00062/10/NL
WP 173

Advies 3/2010 over het verantwoordingsbeginsel

Goedgekeurd op 13 juli 2010

SAMENVATTING EN TOELICHTING

EU-beginselen en -verplichtingen op het gebied van gegevensbescherming komen vaak onvoldoende tot uitdrukking in concrete interne maatregelen en praktijken. Zolang gegevensbescherming niet behoort tot de gedeelde waarden en praktijken binnen een organisatie, en er niet uitdrukkelijk verantwoordelijken voor worden aangewezen, blijven er aanzienlijke risico's bestaan voor een doeltreffende naleving, en zullen incidenten met betrekking tot gegevensbescherming zich naar alle waarschijnlijkheid blijven voordoen.

Om gegevensbescherming in de praktijk te bevorderen moet het regelgevingskader van de EU worden uitgebreid met aanvullende mechanismen. Het doel van dit advies is de Commissie te adviseren over de wijze waarop de richtlijn gegevensbescherming gewijzigd moet worden om het beoogde effect te bereiken. In dit advies wordt in het bijzonder een concreet voorstel gedaan voor een verantwoordingsbeginsel dat de voor de verwerking verantwoordelijken ertoe verplicht passende en doeltreffende maatregelen te nemen om te waarborgen dat de beginselen en verplichtingen die in de richtlijn zijn vastgelegd worden nageleefd en om op verzoek van de toezichthoudende autoriteiten aan te kunnen tonen dat dit het geval is. Dit moet ertoe bijdragen dat gegevensbescherming wordt vertaald van 'de theorie naar de praktijk' en moet de gegevensbeschermingsautoriteiten helpen bij de uitoefening van hun toezichthoudende en handhavende taken.

In het advies worden suggesties gedaan die ervoor moeten zorgen dat het verantwoordingsbeginsel enerzijds rechtszekerheid biedt en anderzijds differentiatie toestaat (d.w.z. dat het mogelijk moet zijn om de vaststelling van de concrete maatregelen die moeten worden genomen af te stemmen op de risico's die de verwerking en het soort te verwerken gegevens met zich brengen). Vervolgens wordt de invloed besproken die een dergelijk beginsel zou kunnen hebben op andere terreinen, met inbegrip van internationale doorgiften van gegevens, aanmeldingsvereisten, sancties, en op termijn ook de ontwikkeling van certificeringsprogramma's of keurmerken.

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

Opgericht bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

Gelet op artikel 29 en artikel 30, lid 1, onder a), en lid 3, van die richtlijn, en artikel 15, lid 3, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002,

Gelet op het reglement van orde van de Groep,

heeft het volgende advies goedgekeurd:

1. INLEIDING

1. Gegevensbescherming moet van 'de theorie naar de praktijk' worden vertaald. Wettelijke vereisten moeten worden omgezet in daadwerkelijke maatregelen ter bescherming van gegevens. Om gegevensbescherming in de praktijk te bevorderen moet het regelgevingskader van de EU worden uitgebreid met aanvullende mechanismen. In discussies over de toekomst van de Europese en mondiale kaders voor gegevensbescherming zijn op verantwoording gebaseerde mechanismen voorgesteld als een manier om voor de verwerking verantwoordelijken aan te moedigen praktische instrumenten voor doeltreffende gegevensbescherming ten uitvoer te leggen.

2. In haar document over de toekomst van privacy (*The Future of Privacy* – WP168) uit december 2009 stelde de Groep gegevensbescherming artikel 29 dat het huidige rechtskader er niet volledig in is geslaagd te waarborgen dat vereisten op het gebied van gegevensbescherming worden omgezet in doeltreffende mechanismen die leiden tot daadwerkelijke bescherming. Ter verbetering van deze situatie stelde de Groep gegevensbescherming artikel 29 voor dat de Commissie op verantwoording gebaseerde mechanismen in overweging zou nemen, met bijzondere nadruk op de mogelijkheid om een "verantwoordingsbeginsel" op te nemen in de herziene richtlijn gegevensbescherming.[1] Dit beginsel zou de rol van de voor verwerking

[1] "Om dit probleem aan te pakken zou het gepast zijn om in het allesomvattende kader een verantwoordingsbeginsel op te nemen. Dit beginsel zou voor de verwerking verantwoordelijken ertoe moeten verplichten de nodige maatregelen te nemen om te waarborgen dat de materiële beginselen en verplichtingen die zijn vastgelegd in de geldende richtlijn bij de verwerking van persoonsgegevens worden nageleefd. Een dergelijke bepaling kan de noodzaak versterken om beleid en mechanismen in te voeren waarmee gevolg wordt gegeven aan de materiële beginselen en verplichtingen die zijn neergelegd in de geldende richtlijn. Zij kan dienen ter versterking van de noodzaak om doeltreffende stappen te ondernemen die leiden tot een doeltreffende interne tenuitvoerlegging van de materiële verplichtingen en beginselen die momenteel zijn vervat in de richtlijn. Daarnaast zou het verantwoordingsbeginsel voor de verwerking verantwoordelijken ertoe moeten verplichten de noodzakelijke interne mechanismen in te voeren om naleving te bewijzen aan externe belanghebbenden, met inbegrip van nationale gegevensbeschermingsautoriteiten. De daaruit voortvloeiende noodzaak om bewijs te leveren van toereikende maatregelen om de naleving te waarborgen zal de handhaving van de geldende regels aanzienlijk vergemakkelijken" (WP 168, punt 79. Zie voor meer informatie ook de punten 74-78).

verantwoordelijke moeten versterken en zijn verantwoordelijkheid moeten vergroten.

3. In een notendop zou een wettelijk verantwoordingsbeginsel de voor de verwerking verantwoordelijken er uitdrukkelijk toe verplichten passende en doeltreffende maatregelen ten uitvoer te leggen om gevolg te geven aan de beginselen en verplichtingen uit de richtlijn en om dit op verzoek aan te kunnen tonen. In de praktijk zou dit zich moeten vertalen in differentieerbare programma's gericht op de tenuitvoerlegging van de bestaande beginselen voor gegevensbescherming (ook wel 'nalevingsprogramma's' genoemd). Om het beginsel te vervolmaken zouden specifieke aanvullende eisen kunnen worden gesteld die tot doel hebben waarborgen voor gegevensbescherming te realiseren of de doeltreffendheid van dergelijke waarborgen te verzekeren. Een voorbeeld zou een bepaling kunnen zijn waarin de eis wordt vastgelegd dat er een privacy-effectbeoordeling moet worden uitgevoerd voorafgaand aan verwerkingen die een hoger risico met zich brengen.

4. Met dit advies wordt beoogd voort te bouwen op de vorige bijdrage van de Groep gegevensbescherming artikel 29 over dit onderwerp, in het document over de toekomst van privacy, teneinde de Commissie te adviseren bij haar lopende herziening van Richtlijn 95/46. Daarom is dit advies onderverdeeld in vier delen: in het eerste wordt besproken dat de voor de verwerking verantwoordelijken hun praktische interne regelingen (beleid en procedures) dienen te versterken om te waarborgen dat verwerking altijd geschiedt overeenkomstig de geldende regels. Daarnaast wordt ingegaan op de wijze waarop op verantwoording gebaseerde systemen aan de verwezenlijking van dit doel kunnen bijdragen. Vervolgens wordt bekeken hoe de juridische structuur van een op verantwoording gebaseerd systeem eruit zou kunnen zien en komen precedenten op het gebied van gegevensbescherming en andere terreinen aan de orde. In het tweede deel wordt een concreet voorstel gedaan voor een verantwoordingsbeginsel en wordt de *ratio legis* van de verschillende aspecten van het voorstel uiteengezet. In het derde deel worden diverse elementen besproken die verband houden met een rechtsstelsel waarin een algemeen verantwoordingssysteem is geïntegreerd. Hierin wordt onder meer besproken dat een dergelijk voorstel rechtszekerheid moet bieden, terwijl het tegelijkertijd zo ruim geformuleerd moet zijn dat differentiatie mogelijk is (d.w.z. dat het mogelijk moet zijn om de vaststelling van de concrete maatregelen die moeten worden genomen en de verificatiemethoden die moeten worden toegepast, af te stemmen op de risico's die de verwerking en het soort te verwerken gegevens met zich brengen). Vervolgens worden aanverwante kwesties besproken, zoals de relatie met internationale doorgiften, wordt het voordeel geschetst dat een op verantwoording gebaseerd mechanisme zou opleveren voor gegevensbeschermingsautoriteiten, en wordt ingegaan op de rol die certificering zou kunnen spelen.

II. VERANTWOORDING: DOELEN, JURIDISCHE STRUCTUUR, PRECEDENTEN EN TERMINOLOGIE

II.1 Verantwoording als drijvende kracht achter de doeltreffende tenuitvoerlegging van de beginselen voor gegevensbescherming

5. Het wordt voor de voor verwerking verantwoordelijken tegenwoordig steeds noodzakelijker en belangrijker om te waarborgen dat zij doeltreffende maatregelen nemen om gegevens daadwerkelijk te beschermen. Hiervoor bestaan diverse redenen, die hieronder nader zullen worden besproken.

6. Ten eerste is er sprake van een zogenaamd *'data deluge*'-effect. Dit houdt in dat de hoeveelheid persoonsgegevens die beschikbaar is, wordt verwerkt en wordt doorgegeven, blijft groeien. Dit fenomeen wordt versterkt door zowel technologische ontwikkelingen, d.w.z. de groei van informatie- en communicatiesystemen, als door het feit dat individuen steeds beter in staat zijn gebruik te maken van en te reageren op technologieën. Naarmate er meer gegevens beschikbaar zijn en mondiaal worden uitgewisseld, neemt ook het risico toe dat er inbreuk wordt gemaakt op die gegevens. Dit onderstreept nog eens hoe noodzakelijk het is dat voor de verwerking verantwoordelijken, zowel in de publieke als in de private sector, concrete en doeltreffende interne mechanismen ten uitvoer leggen om de bescherming van de informatie van individuen te waarborgen.

7. Ten tweede gaat de almaar toenemende hoeveelheid persoonlijke informatie gepaard met een waardestijging van die informatie in sociaal, politiek en economisch opzicht. In bepaalde sectoren, met name in onlineomgevingen, zijn persoonsgegevens *de facto* een betaalmiddel geworden voor toegang tot onlinecontent. Tegelijkertijd wordt aan gegevensbescherming vanuit maatschappelijk oogpunt in toenemende mate sociale waarde toegekend. Kortom, naarmate persoonlijke informatie waardevoller wordt voor de voor de verwerking verantwoordelijken in alle sectoren, worden burgers, consumenten en de maatschappij als geheel zich ook steeds bewuster van het belang ervan. Dit versterkt op zijn beurt de noodzaak om strikte maatregelen ten uitvoer te leggen ter bescherming van deze informatie.

8. Tot slot volgt uit het bovenstaande dat inbreuken op persoonlijke informatie ernstige negatieve gevolgen kunnen hebben voor de voor de verwerking verantwoordelijken in de publieke en private sector. Eventuele storingen in applicaties voor eOverheid of eGezondheid zullen verwoestende gevolgen hebben, in economisch opzicht maar vooral ook op het vlak van reputatie. Het minimaliseren van risico's, het opbouwen en behouden van een goede reputatie, en het garanderen van het vertrouwen van burgers en consumenten worden cruciaal met betrekking tot voor de verwerking verantwoordelijken in alle sectoren.

9. Kortom, uit het bovenstaande blijkt dat het absoluut noodzakelijk is dat de voor de verwerking verantwoordelijken concrete en doeltreffende maatregelen ter bescherming van gegevens ten uitvoer leggen. Deze maatregelen dienen gericht te zijn op een goed beheer op het terrein van gegevensbescherming en moeten de

juridische, economische en reputatierisico's die het gevolg zijn van tekortschietende praktijken op het gebied van gegevensbescherming minimaliseren. Zoals hieronder verder zal worden uitgewerkt, wordt met op verantwoording gebaseerde mechanismen beoogd deze doelen te verwezenlijken.

II.2 Mogelijke algemene juridische structuur van op verantwoording gebaseerde mechanismen

10. Een relevant punt dat in dit verband moet worden besproken is de manier waarop het rechtskader de voor de verwerking verantwoordelijken ertoe zou kunnen aanzetten maatregelen te nemen die in de praktijk leiden tot daadwerkelijke bescherming. Met andere woorden: hoe zou de juridische structuur van op verantwoording gebaseerde systemen eruit moeten zien?

11. Ter inleiding op de bespreking van een dergelijke structuur moet worden benadrukt dat dergelijke systemen in beginsel op geen enkele wijze verandering aanbrengen in of van invloed zijn op de materiële beginselen voor gegevensbescherming; zij zijn slechts bedoeld om deze beginselen beter te laten werken.

12. Een manier om voor de verwerking verantwoordelijken ertoe aan te zetten dergelijke maatregelen in te voeren zou kunnen zijn het verantwoordingsbeginsel een plaats te geven in de herziene versie van de richtlijn. De verwachte effecten van een dergelijke bepaling zijn onder meer dat er interne maatregelen en procedures ten uitvoer worden gelegd om gevolg te geven aan bestaande beginselen voor gegevensbescherming en de doeltreffendheid van die beginselen te waarborgen, alsmede de verplichting om de tenuitvoerlegging op verzoek van de gegevensbeschermingsautoriteiten aan te tonen. Zoals hieronder nader zal worden omschreven, kan het soort procedures en mechanismen variëren naar gelang de risico's die de verwerking en de aard van de gegevens met zich brengen.

13. Naast het bovenstaande zou kunnen worden nagedacht over specifieke eisen, zoals de verplichting om in bepaalde gevallen privacy-effectbeoordelingen uit te voeren of om functionarissen voor gegevensbescherming aan te stellen. Dergelijke specifieke eisen zouden een aanvulling kunnen vormen op het algemene verantwoordingsbeginsel.

14. De Groep gegevensbescherming artikel 29 onderkent dat voor de verwerking verantwoordelijken wellicht beleid en procedures ten uitvoer willen leggen die strikt genomen niet zijn voorzien in de wetgeving betreffende gegevensbescherming. Zo kan een voor de verwerking verantwoordelijke zichzelf er bijvoorbeeld toe willen verplichten zeer snel te reageren op verzoeken om toegang, ook al biedt de wetgeving enige flexibiliteit. Ook kan een dergelijke verantwoordelijke zichzelf ertoe willen verplichten tegelijkertijd on- en offline te reageren op verzoeken om toegang om de onmiddellijke en doeltreffende ontvangst van dergelijke verzoeken te verzekeren. Daarnaast zijn er situaties denkbaar waarin de voor de verwerking verantwoordelijke verder wil gaan dan de minimumvereisten die zijn vervat in het algemene rechtskader. Een voor de verwerking verantwoordelijke kan bijvoorbeeld beslissen een functionaris voor

gegevensbescherming aan te stellen hoewel hij daartoe op grond van de geldende wetgeving niet verplicht is. Een voor de verwerking verantwoordelijke kan ook een derde willen inhuren voor de uitvoering van een evaluatie van zijn *totale* gegevensverwerking om te beoordelen of die geschiedt overeenkomstig het rechtskader voor gegevensbescherming. De Groep gegevensbescherming artikel 29 juicht deze initiatieven toe en beveelt aan dat in het nieuwe rechtskader voor gegevensverwerking prikkels worden opgenomen voor de voor de verwerking verantwoordelijken om dergelijke initiatieven te ontplooien.

15. Overeenkomstig het bovenstaande zijn in de 'juridische structuur' van de verantwoordingsmechanismen twee niveaus voorzien: het eerste niveau zou worden gevormd door een basale wettelijke verplichting die bindend is voor *alle* voor de verwerking verantwoordelijken. Inhoudelijk omvat deze verplichting twee elementen: de tenuitvoerlegging van maatregelen/procedures, en het bewaren van bewijs van de tenuitvoerlegging. Dit eerste niveau kan worden aangevuld met specifieke eisen. Een tweede niveau zou worden gevormd door vrijwillige verantwoordingssystemen die verder gaan dan de wettelijke minimumeisen ten aanzien van de onderliggende beginselen voor gegevensverwerking (door betere bescherming te bieden dan op grond van de geldende regels verplicht is) en/of ten aanzien van de wijze waarop de maatregelen ten uitvoer worden gelegd of waarop de doeltreffendheid van de maatregelen wordt gewaarborgd (invoering van eisen die boven het minimumniveau liggen). Hoewel het belang en de voordelen van vrijwillige systemen worden onderkend, zal in dit advies met name worden ingegaan op het eerste niveau, in het bijzonder op het algemene verantwoordingsbeginsel.

II.3 Het verantwoordingsbeginsel op het terrein van gegevensbescherming en andere terreinen en terminologie

Precedenten

16. De Groep gegevensbescherming artikel 29 merkt op dat het verantwoordingsbeginsel op zich niet nieuw is. In de privacyrichtsnoeren die in 1980 zijn vastgesteld door de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) wordt het beginsel uitdrukkelijk erkend. Het verantwoordingsbeginsel is daarin als volgt geformuleerd: “Een voor de verwerking verantwoordelijke moet verantwoording kunnen afleggen over de naleving van maatregelen waarmee gevolg wordt gegeven aan bovenstaande [materiële] beginselen”.

17. Het beginsel is onlangs uitdrukkelijk vastgelegd in de door de Internationale Conferentie van commissarissen voor de bescherming van gegevens en de privacy ontwikkelde internationale normen die zijn neergelegd in de Verklaring van Madrid.[2] Daarnaast maakt het beginsel deel uit van de nog recentere ontwerp-ISO-norm 29100 tot vaststelling van een privacykader en is het een van de

[2] De verantwoordelijke: “a. neemt alle noodzakelijke maatregelen om de beginselen en verplichtingen die in dit Document en in de geldende nationale wetgeving zijn vastgelegd na te leven, en b. beschikt over de noodzakelijke interne mechanismen om die naleving te bewijzen aan zowel betrokkenen als toezichthoudende autoriteiten die optreden overeenkomstig hun bevoegdheden, zoals bepaald in artikel 23.”

voornaamste concepten in het privacykader van de Economische Samenwerking Azië-Stille Oceaan (APEC) en haar grensoverschrijdende privacyregels.[3]

18. Als het om wetgeving gaat, wijst de Groep gegevensbescherming artikel 29 erop dat verantwoording deel uitmaakt van de Canadese beginselen betreffende eerlijke informatie die zijn vastgelegd in de *Personal Information Protection and Electronic Documents Act* (Wet bescherming persoonlijke informatie en elektronische documenten). Het eerste van die beginselen vereist onder meer de ontwikkeling en tenuitvoerlegging van beleid en praktijken om gevolg te geven aan de tien beginselen van eerlijke informatie, waaronder de tenuitvoerlegging van procedures ter bescherming van persoonlijke informatie en de vaststelling van procedures voor het ontvangen van en het reageren op klachten en vragen.

19. In aanvulling op het bovenstaande merkt de Groep gegevensbescherming artikel 29 op dat het verantwoordingsbeginsel ook tot uitdrukking komt in zogenaamde Binding Corporate Rules (bindende bedrijfsregels – BCR's), die gebruikt worden in verband met internationale doorgiften van gegevens. BCR's zijn immers praktijkrichtlijnen die door multinationale organisaties worden opgesteld en gevolgd en waarin interne maatregelen worden vastgelegd die bedoeld zijn om gevolg te geven aan beginselen voor gegevensbescherming (het gaat onder meer om audits, opleidingsprogramma's, netwerken van privacyfunctionarissen, systemen voor de afhandeling van klachten). Wanneer BCR's door nationale gegevensbeschermingsautoriteiten zijn geëvalueerd, worden zij geacht voldoende waarborgen te bieden voor doorgiften of categorieën doorgiften van persoonsgegevens tussen de ondernemingen die deel uitmaken van hetzelfde moederbedrijf en die gebonden zijn aan deze bedrijfsregels uit hoofde van de artikelen 25 en 26, lid 2 van Richtlijn 95/46.

20. Behalve op het terrein van de gegevensbescherming zijn ook daarbuiten enkele voorbeelden van verantwoording te vinden, in de vorm van programma's waarin het beleid en de procedures van een voor de verwerking verantwoordelijke zijn vastgelegd om de naleving van wet- en regelgeving te waarborgen. Zo zijn nalevingsprogramma's bijvoorbeeld verplicht op grond van verordeningen inzake financiële diensten. In andere gevallen zijn nalevingsprogramma's niet verplicht maar worden zij aangemoedigd, zoals op het terrein van het mededingingsrecht. In Canada heeft de mededingingscommissaris bijvoorbeeld gedetailleerd beleid opgesteld over nalevingsprogramma's voor bedrijven. Bedrijven besluiten vrijwillig of zij een programma al dan niet willen toepassen. Wel benadrukt de Canadese mededingingscommissaris het belang van nalevingsprogramma's als instrument om risico's te verkleinen en onderstreept hij de juridische, economische en reputatievoordelen[4].

---

[3] Daarnaast werkt het Centre for Information Policy Leadership aan een initiatief om de effecten van het verantwoordingsbeginsel te onderzoeken met betrekking tot gegevensbescherming en privacy. Zie: www.informationpolicycentre.com

[4] www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

Terminologie

21. De term "*accountability*" is afkomstig uit de Angelsaksische wereld, waar deze veel wordt gebruikt en er brede overeenstemming bestaat over de betekenis ervan – ook al is het ingewikkeld om exact te definiëren wat "*accountability*" in de praktijk inhoudt. Toch kan in algemene zin worden gesteld dat de nadruk ligt op het inzichtelijk maken van de manier waarop verantwoordelijkheden worden uitgeoefend en het controleerbaar maken daarvan. Verantwoordelijkheid en verantwoording zijn twee kanten van dezelfde medaille en beide zijn essentiële onderdelen van behoorlijk bestuur. Immers, alleen wanneer kan worden aangetoond dat verantwoordelijkheden in de praktijk doeltreffend worden uitgeoefend, kan er voldoende vertrouwen ontstaan.

22. Met name vanwege verschillen tussen rechtsstelsels is het niet eenvoudig de term "*accountability*" te vertalen in de andere Europese talen. Een gevolg hiervan is dat er een aanzienlijk risico bestaat dat de term verschillend zal worden uitgelegd, waardoor er een gebrek aan harmonisatie kan optreden. Andere woorden die zijn voorgesteld om de betekenis van "*accountability*" te omschrijven, zijn "*reinforced responsibility*" (versterkte verantwoordelijkheid), "*assurance*" (borging), "*reliability*" (betrouwbaarheid), "*trustworthiness*" (betrouwbaarheid) en in het Frans "*obligation de rendre des comptes*" (verantwoordingsplicht) enz. Er kan ook worden gesteld dat de term duidt op de "tenuitvoerlegging van beginselen voor gegevensbescherming".

23. In dit document richten we ons derhalve op de maatregelen die moeten worden genomen of ontwikkeld om naleving op het terrein van gegevensbescherming te waarborgen. De term "*accountability*", hier vertaald als "verantwoording", moet dan ook worden begrepen zoals de term in dit advies wordt gebruikt, onder voorbehoud van een eventuele andere term die het concept dat hier wordt bedoeld beter tot uitdrukking brengt. Daarom wordt in dit document niet specifiek gekeken naar de terminologie, maar wordt de aandacht pragmatisch gericht op de maatregelen die moeten worden genomen en niet zozeer op het concept als zodanig.

III. NAAR EEN VOORSTEL VOOR EEN ALGEMENE BEPALING OVER VERANTWOORDING

III.1 Een algemene bepaling ter bevestiging en versteviging van de verantwoordelijkheid van voor de verwerking verantwoordelijken

24. De Groep gegevensbescherming artikel 29 heeft, in het licht van de overwegingen die in deel I aan de orde zijn gekomen, van gedachten gewisseld over de mogelijkheid om op verantwoording gebaseerde oplossingen op te nemen in het nieuwe allesomvattende rechtskader voor gegevensbescherming.

25. Het resultaat hiervan is dat de Groep de zienswijze zoals die was verwoord in haar document over de toekomst van privacy heeft bevestigd, namelijk dat in een nieuw allesomvattend wetgevingskader een algemeen verantwoordingsbeginsel moet worden opgenomen. Een dergelijke bepaling moet tot doel hebben de

verantwoordelijkheid te bevestigen en te verstevigen die voor de verwerking verantwoordelijken dragen op het vlak van de verwerking van persoonsgegevens. Een dergelijke bepaling staat niet in de weg aan concrete verantwoordingsmaatregelen die een aanvulling op het beginsel kunnen vormen.

26. Deze nieuwe bepaling zou in overeenstemming zijn met specifieke bepalingen die al deel uitmaken van het huidige wetgevingskader. Er kan in het bijzonder worden gedacht aan artikel 6 van Richtlijn 95/46/EG. In lid 1 van dat artikel wordt immers verwezen naar beginselen die samenhangen met de kwaliteit van de gegevens en in lid 2 staat: "Op de voor de verwerking verantwoordelijke rust de plicht om voor de naleving van het bepaalde in lid 1 zorg te dragen". De bepaling zou ook overeenstemmen met artikel 17, lid 1, waarin is bepaald dat de voor de verwerking verantwoordelijken technische en organisatorische maatregelen ten uitvoer dienen te leggen. Een algemene bepaling over verantwoording zou ten aanzien van de voor de verwerking verantwoordelijken immers de noodzaak versterken om de beveiligingseisen uit artikel 17 ten uitvoer te leggen, in aanvulling op de eisen die worden gesteld in de overige bepalingen.

III.2 Naar een concreet voorstel voor een algemeen verantwoordingsbeginsel

27. De nieuwe bepaling zou tot doel hebben de goedkeuring van concrete en praktische maatregelen te bevorderen, door de algemene beginselen voor gegevensbescherming om te zetten in concreet beleid en concrete procedures die op het niveau van de voor de verwerking verantwoordelijke worden vastgesteld, in overeenstemming met de geldende wet- en regelgeving. De voor de verwerking verantwoordelijke moet daarnaast de doeltreffendheid van de genomen maatregelen waarborgen en op verzoek kunnen aantonen dat hij de betreffende maatregelen heeft genomen.

28. Schematisch weergegeven zouden in een dergelijke algemene bepaling twee aspecten worden benadrukt:

    (i) de noodzaak voor een voor de verwerking verantwoordelijke om passende en doeltreffende maatregelen te nemen teneinde de beginselen voor gegevensbescherming ten uitvoer te leggen;
    (ii) de noodzaak om op verzoek te kunnen aantonen dat er passende en doeltreffende maatregelen zijn genomen. De voor de verwerking verantwoordelijke moet derhalve bewijs kunnen overleggen van (i) hierboven.

29. De verplichting moet gelden voor alle voor de verwerking verantwoordelijken en in alle situaties.

30. Het eerste aspect van de verplichting houdt in dat voor de verwerking verantwoordelijken passende maatregelen ten uitvoer moeten leggen. Het soort maatregelen zou in de tekst van de algemene bepaling over verantwoording niet nader worden gespecificeerd. In latere richtsnoeren van nationale gegevensbeschermingsautoriteiten, de Groep gegevensbescherming artikel 29 of de Commissie (d.m.v. comitologieprocedures) zou voor bepaalde gevallen een minimum aan specifieke maatregelen kunnen worden vastgelegd die beschouwd worden als passende maatregelen. Een voorbeeld van dergelijke maatregelen kan

zijn dat er in bepaalde gevallen intern beleid en interne processen worden vastgesteld die noodzakelijk zijn om de beginselen voor gegevensbescherming ten uitvoer te leggen zoals die tot uitdrukking komen in geldende wet- en regelgeving.

31. De tenuitvoerlegging van deze maatregelen en processen kan ook op doeltreffende wijze worden gerealiseerd door verantwoordelijkheden toe te kennen en de medewerkers die betrokken zijn bij de verwerking op te leiden. De voor de verwerking verantwoordelijken zouden in het bijzonder, in overeenstemming met artikel 18 van de richtlijn, moeten worden aangemoedigd om functionarissen voor de bescherming van persoonsgegevens aan te stellen. In ieder geval moet worden aangemoedigd dat er op verschillende niveaus binnen een organisatie verantwoordelijkheid wordt toegekend om te waarborgen dat deze verantwoordelijkheden worden nagekomen.

32. Met betrekking tot doorgiften van persoonsgegevens aan landen buiten de Europese Unie moeten voor de verwerking verantwoordelijken passende maatregelen vaststellen en ten uitvoer leggen om te voldoen aan de eis dat zij "voldoende waarborgen" bieden, zoals is voorzien in artikel 26 van de richtlijn en zoals bij BCR's het geval moet zijn.

33. Voor de verwerking verantwoordelijken moeten verder waarborgen dat de praktische maatregelen die ten uitvoer worden gelegd om de beginselen voor gegevensbescherming na te leven, doeltreffend zijn. Als het gaat om verwerkingen die omvangrijker of ingewikkelder zijn of om verwerkingen die een hoog risico met zich brengen, moet de doeltreffendheid van de maatregelen regelmatig worden gecontroleerd. Er zijn verschillende manieren om de doeltreffendheid (of ondoeltreffendheid) van de maatregelen te beoordelen: monitoring, interne en externe audits, enz.

34. Met inachtneming van bovenstaande opmerkingen heeft de Groep gegevensbescherming artikel 29 de formulering overwogen van een concrete bepaling die zou kunnen worden opgenomen in een allesomvattend wetgevingskader. Een dergelijke bepaling zou als volgt kunnen luiden:

"Artikel X – Tenuitvoerlegging van beginselen voor gegevensbescherming

1. De voor de verwerking verantwoordelijke legt passende en doeltreffende maatregelen ten uitvoer om te waarborgen dat de in de richtlijn vastgelegde beginselen en verplichtingen worden nageleefd.
2 De voor de verwerking verantwoordelijke toont op verzoek van de toezichthoudende autoriteit aan dat lid 1 wordt nageleefd."

IV. BESPREKING VAN DIVERSE ASPECTEN DIE VERBAND HOUDEN MET HET ALGEMENE VERANTWOORDINGSBEGINSEL

IV.1 Versteviging van bestaande verplichtingen

35. De Groep gegevensbescherming artikel 29 merkt op dat er voor de verwerking verantwoordelijken kunnen zijn die van mening zijn dat het algemene

verantwoordingsbeginsel betekent dat zij worden geconfronteerd met nieuwe belastende juridische verplichtingen, in het bijzonder met het oog de actuele, uitdagende economische situatie in de EU. Dit zou echter onterecht zijn.

36. De Groep gegevensbescherming artikel 29 benadrukt dat het merendeel van de eisen die in deze nieuwe bepaling zijn vastgelegd in werkelijkheid – zij het minder uitdrukkelijk – reeds deel uitmaakt van bestaande wetgeving. Op grond van het bestaande rechtskader zijn de voor de verwerking verantwoordelijken immers al verplicht de beginselen en verplichtingen die zijn vastgelegd in de richtlijn na te leven. Die naleving kan onmogelijk worden gerealiseerd zonder de noodzakelijke procedures op het gebied van gegevensbescherming te ontwikkelen en eventueel te controleren. Zo bezien houdt een bepaling over verantwoording geen grote vernieuwing in en doorgaans vloeien uit de bepaling dan ook geen verplichtingen voort die niet al impliciet aanwezig waren in de bestaande wetgeving. Kortom, de nieuwe bepaling heeft niet tot doel de voor de verwerking verantwoordelijken met nieuwe beginselen te confronteren, maar veeleer om de doeltreffende naleving van bestaande beginselen in de praktijk te waarborgen.

37. In feite heeft zich in 2009 een enigszins vergelijkbare wetgevingsontwikkeling voorgedaan bij de wijziging van Richtlijn 2002/58.[5] In dit geval bevat de wetgeving de verplichting om een beveiligingsbeleid in te voeren: "*een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens"*. De wetgever heeft dus met betrekking tot de beveiligingsbepalingen van die richtlijn besloten dat het noodzakelijk was om uitdrukkelijk te eisen dat er een beveiligingsbeleid werd ingevoerd en ten uitvoer gelegd. Bovendien kunnen in artikel 18 van Richtlijn 95/46, waarin wordt verwezen naar de aanwijzing van functionarissen voor de gegevensbescherming, alsmede naar het hierboven genoemde systeem van bindende bedrijfsregels, al voorbeelden worden gevonden van praktische maatregelen die voor de verwerking verantwoordelijken kunnen nemen.

38. Een kwestie die verband houdt met het bovenstaande betreft de gevolgen die worden verbonden aan de naleving (of niet-naleving) van het verantwoordingsbeginsel. De Groep gegevensbescherming artikel 29 benadrukt dat wanneer wordt voldaan aan het verantwoordingsbeginsel dit niet automatisch betekent dat een voor de verwerking verantwoordelijke ook de materiële beginselen naleeft die in de richtlijn zijn vastgelegd, d.w.z. dat hieruit geen wettelijk vermoeden van naleving voortvloeit noch dat het verantwoordingsbeginsel deze beginselen vervangt. Een voor de verwerking verantwoordelijke kan de maatregelen die hij heeft vastgesteld ten uitvoer hebben gelegd en gecontroleerd en toch onrechtmatig handelen. De vaststelling van maatregelen die bedoeld zijn om de beginselen na te leven mag er dan ook in geen geval toe leiden dat gegevensbeschermingsautoriteiten verzuimen

---

5 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.

handhavingsmaatregelen te treffen tegen voor de verwerking verantwoordelijken. Wel zal het in de praktijk vaak zo zijn dat voor de verwerking verantwoordelijken in de publieke en private sector die hun maatregelen hebben vastgelegd in robuuste nalevingsprogramma's, zich aan de wetgeving houden. Zij hebben immers doeltreffende maatregelen genomen die erop zijn gericht de materiële beginselen voor gegevensbescherming na te leven en hierdoor zou de kans dat zij inbreuk maken op de wetgeving moeten afnemen. Daarom zouden gegevensbeschermingsautoriteiten bij de vaststelling van sancties in verband met de schending van gegevensbescherming, gewicht kunnen toekennen aan de tenuitvoerlegging van maatregelen (of het ontbreken daarvan) en de controle daarop.

IV.2 Passende maatregelen voor de tenuitvoerlegging van de bepalingen in de richtlijn

39. Een bepaling over verantwoording zou voor de verwerking verantwoordelijken ertoe moeten verplichten de noodzakelijke maatregelen vast te stellen en ten uitvoer te leggen om de naleving van de beginselen en verplichtingen uit de richtlijn te waarborgen en om hun doeltreffendheid periodiek te laten controleren.

40. In het voorstel voor een algemeen verantwoordingsbeginsel wordt doelbewust vermeden in detail het soort maatregelen vast te leggen dat ten uitvoer moet worden gelegd. Dit doet twee onderling met elkaar verbonden vragen rijzen: *(i)* welke gemeenschappelijke maatregelen zouden voldoen aan het verantwoordingsbeginsel? *(ii)* hoe kunnen de maatregelen worden gedifferentieerd en afgestemd op specifieke omstandigheden?

De maatregelen: voorbeelden

41. De Groep gegevensbescherming artikel 29 is van mening dat onderstaande niet-uitputtende lijst voorbeelden geeft van gemeenschappelijke verantwoordingsmaatregelen:

- het vaststellen van interne procedures *voordat* nieuwe verwerkingen van persoonsgegevens worden ontwikkeld (interne evaluatie, beoordeling, enz.);[6]
- het opstellen van schriftelijk en bindend beleid betreffende gegevensbescherming dat in aanmerking moet worden genomen bij en toegepast op nieuwe verwerkingen van gegevens (bv. naleving van de gegevenskwaliteit, aanmelding, beveiligingsbeginselen, toegang, enz.), en dat beschikbaar moet zijn voor betrokkenen;
- het in kaart brengen van procedures om de juiste identificatie van alle gegevensverwerkingen te waarborgen en het inventariseren van gegevensverwerkingen;
- het aanstellen van een functionaris voor gegevensbescherming en anderen die verantwoordelijkheid dragen voor gegevensbescherming;
- het aanbieden van voldoende opleiding en voorlichting aan medewerkers met betrekking tot gegevensbescherming. Het gaat dan onder meer om

[6] Voor bestaande verwerkingen zou een overgangsperiode moeten gelden waarin zij in overeenstemming kunnen worden gebracht met de wetgeving.

medewerkers die de persoonsgegevens verwerken of daarvoor verantwoordelijk zijn (zoals personeelschefs) maar ook om IT-beheerders, ontwikkelaars en hoofden van bedrijfsonderdelen. Er moeten voldoende middelen worden toegewezen voor privacybeheer, enz;

- het ontwikkelen van voor betrokkenen transparante procedures voor het beheer van verzoeken om toegang tot en correctie en verwijdering van gegevens;
- het vaststellen van een intern mechanisme voor de afhandeling van klachten;
- het ontwikkelen van interne procedures voor het doeltreffend beheren en rapporteren van inbreuken op de beveiliging;
- het uitvoeren van privacy-effectbeoordelingen in specifieke omstandigheden;
- het ten uitvoer leggen van en toezicht houden op controleprocedures om te waarborgen dat alle maatregelen niet alleen op papier bestaan, maar ook ten uitvoer worden gelegd en in de praktijk functioneren (interne of externe audits, enz.).

42. Denkbaar is ook een complementaire benadering die een aanvulling vormt op het algemene verantwoordingsbeginsel. In een dergelijke benadering zou het rechtskader niet alleen een algemeen verantwoordingsbeginsel omvatten, maar ook een lijst met voorbeelden van maatregelen die op nationaal niveau kunnen worden aangemoedigd[7]. De bepaling zou een niet-uitputtende lijst met voorbeeldmaatregelen kunnen omvatten die voor de verwerking

---

[7] De internationale normen die gegevensbeschermingsautoriteiten in Madrid hebben vastgesteld bevatten in artikel 22 bis bijvoorbeeld een bepaling over proactieve maatregelen. De bepaling luidt als volgt: "*Staten stimuleren degenen die in elke fase van de verwerking bij de verwerking betrokken zijn om, door middel van hun nationaal recht, maatregelen ten uitvoer te leggen ter bevordering van een betere naleving van geldende wetgeving betreffende de bescherming van privacy bij de verwerking van persoonsgegevens. Zulke maatregelen kunnen onder andere bestaan in:*

a) de tenuitvoerlegging van procedures om inbreuken te voorkomen en op te sporen, die gebaseerd kunnen worden op gestandaardiseerde modellen voor het beleid en/of het beheer inzake informatiebeveiliging;

b) de aanstelling van één of meer functionarissen voor gegevensbescherming of privacy, die beschikken over voldoende kwalificaties, middelen en bevoegdheden om hun toezichthoudende functies naar behoren uit te oefenen;

c) de periodieke tenuitvoerlegging van opleidings-, voorlichtings- en bewustwordingsprogramma's bedoeld voor leden van de organisatie gericht op de ontwikkeling van kennis van de geldende wetgeving betreffende de bescherming van privacy bij de verwerking van persoonsgegevens, alsmede van de procedures die de organisatie voor dat doeleinde heeft vastgesteld;

d) de periodieke uitvoering van transparante audits door gekwalificeerde en bij voorkeur onafhankelijke partijen om te controleren of de geldende wetgeving betreffende de bescherming van privacy bij de verwerking van persoonsgegevens en de procedures die de organisatie voor dat doeleinde heeft vastgesteld worden nageleefd;

e) de aanpassing van informatiesystemen en/of technologie voor de verwerking van persoonsgegevens aan de geldende wetgeving betreffende de bescherming van privacy bij de verwerking van persoonsgegevens, in het bijzonder wanneer besluiten worden genomen over technische specificaties en de ontwikkeling en tenuitvoerlegging ervan;

f) de tenuitvoerlegging van privacy-effectbeoordelingen voorafgaand aan de invoering van nieuwe informatiesystemen en/of technologie voor de verwerking van persoonsgegevens, alsmede voorafgaand aan de uitvoering van nieuwe verwerkingsmethoden voor persoonsgegevens of substantiële wijzigingen in de bestaande verwerking;.

g) de goedkeuring van bindende praktijkrichtlijnen die elementen bevatten die het mogelijk maken de doelmatigheid ervan te meten voor de naleving en het beschermingsniveau van persoonsgegevens, en die doeltreffende maatregelen omvatten in geval van niet-naleving;

h) de tenuitvoerlegging van een reactieplan dat richtsnoeren omvat met betrekking tot de maatregelen die moeten worden genomen wanneer er een inbreuk wordt geconstateerd op de geldende wetgeving betreffende de bescherming van privacy bij de verwerking van persoonsgegevens en dat ten minste de verplichting bevat om de oorzaak en omvang van de inbreuk vast te stellen, de schadelijke effecten ervan te omschrijven en passende maatregelen te nemen om verdere inbreuken te voorkomen."

verantwoordelijken zouden kunnen nemen. Op die manier zou de bepaling houvast kunnen bieden aan voor de verwerking verantwoordelijken met betrekking tot de vraag wat, in een specifiek geval, de passende maatregelen kunnen zijn die de voor de verwerking verantwoordelijke moet vaststellen. Deze lijst met voorbeelden zou uiteraard slechts vergezeld gaan van de algemene wettelijke verplichting om passende maatregelen te nemen.

De maatregelen differentiëren

43. De bovenstaande opsomming is een lijst met voorbeeldmaatregelen die voor de verwerking verantwoordelijken zouden kunnen nemen om te voldoen aan het eerste deel van het verantwoordingsbeginsel (*De voor de verwerking verantwoordelijke legt passende en doeltreffende maatregelen ten uitvoer om te waarborgen dat de in de richtlijn vastgelegde beginselen en verplichtingen worden nageleefd)*

44. Een deel van de maatregelen zijn 'basismaatregelen' die bij het merendeel van de verwerkingen ten uitvoer zullen moeten worden gelegd. Het opstellen van intern beleid en interne procedures om de beginselen ten uitvoer te leggen (procedures voor het afhandelen van verzoeken om toegang, klachten) kan een voorbeeld zijn van een passende maatregel voor een bepaalde gegevensverwerking. Of een bepaalde maatregel geschikt is zal per geval moeten worden besloten. Dergelijke besluiten moeten worden genomen door de voor de verwerking verantwoordelijken, op basis van eventueel beschikbare richtsnoeren die zijn opgesteld door nationale gegevensbeschermingsautoriteiten en de Groep gegevensbescherming artikel 29 (zie verder).

45. Uit het bovenstaande volgt dat er bij de vaststelling van het soort maatregelen dat ten uitvoer moet worden gelegd altijd maar één optie is, namelijk het vinden van een "maatwerkoplossing". Welke specifieke maatregelen er moeten worden genomen moet immers worden vastgesteld aan de hand van de feiten en omstandigheden van elk afzonderlijk geval, met bijzondere aandacht voor de risico's die de verwerking en het soort gegevens met zich brengen. Een standaardbenadering zou de voor de verwerking verantwoordelijken slechts in een keurslijf dwingen dat uiteindelijk tekortschiet.

46. Deze benadering moet de voor de verwerking verantwoordelijken de gelegenheid bieden hun maatregelen af te stemmen op de concrete kenmerken van de voor de verwerking verantwoordelijke en de gegevensverwerking in kwestie. De Groep gegevensbescherming artikel 29 wijst in dit verband op de criteria die in artikel 17 van de huidige richtlijn[8] zijn vastgelegd om het soort beveiligingsmaatregelen dat moet worden toegepast te bepalen: namelijk, de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen. Deze twee factoren zouden naar analogie kunnen worden gebruikt om in het algemeen het soort maatregelen vast te stellen dat moet worden toegepast. In meer concrete zin kunnen aspecten als de omvang van de gegevensverwerking(en), de beoogde doelen van de verwerking en het voorziene aantal doorgiften het risiconiveau bepalen. Het soort

[8] *"Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen".*

gegevens, met inbegrip van de vraag of het gaat om gegevens van gevoelige aard, zou ook in aanmerking kunnen worden genomen. In het licht van dit verantwoordingsbeginsel zou ook kunnen worden nagedacht over de noodzaak om de gegevensverwerker of de ontwerpers en/of fabrikanten van ICT (informatie- en communicatietechnologie) te onderwerpen aan bepaalde verplichtingen.

47. Op grond van deze criteria dienen, in beginsel, vooral grote voor de verwerking verantwoordelijken strenge maatregelen ten uitvoer te leggen. In bepaalde gevallen zullen echter ook kleine of middelgrote voor de verwerking verantwoordelijken strikte waarborgen moeten invoeren, bijvoorbeeld als zij zich bezighouden met risicovolle gegevensverwerkingen, zoals bepaalde verwerkingen op het gebied van eGezondheid. Om een geloofwaardig en doeltreffend informatiebeheer te waarborgen zijn bijvoorbeeld voor een lokale overheid (college van burgemeester en wethouders), een multinational, een kleine (internet)onderneming, een organisatie waarvoor gegevensverwerking een kernactiviteit is en een organisatie die in het verleden de wetgeving heeft overtreden allemaal verschillende specifieke maatregelen vereist. Dit heeft tot gevolg dat, in eenvoudige en standaardgevallen, zoals bij de verwerking van persoonsgegevens van medewerkers om een interne adressenlijst op te stellen, eenvoudig kan worden voldaan aan de "bewijsplicht" die is vastgelegd in lid 2 van de bepaling over verantwoording (bijvoorbeeld door middel van de gebruikte mededeling, de omschrijving van basale beveiligingsmaatregelen enz.). In andere, ingewikkelder gevallen, zoals bijvoorbeeld bij het gebruik van innovatieve biometrische apparatuur, zouden er nadere eisen gesteld kunnen worden om te voldoen aan de "bewijsplicht". Zo moet de voor de verwerking verantwoordelijke wellicht kunnen aantonen dat hij een privacy-effectbeoordeling heeft uitgevoerd, dat de medewerkers die betrokken zijn bij de verwerking regelmatig worden opgeleid en geïnformeerd, enz.

48. Transparantie vormt een integraal onderdeel van veel verantwoordingsmaatregelen. Transparantie ten opzichte van de betrokkenen en het bredere publiek versterkt de verantwoordingsplicht van voor de verwerking verantwoordelijken. Zo wordt bijvoorbeeld een hoger verantwoordingsniveau bereikt door privacybeleid op internet openbaar te maken, door interne klachtenprocedures inzichtelijk te maken, en door publicatie in jaarverslagen.

Richtsnoeren en rechtszekerheid

49. Hoewel de behoefte aan differentiatie en de bijbehorende flexibiliteit noopt tot het gebruik van ruime formuleringen, is de Groep gegevensbescherming artikel 29 zich ervan bewust dat een brede bepaling die ruimte biedt voor flexibiliteit en differentiatie ook onzekerheid kan opleveren. Voor de verwerking verantwoordelijken kunnen de mening zijn toegedaan dat de bepaling onvoldoende gedetailleerd is om rechtszekerheid te verschaffen. Er kan bij hen bijvoorbeeld onzekerheid bestaan over vragen als: hoe gedetailleerd moeten privacybeleid en -procedures zijn, wanneer en hoe moet een functionaris voor gegevensbescherming worden aangewezen, wanneer moeten er opleidingen worden georganiseerd, enz. De onzekerheid kan daarnaast betrekking hebben op het soort controle dat noodzakelijk is: controle door derden of interne controle.

Bovendien kan onder voor de verwerking verantwoordelijken ook de angst leven dat zij worden geconfronteerd met uiteenlopende en willekeurige nationale interpretaties van de aard en omvang van hun verplichtingen.

50. De Groep gegevensbescherming artikel 29 heeft begrip voor deze bezorgdheid. Vanwege de bovenstaande redenen met betrekking tot de behoefte aan flexibiliteit en differentiatie kunnen de problemen op het gebied van rechtszekerheid echter niet worden opgelost in de richtlijn zelf. De Groep gegevensbescherming artikel 29 is van mening dat geharmoniseerde richtsnoeren die worden vastgesteld door de Commissie (bijvoorbeeld d.m.v. technische uitvoeringsmaatregelen) en/of de Groep gegevensbescherming artikel 29 zouden kunnen fungeren als nuttige hulpmiddelen om de benodigde rechtszekerheid te verschaffen. Op die manier ontstaat meer zekerheid en worden eventuele verschillen op uitvoeringsniveau weggenomen.[9] De Groep gegevensbescherming artikel 29 zou ook een algemene leidraad kunnen opstellen waarin de noodzakelijke basiselementen voor een gewone voor de verwerking verantwoordelijke worden omschreven. Deze basiselementen kunnen vervolgens exact worden afgestemd op de specifieke behoeften van elke voor de verwerking verantwoordelijke.

51. Daarnaast zou het nuttig kunnen zijn om een *model-nalevingsprogramma* te ontwikkelen dat middelgrote en grote voor de verwerking verantwoordelijken kunnen gebruiken als basis om hun eigen programma's te ontwikkelen. De Groep heeft hetzelfde gedaan met betrekking tot de BCR's door daarvoor richtsnoeren op te stellen[10]. Dergelijke modellen moeten wordt opgesteld na grondige analyse van de bestaande praktijken, de beschikbare modellen, en na raadpleging van alle relevante belanghebbenden. Dit is immers een terrein waarop serieuze inbreng van alle belanghebbenden noodzakelijk is.

De doeltreffendheid van maatregelen

52. Bij het waarborgen van de doeltreffendheid van maatregelen spelen dezelfde kwesties die hierboven zijn besproken met betrekking tot de te nemen maatregelen. De manier waarop de doeltreffendheid kan worden gewaarborgd zal afhangen van het soort gegevensverwerking.

53. Er zijn vele verschillende manieren waarop voor de verwerking verantwoordelijken de doeltreffendheid of (ondoeltreffendheid) van maatregelen kunnen beoordelen. Interne en externe audits zijn veelgebruikte controlemethoden voor verwerkingen die omvangrijker of ingewikkelder zijn of een hoog risico met zich brengen. Ook de wijze waarop audits worden uitgevoerd kan verschillen, variërend van volledige tot negatieve audits (die op hun beurt weer verschillende

---

9 Een voorbeeld van een dergelijk richtsnoer is het PIPEDA Self-assessment tool, dat door het Canadese bureau van de privacycommissaris is opgesteld om middelgrote en grote voor de verwerking verantwoordelijken te helpen bij de ontwikkeling en tenuitvoerlegging van een goed privacybeleid en -beheer. Dit document voor zelfevaluatie is beschikbaar op: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf .

10 Working Document 153 setting up a table with the elements and principles to be found in Binding Corporate Rules (Werkdocument 153 tot vaststelling van een tabel met de elementen en beginselen die in BCR's moeten voorkomen) en Working Document 154 setting up a framework for the structure of Binding Corporate Rules (Werkdocument 154 tot vaststelling van een kader voor de opbouw van BCR's).

vormen kunnen aannemen). Voor het nemen van besluiten over de wijze waarop de doeltreffendheid van de maatregelen kan worden gewaarborgd, stelt de Groep gegevensbescherming artikel 29 voor dezelfde criteria te hanteren als voor besluiten over de te nemen maatregelen. Deze criteria zijn afkomstig uit artikel 17 van Richtlijn 95/46/EG: de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen. De manier waarop een voor de verwerking verantwoordelijke de doeltreffendheid van maatregelen dient te waarborgen zal derhalve afhangen van de gevoeligheid van de gegevens, de hoeveelheid te verwerken gegevens en de specifieke risico's die de gegevensverwerking met zich brengt. De richtsnoeren van de Groep gegevensbescherming artikel 29 over de maatregelen zouden ook betrekking kunnen hebben op dit aspect.

IV.3 Verband met andere vereisten

Voorafgaande aanmeldingen

54. Er kan worden nagedacht over de mogelijke effecten voor voorafgaande aanmeldingen indien er passende waarborgen zijn vastgesteld op het niveau van de voor de verwerking verantwoordelijke. Bekeken zou kunnen worden of bepaalde verantwoordingsmechanismen geheel of gedeeltelijk de plaats kunnen innemen van administratieve eisen die zijn vastgelegd in de geldende wetgeving inzake gegevensbescherming. De Groep gegevensbescherming artikel 29 heeft deze suggestie eerder gedaan in haar document over de toekomst van privacy.

Internationale doorgiften van gegevens

55. BCR's zijn een voorbeeld van een manier waarop beginselen voor gegevensbescherming ten uitvoer kunnen worden gelegd op basis van het verantwoordingsbeginsel. Het is een door de Groep gegevensbescherming artikel 29 erkende en aanvaarde manier om voldoende waarborgen te bieden voor doorgiften buiten de Europese Unie.

56. Dit is een terrein waarop nadere analyse in het licht van de herziening van Richtlijn 95/46 een positieve uitwerking kan hebben. Het is met name van belang om te overwegen of BCR's en uiteindelijk ook vergelijkbare bindende verantwoordingsmechanismen die voldoende waarborgen moeten bieden, volledig vallen onder de werkingssfeer van artikel 26, lid 2 van de richtlijn ("*een lidstaat* [kan] *toestemming geven voor een doorgifte* (...) *indien de voor de verwerking verantwoordelijke voldoende waarborgen biedt; deze waarborgen kunnen met name voortvloeien uit passende contractuele bepalingen*").

57. In dit verband is het buitengewoon relevant om onder andere de mechanismen te beoordelen die worden gebruikt om gevolg te geven aan de beginselen voor gegevensverwerking binnen de voor de verwerking verantwoordelijken en de controlesystemen. Verder is een bespreking van de mechanismen relevant voor het stroomlijnen van het huidige systeem, dat is gebaseerd op de verlening van toestemming voor doorgiften van gegevens door nationale gegevensbeschermingsautoriteiten.

IV.4 De rol van gegevensbeschermingsautoriteiten

58. Een kwestie die aan de orde moet worden gesteld is of het verantwoordingsbeginsel zoals dat in dit advies wordt voorgesteld gevolgen zal hebben voor de bevoegdheden van gegevensbeschermingsautoriteiten, met name op het terrein van de handhaving. Zoals hieronder nader zal worden beschreven, doet het beginsel niets af aan de bevoegdheden van de gegevensbeschermingsautoriteiten. Integendeel, het levert voordelen voor hen op.

59. Met betrekking tot de handhaving wordt in het voorgestelde beginsel de bevoegdheid van de gegevensbeschermingsautoriteiten onderkend om de voor de verwerking verantwoordelijke te verzoeken aan te tonen dat het verantwoordingsbeginsel wordt nageleefd. Op die manier breidt het beginsel de handhavingsactiviteiten van de autoriteiten uit. Daardoor blijven de autoriteiten te allen tijde bevoegd om handhavingsmaatregelen te treffen. Er moet duidelijk worden gemaakt dat gegevensbeschermingsautoriteiten in elk geval bevoegd zullen blijven om niet alleen toezicht uit te oefenen op de maatregelen die de voor de verwerking verantwoordelijken hebben genomen, maar eerst en vooral om toezicht te houden op de naleving van de onderliggende beginselen en verplichtingen.

60. Daarnaast zal de tenuitvoerlegging van het verantwoordingsbeginsel de gegevensbeschermingsautoriteiten voorzien van nuttige informatie om de nalevingsniveaus te monitoren. Doordat de voor de verwerking verantwoordelijken aan de autoriteiten zullen moeten aantonen of en hoe zij de maatregelen ten uitvoer hebben gelegd, kan er zelfs uiterst relevante informatie in verband met de naleving beschikbaar komen voor de autoriteiten. Zij kunnen deze informatie vervolgens gebruiken in de context van hun handhavingsmaatregelen. Bovendien zouden gegevensbeschermingsautoriteiten onmiddellijk tot actie kunnen overgaan indien de betreffende informatie na een verzoek daartoe niet wordt overgelegd, ongeacht de vermeende schending van onderliggende beginselen voor gegevensbescherming.

61. Het beginsel kan voor gegevensbeschermingsautoriteiten ook nuttig zijn omdat het hen kan helpen selectiever en strategischer op te treden, hetgeen hun de gelegenheid biedt hun middelen zodanig te investeren dat zij op zo groot mogelijke schaal resulteren in naleving.

62. De Groep gegevensbescherming artikel 29 merkt op dat het verantwoordingsbeginsel een bijdrage kan leveren aan de ontwikkeling van juridische en technische kennis op het gebied van de tenuitvoerlegging van vereisten voor gegevensbescherming. Mensen die zeer goed zijn ingevoerd en beschikken over technische en juridische kennis op het gebied van gegevensbescherming, en daarnaast in staat zijn te communiceren, medewerkers op te leiden, beleid te ontwikkelen en ten uitvoer te leggen, en audits uit te voeren zullen onmisbaar zijn op dit terrein. Dergelijke kennis wordt noodzakelijk, zowel binnen organisaties als in de vorm van externe dienstverlening die bedrijven kunnen inhuren. Deze ontwikkeling wordt cruciaal om te waarborgen dat voor de verwerking verantwoordelijken hun verplichtingen kunnen nakomen, met inbegrip

van de uitvoering van interne en externe/interne audits. Tegelijkertijd zal deze ontwikkeling voordeel opleveren voor gegevensbeschermingsautoriteiten omdat het systeem zal bijdragen aan de algehele naleving, de autoriteiten hierdoor kunnen beschikken over grondiger informatie over de interne praktijken van bedrijven, en de ontwikkeling van zeer goed ingevoerde en bekwame professionals voor gegevensbescherming de contacten met de voor de verwerking verantwoordelijken zeker ten goede zal komen.

63. Geconcludeerd kan worden dat de activiteiten van gegevensbeschermingsautoriteiten vooral gericht zijn op het vervullen van een rol 'ex post' (d.w.z. nadat de gegevensverwerking is aangevangen) en niet op een rol 'ex ante'. Omdat met verantwoording de nadruk wordt gelegd op bepaalde resultaten die moeten worden geboekt ten aanzien van het beleid inzake goede gegevensbescherming, kan gesteld worden dat verantwoording resultaatgericht is; de nadruk ligt op 'ex post'.

IV. 5 Sancties

64. Het voorgestelde systeem kan alleen functioneren als gegevensbeschermingsautoriteiten de daadwerkelijke bevoegdheid krijgen om sancties op te leggen. In het bijzonder als en wanneer voor de verwerking verantwoordelijken verzuimen het verantwoordingsbeginsel na te leven, zijn daadwerkelijke sancties een noodzaak. Er moeten bijvoorbeeld sancties kunnen worden opgelegd indien een voor de verwerking verantwoordelijke zich niet houdt aan bepalingen van bindend intern beleid. Dit komt uiteraard bovenop de bevoegdheid sancties op te leggen in geval van de feitelijke inbreuken op materiële beginselen voor gegevensbescherming.

65. In aanvulling op het bovenstaande is de Groep gegevensbescherming artikel 29 van mening dat nationale gegevensbeschermingsautoriteiten de bevoegdheid moeten krijgen om precieze aanwijzingen te geven aan voor de verwerking verantwoordelijken met betrekking tot hun nalevingsprogramma.

IV.6 De ontwikkeling van certificeringsprogramma's

66. Op de langere termijn kan de bepaling over verantwoording de ontwikkeling bevorderen van certificeringsprogramma's of keurmerken. Dergelijke programma's kunnen helpen aantonen dat een voor de verwerking verantwoordelijke de bepaling heeft nageleefd, oftewel dat hij passende maatregelen heeft vastgesteld en ten uitvoer gelegd die periodiek zijn gecontroleerd. Diverse factoren kunnen een dergelijke ontwikkeling bevorderen.

67. In het algemeen valt te verwachten dat dienstverleners op het gebied van gegevensbescherming/audits/privacy-effectbeoordelingen in toenemende mate certificaten/keurmerken zullen aanbieden, zodat zij zich in positieve zin kunnen onderscheiden van concurrenten en op kunnen vallen binnen hun markt. Voor de verwerking verantwoordelijken kunnen besluiten te kiezen voor betrouwbare dienstverleners die certificaten afgeven. Wanneer bepaalde keurmerken bekend komen te staan vanwege de strenge controle ervan, zullen de voor de verwerking verantwoordelijken geneigd zijn daaraan de voorkeur te geven, niet alleen

vanwege het concurrentievoordeel dat ze opleveren maar ook omdat ze meer nalevingszekerheid bieden.

68. Voorwaarde voor het gebruik van BCR's als rechtsgrondslag voor internationale gegevensdoorgiften is dat voor de verwerking verantwoordelijken kunnen aantonen dat zij voldoende waarborgen bieden. Als dat het geval is, kunnen gegevensbeschermingsautoriteiten toestemming geven voor de doorgiften. Dit is een terrein waarop certificeringsdiensten van pas zouden komen. De verleners van dergelijke diensten zouden de waarborgen die de voor de verwerking verantwoordelijke biedt moeten analyseren en, indien van toepassing, het betreffende keurmerk moeten afgeven. Een gegevensbeschermingsautoriteit zou de certificering die een bepaald certificeringsprogramma biedt kunnen gebruiken in haar analyse van BCR's om te bepalen of een voor de verwerking verantwoordelijke voldoende waarborgen heeft geboden om internationale gegevensdoorgiften te rechtvaardigen. Op die manier kan een bijdrage worden geleverd aan het stroomlijnen van het proces van toestemmingsverlening voor internationale gegevensdoorgiften.

IV.7 De regulering van certificeringsprogramma's

69. Uit de redenen die ten grondslag liggen aan de ontwikkeling van certificeringsdiensten vloeit ook de noodzaak voort om dergelijke diensten te reguleren. Indien dergelijke diensten immers bedoeld zijn om betrouwbaar bewijs te leveren van de naleving van gegevensbescherming (aan gegevensbeschermingsautoriteiten, aan voor de verwerking verantwoordelijken en aan consumenten in het algemeen) en soepel moeten kunnen functioneren in de interne markt, lijkt het noodzakelijk regels vast te stellen voor de eisen waaraan de verlening van dergelijke diensten moet voldoen. Gegevensbeschermingsautoriteiten moeten een sleutelrol vervullen bij de ontwikkeling van zulke regels (bv. door te verwijzen, modellen op te stellen, enz.) en moeten de tenuitvoerlegging ervan kunnen handhaven. Dit vereist verder dat zij moeten kunnen beschikken over voldoende middelen. Bovendien moeten gegevensbeschermingsautoriteiten een rol spelen bij het certificeren van de certificeringsdiensten. Dit kan vooral relevant zijn op het terrein van internationale gegevensdoorgiften. Aangezien de kwaliteit van de dienstverleners en de noodzaak dat zij binnen de interne markt opereren de voornaamste criteria zijn, zal de wetgeving de voorwaarden moeten scheppen voor het bereiken van een dergelijke kwaliteit. Het lijkt erop dat dit niet aan de markt kan worden overgelaten. Uit ervaringen op andere terreinen, zoals de certificering van goederen, is gebleken dat er een neiging bestaat de bodem op te zoeken. Concurrentie tussen dienstverleners zou kunnen leiden tot lagere prijzen, maar ook tot een zekere flexibiliteit of versoepeling van de procedures. Kortom, of het nu gaat om een grensoverschrijdende situatie of niet, regels lijken noodzakelijk om een goede kwaliteit van de diensten en eerlijke concurrentie te garanderen.

70. De Groep gegevensbescherming artikel 29 merkt op dat de bestaande wetgeving inzake accreditatie[11] van toepassing kan zijn op certificeringsdiensten voor gegevensbescherming. Deze wetgeving bevat al de noodzakelijke structuur, met regels betreffende de organisatie en werking van accreditatie-instanties. Deze regels gelden zowel voor vrijwillige accreditatie als in de specifieke gevallen waarin accreditatie verplicht is.

71. Uiteraard kunnen dit soort diensten ook een impuls geven aan de harmonisatie van de onderliggende normen waaraan moet worden voldaan. De reeds genoemde richtsnoeren (van de Groep gegevensbescherming artikel 29 of van de Commissie) waarin wordt voorzien in model-nalevingsprogramma's, kunnen hierbij zeer relevant zijn.

V. CONCLUSIES

72. De ontwikkeling van nieuwe technologieën en de voortschrijdende mondialisering van economie en maatschappij hebben geleid tot een zeer snelle vermenigvuldiging van de persoonlijke informatie die wordt verzameld, gesorteerd, doorgegeven of anderszins wordt bewaard. Hierdoor nemen ook de risico's toe dat er inbreuk wordt gemaakt op dergelijke gegevens.

73. De Groep gegevensbescherming artikel 29 is ervan overtuigd dat de toename van zowel de risico's voor als de waarde van persoonsgegevens *op zich* al voldoende de noodzaak onderstrepen om de rol en verantwoordelijkheid van voor de verwerking verantwoordelijken te verstevigen. Een regelgevingskader dat inspeelt op deze nieuwe realiteit moet de noodzakelijke instrumenten omvatten om voor de verwerking verantwoordelijken aan te moedigen in de praktijk passende en doeltreffende maatregelen ten uitvoer te leggen waarmee gevolg wordt gegeven aan de beginselen voor gegevensbescherming. Voorbeelden van dergelijke maatregelen zijn procedures om de identificatie van alle gegevensverwerkingen te waarborgen, procedures om te reageren op verzoeken om toegang, en de toewijzing van middelen, met inbegrip van de aanwijzing van medewerkers die verantwoordelijk zijn voor de organisatie van de naleving van gegevensbescherming.

74. Om gegevensbescherming in de praktijk te bevorderen stelt de Groep gegevensbescherming artikel 29 eerst en vooral voor om in de voorstellen tot wijziging van de richtlijn gegevensbescherming een nieuwe bepaling op te nemen. Deze bepaling moet voor de verwerking verantwoordelijken ertoe verplichten passende en doeltreffende maatregelen ten uitvoer te leggen om te waarborgen dat de beginselen en verplichtingen die zijn vastgelegd in de richtlijn gegevensbescherming, worden nageleefd en op verzoek van de autoriteiten aan te tonen dat dit het geval is. Deze maatregelen moeten de naleving van de beginselen en verplichtingen op het gebied van gegevensbescherming bevorderen en het gevaar van toegang door onbevoegden, misbruik, verlies, enz. zoveel mogelijk terugdringen. De verplichting om op verzoek aan te tonen dat de noodzakelijke

[11] Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93.

maatregelen zijn genomen, kan een nuttig instrument zijn voor gegevensbeschermingsautoriteiten bij de uitoefening van hun handhavende taken.

75. De plicht om deze maatregelen ten uitvoer te leggen moet gelden met betrekking tot de voor de verwerking verantwoordelijken in alle sectoren (publiek en privaat) en moet differentieerbaar zijn, zodat het soort maatregelen kan worden afgestemd op de risico's die de verwerking en de aard van de gegevens met zich brengen.

Brussel, 13 juli 2010

Namens de Groep
Jacob Kohnstamm
Voorzitter