worden ontwikkeld om de betrokkene een passende verhaalmogelijkheid te bieden. Zoals gezegd, bieden sommige rechtsstelsels derden de mogelijkheid om aan een overeenkomst rechten te ontlenen; hiervan zou gebruik kunnen worden gemaakt om de betrokkenen rechten te verlenen in het kader van een open, gepubliceerde overeenkomst tussen overdrager en ontvanger. De positie van de betrokkene zou verder kunnen worden versterkt indien de partijen zich, als een onderdeel van het contract, zouden verbinden tot een soort van bindende arbitrage in gevallen waarin een betrokkene betwist dat de overeenkomst wordt nageleefd. Sommige sectorale zelfreguleringscodes bevatten dergelijke arbitrageclausules en het gebruik van contracten in combinatie met dergelijke codes zou een mogelijkheid kunnen zijn.

Een andere mogelijkheid is dat degene die de gegevens doorgeeft, wellicht op het ogenblik waarop hij de gegevens in eerste instantie van de betrokkene verkrijgt, met de betrokkene een afzonderlijke overeenkomst aangaat waarin wordt bepaald dat hij (de overdrager) aansprakelijk blijft voor elke schade en elk nadeel dat het gevolg zou zijn van het feit dat de ontvanger na een gegevensdoorgifte de overeengekomen basisbeginselen inzake gegevensbescherming niet in acht neemt. Op die manier beschikt de betrokkene over een verhaalmogelijkheid tegen de overdrager voor overtredingen die door de ontvanger worden begaan. Het is dan aan de overdrager om eventuele

---

12 Zie artikel 23 van Richtlijn 95/46/EG.

13 Dit ondanks het feit dat de wet, omdat deze zaak onder een wet viel die aan de richtlijn voorafging, niet automatisch van toepassing was op elke verwerking die onder de verantwoordelijkheid van een in Duitsland gevestigde persoon of instantie viel. De verhaalmogelijkheid van de betrokkene was in dit geval dan ook gebaseerd op de mogelijkheid die het Duitse contractenrecht biedt om rechten voor derden in het leven te roepen.

schade die hij aan de betrokkene heeft moeten betalen, vergoed te krijgen door middel van een rechtsvordering wegens contractbreuk tegen de ontvanger.

Een dergelijke ingewikkelde "drietraps"-oplossing is wellicht gemakkelijker toe te passen dan het op het eerste gezicht lijkt. De overeenkomst met de betrokkene zou een onderdeel kunnen worden van de standaardvoorwaarden die bijvoorbeeld een bank of reisbureau in het kader van de dienstverlening aan hun klanten hanteren. Dit heeft het voordeel van transparantie: de betrokkene is volledig op de hoogte van zijn rechten.

Tenslotte zou, als een alternatief voor een overeenkomst met de betrokkene, de mogelijkheid kunnen worden overwogen dat een lidstaat bij wet aan verantwoordelijken voor gegevens die deze naar landen buiten de Gemeenschap overdragen, een doorlopende aansprakelijkheid oplegt voor schade die voortvloeit uit gedragingen van de ontvanger van de doorgegeven gegevens.

Verlenen van bijstand aan de betrokkenen

Een van de belangrijkste moeilijkheden voor betrokkenen wier gegevens naar een derde land met een ander rechtsstelsel worden doorgegeven, is dat zij er niet in slagen de eigenlijke oorzaak te ontdekken van het specifieke probleem dat zij ondervinden, en dat zij derhalve niet kunnen beoordelen of de voorschriften inzake gegevensbescherming naar behoren in acht zijn genomen dan wel of er sprake is van juridisch aanvechtbare handelingen[14]. Een passend beschermingsniveau veronderstelt dan ook dat er enig institutioneel mechanisme voorhanden is dat een onafhankelijk onderzoek van klachten mogelijk maakt.

De controlerende en onderzoeksbevoegdheid van de toezichthoudende autoriteit van een lidstaat is beperkt tot gegevensverwerking die plaatsvindt op het grondgebied van de lidstaat[15]. Wanneer gegevens worden doorgegeven naar een andere lidstaat, zorgt een systeem van wederzijdse bijstand tussen de toezichthoudende autoriteiten ervoor dat een klacht van een betrokkene in de eerste lidstaat naar behoren wordt onderzocht. Wanneer de doorgifte plaatsvindt naar een derde land, zal een dergelijke waarborg in de meeste gevallen niet voorhanden zijn. De vraag is dan ook wat voor compenserende regeling mogelijk is in het kader van een gegevensdoorgifte op basis van een contract.

Eén mogelijkheid zou zijn om gewoon voor te schrijven dat in de overeenkomst een bepaling moet worden opgenomen die aan de toezichthoudende autoriteit van de lidstaat waar de overdrager van de gegevens gevestigd is het recht verleent om controle uit te oefenen op de verwerking die door de verwerker in het derde land wordt uitgevoerd. Deze controle zou in de praktijk kunnen worden uitgeoefend door een door de toezichthoudende autoriteit aangestelde tussenpersoon (bijvoorbeeld een gespecialiseerd auditbureau), indien dit als een geschikte werkwijze wordt beschouwd. Een moeilijkheid bij deze aanpak is evenwel dat de toezichthoudende autoriteit over

[14] Zelfs indien de betrokkene aan een overeenkomst rechten ontleent, zal hij vaak niet kunnen beoordelen of er sprake is van contractbreuk, en zo ja, door wie. Een onderzoekprocedure buiten een formeel proces voor de civiele rechter is derhalve noodzakelijk.

[15] Zie artikel 28, lid 1, van Richtlijn 95/46/EG.

het algemeen[16] geen partij is bij de overeenkomst en zich er dus in sommige rechtsstelsels wellicht niet op zal kunnen beroepen om toegang te krijgen. Een andere mogelijkheid zou zijn dat de ontvanger in het derde land rechtstreeks tegenover de toezichthoudende autoriteit van de betrokken lidstaat de verplichting aangaat, aan deze autoriteit of een door haar aangestelde tussenpersoon toegang te verlenen indien wordt vermoed dat de beginselen inzake gegevensbescherming niet zijn nageleefd. De aangegane verbintenis zou tevens de verplichting kunnen omvatten dat de partijen bij de gegevensdoorgifte de toezichthoudende autoriteit in kennis stellen van elke klacht die zij van een betrokkene ontvangen. In het kader van een dergelijke regeling zou een dergelijke verbintenis moeten worden aangegaan voordat toestemming wordt verleend voor de doorgifte van gegevens.

Voor welke oplossing ook wordt gekozen, het blijft hoe dan ook twijfelachtig of het voor een toezichthoudende autoriteit van een EU-lidstaat uit het oogpunt van middelen wenselijk, praktisch of zelfs haalbaar is de verantwoordelijkheid op zich te nemen voor onderzoek naar en controle op gegevensverwerking die in een derde land plaatsvindt.

Verzekeren van een goede naleving van de voorschriften

Zelfs zonder dat een betrokkene met een specifieke klacht of moeilijkheid wordt geconfronteerd, moet erop vertrouwd worden dat de contractpartijen zich daadwerkelijk aan de contractuele bepalingen houden. Het probleem met de contractuele oplossing is dat het moeilijk is aan inbreuken sancties te verbinden die een voldoende afschrikkend effect hebben om dit vertrouwen te waarborgen. Zelfs wanneer de daadwerkelijke controle op de gegevens nog steeds binnen de Gemeenschap wordt uitgeoefend, is het wellicht niet mogelijk de ontvanger van de doorgegeven gegevens rechtstreeks te bestraffen indien hij gegevens in strijd met de overeenkomst zou verwerken. De aansprakelijkheid zou in dat geval berusten bij de in de Gemeenschap gevestigde overdrager van de gegevens, die op zijn beurt moet zien eventuele schade vergoed te krijgen door middel van een afzonderlijke rechtsvordering tegen de ontvanger. Die indirecte aansprakelijkheid is wellicht niet voldoende om de ontvanger aan te moedigen om alle details van de overeenkomst na te leven.

Bijgevolg zal een contractuele oplossing waarschijnlijk in de meeste gevallen op zijn minst moeten worden aangevuld met de mogelijkheid van enige vorm van externe controle op de verwerkingsactiviteiten van de ontvanger, bijvoorbeeld een audit door een normalisatie-instelling of door een gespecialiseerd auditbureau.

5. Het probleem van dwingende rechtsbepalingen

Een specifieke moeilijkheid met de contractuele aanpak is dat de wetgeving van het derde land bepalingen kan behelzen die de ontvanger van doorgegeven gegevens er in bepaalde omstandigheden toe verplichten persoonsgegevens vrij te geven aan de staat (bijvoorbeeld de politie, het gerecht of de belastingdiensten), en dat dergelijke wettelijke voorschriften voorrang kunnen hebben op elke overeenkomst waarbij de

[16] De Franse delegatie kon zich situaties voorstellen waarin de toezichthoudende autoriteit partij was bij het contract.

verwerker partij is[17]. Voor verwerkers in de Gemeenschap wordt deze mogelijkheid aangehaald in artikel 16 van de richtlijn, dat de verwerkers voorschrijft gegevens slechts in opdracht van de voor de verwerking verantwoordelijke te verwerken, *"behoudens op grond van wettelijke verplichtingen"*. Overeenkomstig de richtlijn moet een dergelijk vrijgeven (dat per definitie voor een ander doel is dan dat waarvoor de gegevens werden verzameld) worden beperkt tot hetgeen in democratische samenlevingen noodzakelijk is om een van de in artikel 13, lid 1, van de richtlijn genoemde redenen van openbare orde (zie voetnoot 2). Artikel 6 van het Verdrag van Amsterdam waarborgt eveneens de inachtneming van de grondrechten die in het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden zijn neergelegd. In derde landen zijn dergelijke beperkingen van de mogelijkheid van de staat om van ondernemingen en andere organisaties die op hun grondgebied werkzaam zijn te verlangen dat zij persoonsgegevens verstrekken, niet altijd voorhanden.

Er is geen eenvoudige manier om deze moeilijkheid op te lossen. Het is de bedoeling gewoon de beperkingen van de contractuele aanpak aan te tonen. In sommige gevallen is een overeenkomst een te broos instrument om passende waarborgen inzake gegevensbescherming te bieden en doorgiften naar bepaalde landen mogen niet worden toegestaan.

6. Praktische overwegingen in verband met het gebruik van contracten

De voorgaande analyse heeft aangetoond dat elke contractuele oplossing in detail moet worden uitgewerkt en nauwkeurig moet worden afgestemd op de specifieke gegevensdoorgifte. Deze behoefte aan details inzake het precieze doel en de voorwaarden waaronder de doorgegeven gegevens moeten worden verwerkt, sluit de mogelijkheid van het opstellen van een modelcontract niet uit, maar houdt wel in dat elke overeenkomst die op dit modelcontract gebaseerd is, verder aangevuld wordt op een manier die beantwoordt aan de specifieke omstandigheden van het geval.

Uit de analyse is tevens gebleken dat zich bij het onderzoek naar inbreuken op de overeenkomst bepaalde praktische moeilijkheden voordoen wanneer de verwerking buiten de EU plaatsvindt en wanneer er in het betrokken derde land geen toezichthoudende autoriteit bestaat. Uit deze beide overwegingen kan worden afgeleid dat een contractuele aanpak in sommige gevallen een geschikte oplossing zal zijn, en dat het in andere gevallen onmogelijk zal zijn om langs contractuele weg de vereiste 'passende bescherming' te waarborgen.

De noodzaak om een overeenkomst nauwkeurig af te stemmen op de specifieke kenmerken van de doorgifte betekent dat een overeenkomst vooral geschikt is in situaties waarin gegevensdoorgiften gelijksoortig en repetitief zijn. Gezien de moeilijkheden in verband met toezicht is een contractuele oplossing wellicht het meest doeltreffend wanneer de contractpartijen grote ondernemingen of organisaties zijn die

[17] De omvang van de bevoegdheid van de staat om het vrijgeven van informatie te verlangen, is ook een element dat in aanmerking wordt genomen bij de algemene beoordeling van het passende beschermingsniveau in een derde land.

reeds onderworpen zijn aan controle en regulering door de overheid[18]. Grote internationale netwerken, zoals die welke worden gebruikt voor kredietkaarttransacties en vliegticketreservaties, vertonen deze beide kenmerken en lenen zich dus bij uitstek voor het gebruik van contracten. In deze gevallen zouden zij zelfs kunnen worden aangevuld met multilaterale verdragen, die een grotere rechtszekerheid bieden.

Ook wanneer de partijen bij de overeenkomst dochterondernemingen of afdelingen van hetzelfde concern zijn, zal de mogelijkheid om inbreuken op de overeenkomst te onderzoeken waarschijnlijk veel groter zijn, gezien de sterke band tussen de ontvanger in het derde land en de in de Gemeenschap gevestigde overdrager. Doorgiften binnen dezelfde bedrijvengroep zijn derhalve een ander terrein waarop er duidelijk mogelijkheden zijn om doeltreffende contractuele oplossingen te ontwikkelen.

Belangrijkste conclusies en aanbevelingen

- Contracten worden binnen de Gemeenschap gebruikt als een middel om de verdeling van de aansprakelijkheid inzake inachtneming van de gegevensbescherming tussen de voor de voor de verwerking verantwoordelijke en een in opdracht werkende verwerker nauwkeurig te bepalen. Wanneer een overeenkomst wordt gebruikt met betrekking tot gegevensstromen naar derde landen, moet het veel meer doen: het moet de betrokkene aanvullende garanties bieden, die noodzakelijk zijn ten gevolge van het feit dat de ontvanger in het derde land niet onderworpen is aan een afdwingbaar geheel van gegevensbeschermingvoorschriften die een passende mate van bescherming bieden.
- De toereikendheid van de waarborgen die door een contractuele oplossing worden geboden, wordt beoordeeld op dezelfde grondslag als die waarop het algemene beschermingsniveau in een derde land wordt beoordeeld. Een contractuele oplossing moet alle basisbeginselen inzake gegevensbescherming omvatten en voorzien in middelen aan de hand waarvan deze beginselen kunnen worden afgedwongen.
- In de overeenkomst moet een gedetailleerde beschrijving worden gegeven van het doel, de middelen en de voorwaarden waaronder de doorgegeven gegevens moeten worden verwerkt, alsmede van de wijze waarop de basisbeginselen inzake gegevensbescherming in praktijk moeten worden gebracht. Een grotere rechtszekerheid wordt geboden door contracten die de mogelijkheid van de ontvanger beperken om de gegevens zelfstandig voor eigen rekening te verwerken. De overeenkomst dient derhalve zoveel mogelijk te worden gebruikt als een middel waarmee de overdrager van de gegevens zich het beslissingsrecht over de in het derde land uitgevoerde gegevensverwerking voorbehoudt.
- Wanneer de ontvanger enige zelfstandigheid heeft met betrekking tot de verwerking van de doorgegeven gegevens, is de situatie niet eenduidig en zal een enkele overeenkomst tussen de partijen bij de doorgifte voor individuele betrokkenen wellicht niet altijd een voldoende grondslag opleveren om hun rechten te kunnen uitoefenen. Mogelijk zal een regeling noodzakelijk zijn, op grond waarvan de overdrager in de Gemeenschap aansprakelijk blijft voor elke schade die zou kunnen voortvloeien uit de verwerking in het derde land.

[18] In de zaak Citibank 'Bahncard' werkte de Berlijnse commissaris voor gegevensbescherming samen met de Amerikaanse autoriteiten op het gebied van banktoezicht.

- Verdere doorgifte naar instanties of organisaties die niet gebonden zijn door de overeenkomst moet door de overeenkomst specifiek worden uitgesloten, tenzij het mogelijk is dergelijke derden er contractueel toe te verplichten dezelfde beginselen inzake gegevensbescherming in acht te nemen.
- Het vertrouwen dat de gegevensbeschermingsbeginselen na de doorgifte in acht zullen worden genomen, zou worden versterkt indien de naleving van de regels inzake gegevensbescherming door de ontvanger van de doorgegeven gegevens onderworpen is aan externe controle door bijvoorbeeld een gespecialiseerd auditbureau of een normalisatie- of certificeringsinstelling.
- Indien een betrokkene een moeilijkheid ondervindt, die mogelijk het gevolg is van een inbreuk op de door de overeenkomst gewaarborgde regels inzake gegevensbescherming, is er een algemeen probleem om te waarborgen dat de klacht van de betrokkene naar behoren wordt onderzocht. De toezichthoudende autoriteiten van de EU-lidstaten zullen het in de praktijk moeilijk hebben om een dergelijk onderzoek uit te voeren.
- Contractuele oplossingen zijn wellicht het meest geschikt voor grote internationale netwerken (kredietkaarten, vliegticketreservaties), die worden gekenmerkt door grote hoeveelheden repetitieve en soortgelijke gegevensdoorgiften en door een klein aantal grote ondernemingen of organisaties zijn die reeds onderworpen zijn aan ruime controle en regulering door de overheid. Doorgiften binnen dezelfde bedrijvengroep zijn een ander terrein waarop er duidelijk mogelijkheden zijn voor het gebruik van contracten.
- Landen waar de bevoegdheden van de overheid om toegang te krijgen tot informatie verder gaan dan volgens de internationale normen inzake bescherming van de mensenrechten geoorloofd is, zijn geen veilige bestemmingen voor de doorgifte van gegevens op basis van contractuele bepalingen.

HOOFDSTUK 5: AFWIJKINGEN VAN DE EISEN INZAKE HET PASSEND BESCHERMINGSNIVEAU

Artikel 26, lid 1, van de richtlijn noemt een beperkt aantal situaties waarin een afwijking mogelijk is van de eis inzake passende bescherming voor doorgiften naar een derde land. Deze afwijkingen, die precies zijn omschreven, hebben meestal betrekking op gevallen waar de risico's voor de betrokkene vrij beperkt zijn of waar andere belangen (overheidsbelang of belang van de betrokkene zelf) belangrijker zijn dan de bescherming van de persoonlijke levenssfeer van de betrokkene. Als afwijkingen van een algemeen beginsel moeten zij restrictief worden geïnterpreteerd. Bovendien kunnen lidstaten in hun nationaal recht bepalen dat de afwijkingen in specifieke gevallen niet gelden. Dit kan bijvoorbeeld het geval zijn bij bijzonder kwetsbare groepen personen, zoals werknemers of patiënten.

De eerste van deze afwijkingen heeft betrekking op gevallen waarin de betrokkene zijn *ondubbelzinnige* toestemming voor de voorgenomen doorgifte heeft gegeven. Een belangrijk punt hierbij is dat de toestemming, volgens de definitie in artikel 2, onder h), van de richtlijn, op een vrije, specifieke en op informatie berustende wilsuiting moet zijn gebaseerd. De voorwaarde inzake informatie is bijzonder relevant, aangezien deze inhoudt dat de betrokkene naar behoren op de hoogte wordt gebracht van het risico dat zijn gegevens worden doorgegeven naar een land dat onvoldoende bescherming biedt. Indien deze informatie niet wordt verstrekt, is deze afwijking niet van toepassing. Aangezien de toestemming ondubbelzinnig moet zijn, is bij elke twijfel omtrent het feit of toestemming is gegeven, de afwijking niet van toepassing. Dit komt er meestal op neer dat deze afwijking niet geldt voor vele situaties waarin toestemming geacht wordt impliciet te zijn gegeven (bijvoorbeeld wanneer iemand van een doorgifte op de hoogte is gebracht en geen bezwaar heeft gemaakt). De afwijking zou echter nuttig kunnen zijn in gevallen waarin degene die de gegevens doorgeeft rechtstreeks contact heeft met de betrokkene en waarin de vereiste informatie gemakkelijk kan wordt verstrekt en ondubbelzinnige toestemming kan worden verkregen. Dit kan vaak het geval zijn bij doorgiften in het kader van verzekeringsdiensten bijvoorbeeld.

De tweede en derde afwijking hebben betrekking op doorgiften die *noodzakelijk* zijn voor de uitvoering van een overeenkomst tussen de betrokkene en de voor de verwerking verantwoordelijke (of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen) of voor de sluiting of de uitvoering van een *in het belang van de betrokkene* tussen de voor de verwerking verantwoordelijke en een derde gesloten overeenkomst. Deze afwijkingen lijken vrij ruim opgezet, maar zoals bij de vierde en vijfde afwijking is de toepassing ervan in de praktijk beperkt door de voorwaarde inzake de noodzakelijkheid: alle doorgegeven gegevens moeten noodzakelijk zijn voor de uitvoering van de overeenkomst. Indien aanvullende niet-essentiële gegevens worden doorgegeven of indien de doorgifte niet voor de uitvoering van de overeenkomst bedoeld is maar een ander doel heeft (bijvoorbeeld follow-up van marketing) geldt de afwijking niet meer. Precontractuele situaties hebben alleen betrekking op situaties die door toedoen van de betrokkene zijn ontstaan (zoals een verzoek om informatie over een bepaalde dienst) en niet diegene die voortvloeien uit marketingdoeleinden van de voor de verwerking verantwoordelijke.

Ondanks dit voorbehoud zijn de tweede en derde afwijking niet betekenisloos. Zij zullen waarschijnlijk vaak toepasbaar zijn wanneer bijvoorbeeld voor de doorgiften die noodzakelijk zijn voor vliegticketreservaties of voor doorgiften van persoonsgegevens die noodzakelijk zijn voor het verrichten van een internationale betaling via de bank of met een kredietkaart. De afwijking voor overeenkomsten "in het belang van de betrokkene" (artikel 26, lid 1, onder c)) heeft namelijk specifiek betrekking op de doorgifte van gegevens over de ontvangers van betalingen via een bank die, hoewel zij betrokkenen zijn, vaak geen partij zijn bij een overeenkomst met de voor de verwerking verantwoordelijke.

De vierde afwijking omvat twee aspecten. Het eerste heeft betrekking op doorgiften die noodzakelijk of wettelijk verplicht zijn vanwege een zwaarwegend algemeen belang. Dit kan slaan op bepaalde beperkte doorgiften tussen overheidsdiensten, hoewel deze bepaling niet te ruim mag worden geïnterpreteerd. Een eenvoudig algemeen belang voor het rechtvaardigen van een doorgifte is niet voldoende; het moet gaan om een *zwaarwegend* algemeen belang. Volgens overweging 58 vallen gegevensdoorgiften tussen belasting- of douanediensten of tussen voor de sociale zekerheid bevoegde diensten in het algemeen onder deze afwijking. Doorgiften tussen toezichthoudende autoriteiten in de financiële dienstensector kunnen ook onder deze afwijking vallen. Het tweede aspect heeft betrekking op doorgiften die plaatsvinden in het kader van internationale geschillen of rechtsgedingen, met name doorgiften die noodzakelijk zijn voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

De vijfde afwijking heeft betrekking op doorgiften die noodzakelijk zijn ter vrijwaring van het vitale belang van de betrokkene. Een duidelijk voorbeeld van een dergelijke doorgifte is de dringende doorgifte van medische bestanden aan een derde land waar een toerist die tevoren in de EU een medische behandeling heeft ondergaan, het slachtoffer is geworden van een ongeval of ernstig ziek is geworden. Er moet echter rekening mee worden gehouden dat overweging 31 van de richtlijn ‘vitaal belang’ vrij restrictief wordt opgevat als een “belang dat voor het leven van de betrokkene essentieel is”. Dit sluit normaalgesproken bijvoorbeeld financiële, eigendoms- of familiebelangen uit.

De zesde en laatste afwijking heeft betrekking op doorgiften vanuit openbare registers, die krachtens de wet bedoeld zijn om door het publiek te worden geraadpleegd, voorzover in het desbetreffende geval voldaan is aan de voorwaarden voor raadpleging. Doel van deze afwijking is dat wanneer een register in een lidstaat beschikbaar is voor openbare raadpleging of voor raadpleging door personen die zich op een rechtmatig belang kunnen beroepen, het feit dat de persoon die het recht heeft het register te raadplegen zich daadwerkelijk in een derde land bevindt en het feit dat raadpleging een gegevensdoorgifte omvat, niet mogen verhinderen dat de informatie aan hem wordt doorgegeven. Overweging 58 verduidelijkt dat geen hele registers of hele categorieën gegevens uit registers in het kader van deze afwijking mogen worden doorgegeven. Gezien deze beperkingen mag deze afwijking niet als algemene afwijking voor de doorgifte van gegevens uit openbare registers worden beschouwd. Het is bijvoorbeeld duidelijk dat massale doorgiften van gegevens uit openbare registers voor

commerciële doeleinden of het aanwenden van openbaar beschikbare gegevens voor het profileren van bepaalde personen niet voor deze afwijking in aanmerking komen.

HOOFDSTUK 6: PROCEDURELE VRAAGSTUKKEN

Artikel 25 voorziet in een aanpak geval per geval waarbij het passend beschermingsniveau wordt beoordeeld in het licht van specifieke doorgiften of categorieën doorgiften. Het is evenwel duidelijk dat gelet op het groot aantal persoonsgegevens dat dagelijks vanuit de Gemeenschap wordt doorgegeven en op het aantal daarbij betrokken actoren, geen enkele lidstaat - ongeacht zijn wijze van tenuitvoerlegging van artikel 25[19] - zal kunnen garanderen dat elk geval in detail wordt onderzocht. Dit betekent niet dat geen enkel geval in detail wordt bezien, maar veeleer dat mechanismen moeten worden ontwikkeld die de beslissingsprocedure voor een groot aantal gevallen rationaliseren, zodat beslissingen, of althans voorlopige beslissingen, zonder al te veel moeilijkheden of kosten kunnen worden genomen.

Een dergelijke rationalisatie is noodzakelijk, ongeacht wie de beslissing neemt, de verantwoordelijke voor de verwerking, de toezichthoudende autoriteit of enige andere volgens een nationale procedure daarmee belaste instantie.

(i) Toepassing van artikel 25, lid 6, van de richtlijn

Een voor de hand liggende oplossing voor de rationalisatie, waarin de richtlijn voorziet, bestaat erin vast te stellen dat bepaalde derde landen een passend beschermingsniveau bieden. Dergelijke constateringen zijn 'enkel als richtsnoer' bedoeld en vormen dan ook geen nadeel voor gevallen die bijzondere moeilijkheden zouden opleveren. Het zou echter wel een praktisch antwoord op het probleem zijn.
Dergelijke constateringen zouden meer bepaald economische subjecten enige zekerheid bieden ten aanzien van de landen die worden geacht in het algemeen een passend beschermingsniveau te waarborgen. Zij zouden tevens een duidelijke en publieke stimulans bieden voor de derde landen die nog bezig zijn hun beschermingssysteem op te zetten en te verbeteren. Bovendien zou een reeks van dergelijke constateringen op communautair niveau kunnen bijdragen tot de totstandkoming van een samenhangende aanpak van dit vraagstuk en de ontwikkeling voorkomen van talrijke verschillende en wellicht tegenstrijdige 'witte lijsten' die worden opgesteld door nationale overheden of gegevensbeschermingsautoriteiten.

Een moeilijkheid van deze aanpak is dat in verscheidene derde landen het beschermingsniveau niet in alle sectoren hetzelfde is. Zo hebben tal van landen een gegevensbeschermingswetgeving voor de publieke sector, maar niet voor de particuliere sector. Zo bestaan bijvoorbeeld in de Verenigde Staten voor bepaalde sectoren specifieke wetten, zoals voor solvabiliteitsinformatie en videoverhuur, terwijl voor andere sectoren geen regelingen bestaan. Een extra moeilijkheid doet zich voor met federale landen, zoals de Verenigde Staten, Canada en Australië, waar er vaak verschillen tussen de deelstaten bestaan. Het is dan ook onwaarschijnlijk dat momenteel vele derde landen kunnen worden geacht over de hele linie een passend

[19] De lidstaten kunnen verschillende administratieve procedures toepassen om aan de verplichtingen van artikel 25 te voldoen. Zo kunnen zij een directe verplichting opleggen aan de voor de verwerking verantwoordelijken en/of kunnen zij een stelsel van voorafgaande toestemming of van controle a posteriori door de toezichthoudende autoriteit invoeren.

beschermingsniveau te bieden. Hoe kleiner het aantal landen waarvoor positieve constateringen kunnen worden gedaan, hoe minder zekerheid dit uiteraard voor de voor de verwerking verantwoordelijken oplevert. Een ander risico is dat sommige derde landen het ontbreken van een constatering dat zij passende bescherming bieden als politieke provocatie of op zijn minst als discriminatie zouden kunnen opvatten, aangezien de afwezigheid van een constatering evengoed het resultaat kan zijn van het feit dat hun situatie niet is onderzocht als van een beoordeling van hun gegevensbeschermingssysteem.

Na zorgvuldige afweging van deze argumenten is de Groep niettemin van mening dat werkzaamheden die moeten uitmonden in een reeks constateringen overeenkomstig artikel 25, lid 6, een nuttige stap zouden zijn. Een dergelijke procedure moet als een continue procedure worden beschouwd, die dus niet tot een definitieve lijst leidt maar tot een lijst die in het licht van de ontwikkelingen constant wordt aangevuld en aangepast. Een positieve constatering mag in principe niet beperkt zijn tot landen met horizontale gegevensbeschermingswetten, maar moet ook specifieke sectoren binnen een land omvatten waar het gegevensbeschermingsniveau passend is, ook al is dat voor andere sectoren in datzelfde land niet het geval.

Er zij op gewezen dat de krachtens artikel 29 opgerichte Groep geen expliciete taak heeft bij beslissingen over specifieke gegevensdoorgiften of bij het bepalen van een "passend beschermingsniveau" overeenkomstig artikel 25, lid 6. Beide zijn onderworpen aan de comitologieprocedure zoals bepaald in artikel 31. Een van de specifieke taken van de krachtens artikel 29 opgerichte Groep is echter wel de Commissie advies te verstrekken over het beschermingsniveau in derde landen (zie artikel 30, lid 1, onder b)). Het valt dan ook onder de bevoegdheid van de Groep om de situatie in bepaalde derde landen te onderzoeken en een voorlopig standpunt betreffende het passend beschermingsniveau te bepalen. Positieve constateringen, die zijn bevestigd overeenkomstig artikel 25, lid 6, zijn alleen nuttig als zij op ruime schaal worden bekendgemaakt. Wanneer anderzijds niet wordt geoordeeld dat een land een passend beschermingsniveau biedt, hoeft dit niet te betekenen dat het land impliciet of expliciet op de 'zwarte lijst' komt, maar is de boodschap veeleer dat nog geen algemene richtsnoeren over dat land beschikbaar zijn.

(ii) Risicoanalyse van specifieke doorgiften

Hoewel de toepassing van artikel 25, lid 6, zoals hierboven beschreven, weliswaar een waardevol hulpmiddel kan zijn voor de beslissingen bij een groot aantal gegevensdoorgiften, zal voor het derde land in kwestie in vele gevallen toch geen positieve constatering voorhanden zijn. De lidstaten kunnen dan afhankelijk van hun omzetting van artikel 25 in het nationale recht op verschillende manieren te werk gaan (zie voetnoot op de vorige bladzijde). Wanneer de toezichthoudende autoriteit een specifieke rol heeft bij de voorafgaande toestemming voor doorgiften of bij de controle a posteriori, kan het alleen al vanwege het aantal doorgiften noodzakelijk zijn een systeem uit te werken om vast te stellen welke zaken de toezichthoudende autoriteit bij voorrang moet behandelen. Een dergelijk systeem kan bestaan in een reeks afgesproken criteria op grond waarvan een gegevensdoorgifte of categorie doorgiften als risico voor de persoonlijke levenssfeer kan worden aangemerkt.

Een dergelijk systeem doet niet af aan de verplichting van elke lidstaat om erop toe te zien dat enkel gegevens worden doorgegeven aan derde landen die een passend beschermingsniveau waarborgen. Met dit systeem kan ook worden uitgemaakt welke gevallen van gegevensdoorgiften moeten worden aangemerkt als "bij voorrang te behandelen" of waarvoor een onderzoek of zelfs een opsporingsonderzoek moet worden gestart. Op die manier zouden de beschikbare middelen direct kunnen worden aangewend voor doorgiften die vanuit het oogpunt van bescherming van de persoonlijke levenssfeer het meeste aandacht verdienen.

De Groep is van oordeel dat de volgende categorieën doorgiften bijzonder risicodragend zijn voor de persoonlijke levenssfeer:

- doorgiften die verband houden met gevoelige-gegevenscategorieën overeenkomstig artikel 8 van de richtlijn;
- doorgiften die een financieel risico inhouden (zoals kredietkaartbetalingen via Internet);
- doorgiften die een gevaar voor de veiligheid van personen inhouden;
- doorgiften gericht op het nemen van beslissingen die voor de betrokkene van groot belang kunnen zijn (zoals aanwerving, promotie, kredietverlening enz.);
- doorgiften die de betrokkene in verlegenheid kunnen brengen of zijn reputatie kunnen schaden;
- doorgiften die kunnen leiden tot handelingen die een duidelijke inbreuk op de persoonlijke levenssfeer vormen, zoals ongewenste telefonische contacten;
- herhaaldelijke doorgifte van grote hoeveelheden gegevens (bijvoorbeeld via telecommunicatienetwerken, Internet enz. verwerkte elektronische gegevens);
- doorgiften die betrekking hebben op een versleutelde of geheime inzameling van gegevens (zoals "Internet-cookies" of elektronische visitekaartjes).

(iii) Modelcontractbepalingen

Zoals in Hoofdstuk 4 uitgebreid is besproken is in de richtlijn de mogelijkheid voorzien dat, zelfs wanneer het beschermingsniveau niet passend is, een voor de verwerking verantwoordelijke door middel van een overeenkomst passende waarborgen voor een gegevensdoorgifte kan bieden. Artikel 26, lid 2, van de richtlijn biedt lidstaten de mogelijkheid toestemming te geven voor doorgiften op basis van dergelijke contractuele bepalingen, een beslissing waarvan de Commissie vervolgens in kennis moet worden gesteld. Indien er bezwaren tegen de toestemming zijn, kan de beslissing door de Commissie na de comitologieprocedure overeenkomstig artikel 31 ongedaan worden gemaakt of worden bevestigd. Behalve de toestemmingen door lidstaten, stelt artikel 26, lid 4, van de richtlijn ook de Commissie in staat om, eveneens na de comitologieprocedure overeenkomstig artikel 31, te oordelen of bepaalde modelcontractbepalingen voldoende waarborgen bieden. Deze besluiten zijn dan bindend voor de lidstaten.

Gezien de complexiteit en de moeilijkheden van dergelijke contractuele oplossingen, is er duidelijk behoefte aan overeengekomen richtsnoeren voor de voor de verwerking verantwoordelijken die op die manier contracten willen gebruiken. Op het niveau van de lidstaten zullen de bevoegde nationale instanties waarschijnlijk als eerste verantwoordelijk zijn voor het verstrekken van deze richtsnoeren, vooral bij het verlenen van toestemmingen overeenkomstig artikel 26, lid 2. De nationale overheden

en de Commissie moeten samenwerken en meningen uitwisselen over contractbepalingen die hen worden voorgelegd. Wanneer voorgestelde modelbepalingen bij nationale overheden of rechtstreeks bij de Commissie worden ingediend, moet een procedure worden ontwikkeld, zodat deze bepalingen ook door de Groep kunnen worden onderzocht om te voorkomen dat de nationale praktijken mettertijd gaan uiteenlopen en om te verzekeren dat de Commissie een beroep kan doen op bijstand van deskundigen alvorens besluiten worden genomen overeenkomstig artikel 26, lid 4.

BIJLAGE 1

PRAKTISCHE TOEPASSING VAN DE ARTIKELEN 25 EN 26 VAN DE RICHTLIJN OP HET DOORGEVEN VAN PERSOONSGEGEVENS NAAR DERDE LANDEN

Inleiding

In het hoofdgedeelte van dit document wordt een algemene aanpak voor de doorgifte naar derde landen uiteengezet. Deze aanpak omvat:

- beoordeling of een passend beschermingsniveau wordt geboden in de zin van artikel 25 van de richtlijn gegevensbescherming;
- beoordeling van de alternatieve mogelijkheid om door middel van contractuele oplossingen, zoals bedoeld bij overeenkomstig artikel 26, lid 2, een passend beschermingsniveau te verkrijgen;
- beoordeling van de afwijkingen van het vereiste dat een passend beschermingsniveau moet worden geboden overeenkomstig artikel 26, lid 1.

Voor een volledig begrip van de problematiek moet echter ook worden aangetoond welke het waarschijnlijk effect van deze algemene aanpak op reële doorgiften van persoonsgegevens zal zijn. In deze bijlage worden derhalve een aantal realistische (maar fictieve) casestudy's van gegevensdoorgiften beschreven. Daarbij wordt uitgegaan van de aanpak die waarschijnlijk voor hen zal gelden zodra de nationale wetten tot uitvoering van de richtlijn van kracht zijn geworden.

Er worden drie verschillende gevallen behandeld. De eerste stap bestaat er steeds in te beoordelen of het beschermingsniveau in het land van bestemming, dat voortvloeit uit de wetgeving ter zake of uit effectieve zelfregulering door de particuliere sector, als passend kan worden beschouwd. Zo niet, dan bestaat de tweede stap erin om uit de mogelijkheden van artikel 26, lid 1 (afwijkingen), en lid 2 (contractuele bepalingen), de beste oplossing te kiezen. Alleen als geen van deze oplossingen geschikt is, bestaat de derde stap erin de doorgifte te verhinderen.

CASESTUDY (1) : Doorgifte van gegevens betreffende kredietwaardigheid

Een EU-burger wil een vakantiewoning kopen in land A buiten de Gemeenschap en vraagt bij een financiële instelling van dat land een lening aan. De financiële instelling verzoekt een gespecialiseerd bedrijf om een kredietrapport over de aanvrager. Het bedrijf beschikt zelf niet over gegevens over de aanvrager, maar vraagt bij zijn "zusteronderneming" in het VK, een bureau voor kredietreferenties, alle gegevens over het kredietverleden van de aanvrager aan. Land A is een geïndustrialiseerd land met een hoog ontwikkelingsniveau en een lange democratische traditie met stabiele instellingen. Het justitieel apparaat beschikt over voldoende instrumenten en middelen en functioneert goed. Het land is een constitutionele federatie.

STAP 1 : BEOORDELING VAN HET BESCHERMINGSNIVEAU

Wetten en voorschriften die van toepassing zijn

De voor de verwerking verantwoordelijke die de gegevens ontvangt is gehouden aan een federale wet die regels vastlegt voor persoonlijke informatie met het oog op kredietrisico's. De voor de verwerking verantwoordelijke verklaart bovendien dat hij zich houdt aan de eigen gepubliceerde privacyvoorschriften van het bedrijf. Er is geen wet op staatsniveau van toepassing en er is geen zelfregulering in de vorm van een de gehele bedrijfstak omvattende gedragscode.

Beoordeling van de inhoud van de toepasselijke wetten en voorschriften

Om te beginnen zij erop gewezen dat de communicatie van het in het VK gebaseerde bureau voor kredietreferenties net als andere communicaties met een voor de verwerking verantwoordelijke elders in het VK of in een andere lidstaat moet voldoen aan de normale voorwaarden in de Britse wet die alle artikelen van de richtlijn, afgezien van de artikelen 25 en 26, in nationale wet omzet. Dit is van belang, omdat het om deze reden niet noodzakelijk is na te gaan of de communicatie zelf conform de wet is. De aandacht gaat veeleer uit naar het beschermingsniveau dat na doorgifte naar land A op de gegevens van toepassing is.

Bij een beoordeling van de inhoud van de regelgeving is het logisch om bij de federale wetgeving te beginnen. Als blijkt dat hierin bepaalde lacunes bestaan, zou kunnen worden onderzocht of deze worden aangevuld door de "zachtere" privacyvoorschriften. Hieronder volgt een opsomming van de beginselen die moeten zijn opgenomen en een beantwoording van de vraag of deze beginselen in de wetgeving of in de privacyvoorschriften aanwezig zijn.

Het specificiteitsbeginsel betreft in dit verband alleen de voorwaarde dat eventueel verder gebruik of eventuele verstrekking van de doorgegeven gegevens aan anderen niet onverenigbaar mag zijn met het doel waarvoor de gegevens oorspronkelijk werden doorgegeven. Het gebruik van de gegevens voor een adressenbestand dat op de vrije markt wordt verkocht of verhuurd kan als onverenigbaar worden beschouwd.

Hetzelfde geldt voor verstrekking van de gegevens aan mogelijke werkgevers en zakenpartners die informatie wensen over de kredietwaardigheid van de betrokkene. Verstrekking van de gegevens aan andere kredietverleners (banken, kredietkaartbedrijven) zou echter wel verenigbaar kunnen zijn.
In dit geval zijn in de federale wetgeving een beperkt aantal doeleinden vastgelegd waarvoor persoonlijke kredietgegevens rechtmatig kunnen worden verstrekt. Deze doeleinden omvatten evenwel ook "werkgelegenheid" en "legitieme zakelijke behoeften in verband met zakentransacties met de betrokkene". Dit laatste begrip omvat het gebruik van de gegevens voor bepaalde marketingdoeleinden, waaronder mogelijk ook de marketing door derden van goederen of diensten op andere gebieden dan de kredietverstrekking.
De conclusie lijkt dus te zijn dat de specificiteit in de federale wetgeving onvoldoende is gewaarborgd en dat op dit punt geen passend beschermingsniveau wordt geboden. De privacyvoorschriften van het bedrijf vullen deze lacune niet aan.

Het transparantiebeginsel houdt in dat aan de betrokkene wordt meegedeeld welk gespecialiseerd bedrijf in land A om een kredietrapport is verzocht en in voorkomend geval voor welke nieuwe doeleinden de gegevens worden verwerkt. De precieze wijze waarop dit wordt gedaan moet vergelijkbaar zijn met de in artikel 11 van de richtlijn beschreven procedure.
Wat dit punt betreft bevat de federale wetgeving geen specifieke transparantiebepalingen die rechtstreeks van toepassing zijn op het bedrijf dat het kredietrapport opstelt. De kredietverlener in land A is evenwel verplicht de betrokkene ervan in kennis te stellen dat bij een gespecialiseerd bedrijf een kredietrapport zal worden aangevraagd, hoewel naam en adres van het bedrijf niet hoeven te worden vermeld.
De wet biedt de betrokkene dus geen garantie dat hem wordt medegedeeld welk bedrijf zijn gegevens verwerkt. Aangezien het bedrijf echter geen direct contact heeft met de betrokkene, kan een aan het bedrijf opgelegde verplichting om specifiek met de betrokkene contact op te nemen om hem/haar informatie te verstrekken worden gezien als een verplichting die "onevenredig veel moeite kost" in de zin van artikel 11 van de richtlijn. Vanuit het oogpunt van de transparantie kan het beschermingsniveau dus als passend worden beschouwd.

Het kwaliteits- en evenredigheidsbeginsel omvat een verschillende elementen. De federale wetgeving legt geen beperkingen op met betrekking tot de verzameling en verwerking van onnodige gegevens. Er zijn wel voorschriften ten aanzien van de duur van de opslag ter voorkoming van de verspreiding van verouderde informatie (faillietverklaringen van meer dan 10 jaar gelden), wat er in de praktijk op neerkomt dat deze informatie wordt vernietigd. Er is geen algemene wettelijke plicht om de nauwkeurigheid van de gegevens te waarborgen, hoewel gegevens waarvan de juistheid niet kan worden gecontroleerd moeten worden verwijderd, als de betrokkene die inzage in zijn kredietrapport heeft gevraagd bepaalde gegevens aanvecht.
Ook hier lijkt het beschermingsniveau niet geheel adequaat en vullen de privacyvoorschriften de lacune in de federale wetgeving niet aan.

Het beveiligingsbeginsel komt in de federale wetgeving tot uiting in de verplichting redelijke maatregelen te nemen om onrechtmatige verstrekkingen te voorkomen. Volgens de privacyvoorschriften van het bedrijf wordt er streng op toegezien dat

kredietinformatie niet toegankelijk is voor en niet kan worden gebruikt door onbevoegden. Dit toezicht bestaat uit zowel technische maatregelen (passwords enz.) als regels waaraan werknemers zich op straffe van tuchtmaatregelen dienen te houden. Deze maatregelen lijken een adequate beveiliging te vormen.

Het recht van toegang en rectificatie maakt deel uit van de federale wetgeving die op dit punt vergelijkbaar is met de richtlijn. Als aan een betrokkene krediet wordt geweigerd, is de toegang tot het kredietrapport gratis. Er bestaat evenwel geen recht van verzet, hoewel de betrokkene bij een gespecialiseerde federale instantie een klacht kan indienen of naar het gerecht (zie hieronder) kan stappen, als hij meent dat zijn in de federale wetgeving vastgelegde rechten zijn geschonden.

Gevoelige gegevens met betrekking tot de gezondheid van de betrokkene maken deel uit van de doorgegeven informatie. De federale wetgeving bevat wel strengere bepalingen voor de verwerking van informatie betreffende strafbladen, geslacht, ras, ethnische afkomst, leeftijd en huwelijkse staat, maar niet voor gezondheidsgegevens. In de privacyvoorschriften van het bedrijf dat het kredietrapport opstelt is echter een bepaling opgenomen dat gegevens betreffende de gezondheid niet mogen worden gebruikt voor de beoordeling van de kredietwaardigheid, maar alleen voor controles betreffende de werksituatie of de verzekeringsstatus. In deze twee gevallen verleent de betrokkene op een sollicitatie- of verzekeringsformulier toestemming voor het gebruik van die gegevens.
De gezondheidsgegevens in dit voorbeeld genieten dus een aanzienlijke extra bescherming, ook al is die bescherming niet wettelijk vastgelegd.

Het gebruik van de gegevens door het betrokken bedrijf voor direct marketing (en het doorgeven van de gegevens aan anderen voor dergelijke doeleinden) vormt in dit verband een probleem. Er zijn geen wettelijke bepalingen die een dergelijk gebruik reëel aan banden leggen en er bestaat geen wettelijke verplichting een "opt-out" aan te bieden. De bescherming is op dit punt duidelijk onvoldoende, met name daar de gegevens niet alleen door het bedrijf kunnen worden gebruikt (voor mailings namens kredietverlenende financiële instellingen), maar ook aan derden voor marketingdoeleinden kunnen worden doorgegeven, niet alleen voor aanverwante producten op het gebied van financiële diensten, maar ook voor producten die hier niets mee te maken hebben, zoals maaimachines of vakanties.

De doorgifte kan een geautomatiseerd besluit omtrent de kredietverlening tot doel hebben. De betrokkene moet in dit verband dus extra garanties hebben. Hoewel in de federale wetgeving bepalingen zijn opgenomen die de betrokkene in staat stellen de informatie in het kredietrapport aan te vechten en zo nodig aan het rapport een toelichting toe te voegen, voorziet de wet niet in de mogelijkheid een beslissing die op basis van foutieve of onvolledige informatie wordt genomen aan te vechten en te laten onderzoeken en deze, als blijkt dat de aanvechting terecht is, terug te laten draaien. Het mechanisme maakt het mogelijk een kredietrapport te wijzigen om toekomstige problemen te voorkomen, maar houdt niet noodzakelijkerwijze gevolgen in voor een reeds genomen besluit. Deze bescherming, die geen rectificatie achteraf omvat, is niet voldoende.

Beperkingen inzake verdere doorgifte van de gegevens aan een ander derde land of aan organisaties in andere sectoren van land A die niet vallen onder de in de federale wetgeving vastgelegde voorschriften: noch in de federale wetgeving noch in de eigen privacyvoorschriften van het bedrijf zijn dergelijke restricties opgenomen.

Draagwijdte van de federale wetgeving en de eigen privacyvoorschriften van het bedrijf
Tot slot moet worden gecontroleerd of de wetgeving en de privacyvoorschriften voor informatie over alle personen gelden, dus niet alleen voor gegevens over ingezetenen of onderdanen van land A. In dit geval is zijn er geen dusdanige beperkingen van de draagwijdte.

Beoordeling van de doeltreffendheid van de bescherming

De federale wetgeving heeft kracht van wet en voorziet ook in een overheidsdienst met bepaalde externe toezichthoudende bevoegdheden. De wet voorziet ook in de mogelijkheid om als particulier een geding aan te spannen als rechten worden geschonden. De overheidsdienst is evenwel niet duidelijk verplicht om alle afzonderlijke klachten te onderzoeken en is volgens bepaalde waarnemers nog wel eens laks bij het handhaven van de wet. Een geding is voor een particulier een dure en vaak tijdrovende manier om verhaal te zoeken, met name als men niet woont in het land waar men het geding heeft aangespannen.

De interne privacyvoorschriften van het bedrijf voorzien niet in een onafhankelijk mechanisme dat betrokkenen in staat stelt verhaal te zoeken, maar bevat wel tuchtmaatregelen voor werknemers die deze voorschriften schenden. Verscheidene werknemers zijn in het verleden reeds bestraft omdat zij zich niet aan de voorschriften hielden.

De combinatie van wetgeving en interne privacyvoorschriften moet worden geëvalueerd in het kader van de doelstellingen die voor procedurele mechanismen zijn vastgesteld. In dit geval kunnen daarbij bijvoorbeeld de volgende aspecten centraal staan:

Goede naleving

Het risico van een slechte pers bij niet-nakoming van beloften is voor het bedrijf de belangrijkste stimulans om de eigen privacyvoorschriften na te leven. Bovendien lopen werknemers van het bedrijf het risico van tuchtmaatregelen als zij de beveiligingsvoorschriften niet opvolgen.
Op zich lijken deze mechanismen evenwel niet voldoende om te waarborgen dat de privacyvoorschriften in de praktijk worden nageleefd.
Tot een andere conclusie had men kunnen komen als:
(1) de privacyvoorschriften van het bedrijf een afspiegeling waren geweest van een door de betrokken brancheorganisatie vastgelegde gedragscode voor de gehele bedrijfstak, waarbij niet-naleving van de code door een bedrijf onmiddellijk tot uitsluiting van de organisatie zou leiden;
of als

(2) in de wet een algemeen beginsel was vastgelegd op grond waarvan een overheidsinstantie een bedrijf wegens "oneerlijke en bedrieglijke" praktijken voor het gerecht kan dagen, als het zich niet aan zijn eigen gepubliceerde privacyvoorschriften houdt.

Wat de federale wetgeving betreft wordt naleving gestimuleerd door het risico van rechtszaken die door particulieren bij niet-naleving kunnen worden aangespannen. De mogelijkheid om voor het gerecht gedaagd te worden zal tot op zekere hoogte een afschrikkend effect hebben op degene die voor de verwerrking verantwoordelijk is. De wetgeving schiet evenwel ernstig tekort op het stuk van de directe externe controle van procedures voor de gegevensverwerking, daar de overheidsdienst pas in het geweer komt als zijn aandacht, bijvoorbeeld door een klager of de pers, op een bepaald probleem wordt gevestigd.

Bijstand aan de betrokkene
Het is duidelijk dat een overheidsdienst bestaat en dat deze dient als centraal punt waar betrokkenen klachten over hun kredietrapport kunnen indienen. Het onderzoek van die klachten is gratis voor de betrokkenen.

Passende schadeloosstelling
Bij niet-nakoming van verplichtingen die met redelijke duidelijkheid in de federale wetgeving zijn vastgelegd, kan de betrokkene bij het gerecht verhaal zoeken. Dit is echter een betrekkelijk dure stap, waarbij de betrokkene doorgaans geen financiële hulp van de overheidsdienst krijgt. De rechter kan de voor de verwerking verantwoordelijke opdragen de betrokkene schadeloos te stellen (indien wordt vastgesteld dat schade is toegebracht) en de procedures voor de verwerking van de gegevens en de inhoud van het betrokken dossier te wijzigen. Er zijn geen verhaalmogelijkheden bij schending van gegevensbeschermingsbeginselen die alleen in de privacyvoorschriften zijn vervat.

Oordeel

1) Sommige van de "basisbeginselen" van de gegevensbescherming die in het discussiestuk worden genoemd zijn in een of andere vorm terug te vinden in de federale wet die op het kredietdossier van toepassing is. Andere maken deel uit van de privacyvoorschriften. Maar zelfs de federale wet en de privacyvoorschriften samen bevatten niet alle "basisbeginselen" en sommige van de wel aanwezige beginselen (bijvoorbeeld het specificiteitsbeginsel) zijn in een vrij zwakke vorm opgenomen.
2) Een probleem van meer algemene aard is of de privacyvoorschriften van het bedrijf in de praktijk wel zo effectief zijn dat hiermee rekening moet worden gehouden. Tenzij deze voorschriften worden versterkt en naleving ervan beter wordt gegarandeerd door aan een brancheorganisatie of overheidsinstantie bevoegdheden voor een externe controle toe te kennen, kan naleving hiervan nauwelijks worden afgedwongen en kunnen zij dus buiten beschouwing blijven.
3) Hoewel de overheidinstantie die toezicht houdt op naleving van de federale wetgeving niet helemaal over dezelfde bevoegdheden beschikt als de typische Europese instantie voor gegevensbescherming, biedt de wet toch een zekere wettelijke garantie, met name gezien het goed functionerende justitiële apparaat en de "procedeercultuur"

in land A. Over misschien wel het allerbelangrijkste beginsel op het gebied van de gegevensbescherming - het recht van toegang en rectificatie - bevat de wet duidelijk omschreven bepalingen; ook zijn bepaalde restricties opgenomen met betrekking tot de doeleinden waarvoor de gegevens kunnen worden gebruikt.

Conclusie

Het beschermingsniveau kan niet als passend worden beschouwd, daar te weinig "basisbeginselen" in de wetgeving zijn vastgelegd en de privacyvoorschriften op zich geen effectief instrument zijn om bescherming te bieden. Tot een passend beschermingsniveau zou men kunnen komen door de wetgeving verder te ontwikkelen en hierin principiële bepalingen omtrent de transparantie en de bescherming van gezondheidsgegevens op te nemen of door de privacyvoorschriften op een van de bovengenoemde manieren te versterken (dus door naleving tot voorwaarde van het lidmaatschap van een brancheorganisatie te maken of door een overheidsinstantie bevoegdheden te verlenen om bedrijven wegens misleidende en bedrieglijke praktijken voor het gerecht te dagen, als zij hun eigen voorschriften niet naleven).

STAP 2 : HET ZOEKEN VAN EEN OPLOSSING

Van de mogelijke afwijkingen die in artikel 26, lid 1, zijn uiteengezet lijkt alleen a) - toestemming van de betrokkene - te kunnen worden gebruikt. Afwijking b) - doorgiften die noodzakelijk zijn voor de uitvoering van een overeenkomst - is niet van toepassing, omdat de doorgevende partij, het bureau voor kredietrefenties in het VK, geen overeenkomst met de betrokkene heeft ondertekend. Ook kan moeilijk worden aangevoerd dat de doorgifte noodzakelijk is op basis van een overeenkomst "in het belang van de betrokkene"(afwijking c)).

Toestemming van de betrokkene lijkt evenwel een relatief eenvoudige oplossing voor het probleem. De toestemming kan hetzij rechtstreeks door het bureau voor kredietreferenties in het VK worden verkregen hetzij indirect namens het Britse bureau door de financiële instelling in land A die op de leningaanvraag om toestemming kan verzoeken. Hoe dan ook moet de betrokkene in ieder geval in kennis worden gesteld van het risico dat voortvloeit uit de doorgifte van zijn gegevens aan een land dat geen passend beschermingsniveau biedt.

Daar dit soort doorgiften nog relatief weinig voorkomen, is het per geval vragen om toestemming waarschijnlijk de meest praktische oplossing. Als kredietrapportbureaus en kredietreferentiebureaus in verschillende landen echter vaker gegevens gaan uitwisselen, zouden andere regelingen kunnen worden uitgewerkt, zoals contractuele oplossingen of een internationale gedragscode.

CASESTUDY (2) : Doorgifte van gevoelige gegevens in de luchtvaartsector

Een Portugees burger reserveert bij een reisbureau in Lissabon een vlucht met een luchtvaartmaatschappij van land B. De verzamelde gegevens bevatten onder andere de informatie dat de betrokkene gehandicapt is en een rolstoel gebruikt. De gegevens worden ingevoerd in een internationaal geautomatiseerd reserveringssysteem vanwaar zij door de luchtvaartmaatschappij in haar passagiersgegevensbank in land B worden gedownload. Hier blijven de gegevens voor onbepaalde tijd opgeslagen. De luchtvaartmaatschappij wil de gegevens gebruiken voor een betere dienstverlening aan de passagier, mocht hij in de toekomst opnieuw met dezelfde maatschappij vliegen, en voor de interne bedrijfsplanning. [20]

STAP 1 : BEOORDELING VAN HET BESCHERMINGSNIVEAU

Wetten en voorschriften die van toepassing zijn

Hoewel op de gegevens in het geautomatiseerde reserveringssysteem een internationale gedragscode van toepassing is, zijn er geen voorschriften inzake de bescherming van de gegevens in de eigen gegevensbank van de luchtvaartmaatschappij in land B.

Beoordeling van de inhoud van de toepasselijke wetten en voorschriften

Er zijn geen wetten en voorschriften van toepassing.

Beoordeling van de doeltreffendheid van de bescherming

Niet van toepassing.

Oordeel

Het beschermingsniveau in land B kan niet als passend worden beschouwd, met name niet gezien de gevoeligheid van de betrokken gegevens.

STAP 2 : HET ZOEKEN VAN EEN OPLOSSING

De doorgifte van de gegevens naar het geautomatiseerd reserveringssysteem en gebruik van deze gegevens door de luchtvaartmaatschappij voor het verlenen van de gewenste dienst aan de gehandicapte passagier tijdens de betrokken vlucht zijn noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de luchtvaartmaatschappij (artikel 26, lid 1, onder b)). De langdurige opslag van de gegevens (met inbegrip van gevoelige gegevens over de gezondheid van de betrokkene) in de gegevensbank van de luchtvaartmaatschappij kan evenwel niet op grond van deze argumenten worden gerechtvaardigd. Voor de doorgifte van gegevens

[20] Dit geval vertoont bepaalde overeenkomsten met een reëel geval dat zich in verband met de Zweedse wetgeving heeft voorgedaan en waarbij Amerikaanse luchtvaartmaatschappijen en Lufthansa betrokken zijn. Deze zaak is nog in beroep.

naar de luchtvaartmaatschappij moet dus een andere afwijkingsbepaling worden gebruikt.

Net als bij casestudy (1), lijkt toestemming van de betrokkene de beste oplossing. De toestemming kan namens de luchtvaartmaatschappij door het reisbureau in Lissabon worden verkregen. De betrokkene dient te worden gewezen op de risico's in verband met de opslag van de gegevens in land B en op het feit dat het voor de specifieke vlucht waarvoor de reservering geldt niet noodzakelijk is dat de gegevens worden doorgegeven naar en opgeslagen in de eigen gegevensbank van de luchtvaartmaatschappij.

CASESTUDY (3) : Doorgifte van lijsten voor marketingdoeleinden

Een Nederlands bedrijf is gespecialiseerd in het opstellen van mailing-lists. Het gebruikt daarvoor een grote verscheidenheid van informatiebronnen die in Nederland voor het publiek beschikbaar zijn, alsmede klantenlijsten die het van verscheidene andere Nederlandse ondernemingen huurt. De aldus opgestelde lijsten zouden dan personen omvatten die aan een bepaald sociaal-economisch profiel beantwoorden. Deze lijsten worden door het Nederlandse bedrijf verkocht aan andere ondernemingen, niet alleen in Nederland en de EU, maar ook in een groot aantal andere derde landen. De ondernemingen die de lijsten (met postadressen, telefoonnummers en vaak ook e-mailadressen) kopen, gebruiken deze om de personen op de lijsten te benaderen met het oog op de verkoop van de meest uiteenlopende producten en diensten. Een groot aantal personen die op de lijsten voorkomen, hebben bij het Nederlandse orgaan voor gegevensbescherming over deze benaderingen voor marketingdoeleinden geklaagd.

STAP 1 : BEOORDELING VAN HET BESCHERMINGSNIVEAU

Wetten en voorschriften die van toepassing zijn

Sommige ondernemingen die de door het Nederlands bedrijf aangeboden mailing-lists kopen, zijn gevestigd in landen waar een algemene regelgeving betreffende de gegevensbescherming van kracht is en waar betrokkenen het recht hebben aan te geven dat zij niet van dergelijke marketingcontacten gediend zijn. Andere ondernemingen bevinden zich in landen waar deze kwestie niet is geregeld, maar zijn lid van zelfregulerende organisaties die een gedragscode op het gebied van de gegevensbescherming hebben aangenomen. Op weer andere is geen enkele regeling van toepassing.

Beoordeling van de inhoud van de toepasselijke wetten en voorschriften

Dit specifieke geval zou de beoordeling van een groot aantal verschillende wetten en voorschriften vereisen. Als het in Nederland gevestigde bedrijf ook verder zijn lijsten blijft verkopen of verhuren aan ondernemingen in alle landen van de wereld, is het onvermijdelijk dat het beschermingsniveau niet altijd passend zal zijn.

STAP 2 : HET ZOEKEN VAN EEN OPLOSSING

Aangezien de gegevens in dit geval worden verzameld uit publieke bronnen en zonder rechtstreeks contact met de betrokkene is het voor het Nederlands bedrijf zeer problematisch om van elke betrokkene afzonderlijk toestemming te verkrijgen voor opname op de mailing-lists. Om deze reden zal waarschijnlijk geen beroep kunnen worden gedaan op de afwijkingen van artikel 26, lid 1.

Het Nederlands bedrijf beschikt over twee mogelijkheden die afzonderlijk of in combinatie met elkaar kunnen worden gebruikt. Ten eerste kan het zijn handel in mailing-lists beperken tot ondernemingen die gehouden zijn aan wetten of doeltreffende zelfregeluringsinstrumenten, zodat een passend beschermingsniveau kan worden gewaarborgd. Bij de beslissing hiertoe kan het bedrijf zich laten leiden door een "witte lijst".

De tweede mogelijkheid bestaat erin dat het van al zijn klanten (of in ieder geval van die in gebieden zonder passend beschermingsniveau) verlangt dat deze zich contractueel verplichten tot een passende bescherming van de doorgegeven gegevens. Deze contractuele regelingen dienen in overeenstemming te zijn met de richtsnoeren in hoofdstuk 4 van dit document. Bij deze regelingen moet er met name naar worden gestreefd dat het Nederlands bedrijf volgens de Nederlandse wet aansprakelijk blijft voor schendingen van de beginselen aangaande de gegevensbescherming ten gevolge van acties van een klant aan wie het de mailing-lists heeft doorgegeven.

Bij een goede tenuitvoerlegging zou een dergelijke contractuele oplossing ertoe kunnen bijdragen dat de feitelijke handelsbelemmering die het gevolg is van het gebrek aan passende gegevensbescherming in bepaalde derde landen, wordt weggenomen.

Gedaan te Brussel op 24 juli 1998

Voor de Groep

De voorzitter

P.J. HUSTINX