



**00264/10/NL
WP 169**

**Advies 1/2010 over de begrippen “voor de verwerking verantwoordelijke” en
“verwerker”**

Goedgekeurd op 16 februari 2010

Deze groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Het is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door directoraat D (Grondrechten en burgerschap) van het directoraat-generaal Justitie, vrijheid en veiligheid van de Europese Commissie, 1049 Brussel, België, bureau LX-46 01/190.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

INHOUDSOPGAVE

Samenvatting en toelichting	1
I. Inleiding	3
II. Algemene opmerkingen en beleidspunten	4
II.1. Rol van begrippen.....	5
II.2. Relevante context.....	7
II.3. Enkele centrale uitdagingen.....	9
III. Analyse van definities	9
III.1. Definitie van “voor de verwerking verantwoordelijke”	9
III.1.a) Inleidend element: “vaststelt”	10
III.1.b) Derde element: “het doel van de middelen voor de verwerking”	15
III.1.c) Eerste element: “de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam”	18
III.1.d) Tweede element: “die, respectievelijk dat, alleen of tezamen met anderen” ...	21
III.2. Definitie van verwerker	28
III.3. Definitie van derde	35
IV. Conclusies	36

Samenvatting en toelichting

Het begrip “voor de verwerking verantwoordelijke” en zijn raakvlakken met het begrip “gegevensverwerker” spelen een cruciale rol in de tenuitvoerlegging van Richtlijn 95/46/EG, omdat aan de hand van deze begrippen wordt uitgemaakt wie verantwoordelijk is voor de naleving van de regelgeving met betrekking tot gegevensbescherming, op welke wijze betrokkenen hun rechten kunnen uitoefenen, welk nationaal recht van toepassing is en hoe effectief gegevensbeschermingsautoriteiten hun werk kunnen doen.

Organisatiedifferentiatie in zowel de publieke als de private sector, de ontwikkeling van ICT en de mondialisering van gegevensverwerking maken de wijze waarop persoonsgegevens worden verwerkt steeds gecompliceerder en vragen om verduidelijking van deze begrippen, zodat een effectieve toepassing en de praktische naleving kunnen worden gewaarborgd.

Het begrip “voor de verwerking verantwoordelijke” is autonoom, in die zin dat het met name dient te worden geïnterpreteerd volgens de communautaire wetgeving voor gegevensbescherming. Daarnaast is het functioneel, in die zin dat het bedoeld is om de verantwoordelijkheden te leggen op de plaats waar ook de feitelijke invloed ligt, en dus eerder op een feitelijke dan op een formele analyse gebaseerd.

De definitie in de richtlijn is opgebouwd uit drie hoofdonderdelen:

- het personele aspect (“*de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam*”),
- de mogelijkheid van gezamenlijke verantwoordelijkheid (“*die, respectievelijk dat, alleen of tezamen met anderen*”),
- de wezenlijke aspecten waarmee de voor de verwerking verantwoordelijke van andere partijen kan worden onderscheiden (“*het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*”).

De analyse van deze onderdelen leidt tot een aantal conclusies die zijn opgenomen in paragraaf IV van het advies.

In dit advies wordt ook gekeken naar het begrip “verwerker”, waarvan het bestaan afhangt van een besluit van de voor de verwerking verantwoordelijke, die kan besluiten om gegevens binnen zijn eigen organisatie te verwerken of de verwerking daarvan geheel of gedeeltelijk aan een externe organisatie te delegeren. De twee kernvoorwaarden om een partij als verwerker te kunnen aanmerken zijn dus enerzijds dat het een aparte rechtspersoon is, die los van de voor de verwerking verantwoordelijke staat, en anderzijds dat deze partij persoonsgegevens namens die voor de verwerking verantwoordelijke verwerkt.

De Groep erkent dat het moeilijk is om de definities van de richtlijn toe te passen in een complexe omgeving, waarin vele scenario’s mogelijk zijn met voor de verwerking verantwoordelijken en verwerkers, alleen of gezamenlijk, met verschillende mates van autonomie en verantwoordelijkheid.

In zijn analyse heeft de groep benadrukt dat verantwoordelijkheden zodanig moeten worden belegd dat de naleving van de regelgeving voor gegevensbescherming in de praktijk voldoende is gewaarborgd. De groep heeft echter geen aanleiding gevonden om

te veronderstellen dat het huidige onderscheid tussen voor de verwerking verantwoordelijken en verwerkers vanuit dat oogpunt niet langer relevant en werkbaar zou zijn.

Daarom hoopt de groep dat de toelichting in dit advies en de vele concrete voorbeelden uit de dagelijkse praktijk van gegevensbeschermingsautoriteiten kunnen bijdragen aan effectieve informatie over de wijze waarop deze kerndefinities van de richtlijn moeten worden geïnterpreteerd.

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:

I. Inleiding

Het begrip “voor de verwerking van gegevens verantwoordelijke” en zijn raakvlakken met het begrip “gegevensverwerker” staan centraal bij de uitvoering van Richtlijn 95/46/EG, omdat ermee wordt bepaald wie verantwoordelijk is voor de naleving van de regelgeving met betrekking tot gegevensbescherming en voor de manier waarop betrokkenen in de praktijk hun rechten kunnen uitoefenen. Het begrip “voor de verwerking van gegevens verantwoordelijke” is ook van wezenlijk belang wanneer moet worden vastgesteld welk nationaal recht van toepassing is, en voor de daadwerkelijke uitoefening van de toezichthoudende taken waarmee gegevensbeschermingsautoriteiten zijn belast.

Het is daarom van het grootste belang dat de exacte betekenis van deze begrippen en de criteria voor een juist gebruik ervan voldoende duidelijk zijn, en worden gedeeld door iedereen die in de lidstaten een rol vervult bij de uitvoering van de richtlijn en bij toepassing, evaluatie en handhaving van de nationale bepalingen waarmee de richtlijn in de praktijk gestalte krijgt.

Er zijn signalen dat in ieder geval sommige aspecten van deze begrippen wellicht niet geheel duidelijk zijn, en dat uitvoerenden in verschillende lidstaten er uiteenlopende zienswijzen op na zouden houden, die mogelijk leiden tot verschillende interpretaties van dezelfde beginselen en definities, die juist werden ingevoerd om op Europees niveau tot harmonisatie te komen. Daarom heeft de Groep Artikel 29 in het kader van haar strategisch werkprogramma voor 2008-2009 besloten om bijzondere aandacht te schenken aan het opstellen van een document met een gemeenschappelijke benadering van deze onderwerpen.

De Groep erkent dat de concrete toepassing van de begrippen “voor de verwerking van gegevens verantwoordelijke” en “gegevensverwerker” steeds gecompliceerder wordt. Dit is met name een gevolg van de steeds grotere complexiteit van de omgeving waarin deze begrippen worden gebruikt, en met name van een steeds sterkere tendens tot differentiatie van organisaties in zowel de private als de publieke sector, in combinatie met de ontwikkeling van ICT en een verder gaande mondialisering. Hierdoor kunnen nieuwe en moeilijke problemen ontstaan, die er soms toe leiden dat betrokkenen minder goed worden beschermd.

Hoewel de bepalingen van de richtlijn technologie-neutraal zijn geformuleerd en tot op heden goed bruikbaar zijn gebleven in een zich ontwikkelende omgeving, kunnen deze problemen wel aanleiding geven tot onduidelijkheden met betrekking tot het beleggen van verantwoordelijkheden en de werkingssfeer van relevante nationale wetgeving. Deze onduidelijkheden kunnen op belangrijke gebieden nadelig zijn voor de naleving van de regelgeving voor gegevensbescherming en op de effectiviteit van de wetgeving voor gegevensbescherming als geheel. De Groep heeft zich op specifieke gebieden reeds over een aantal van deze problemen gebogen¹, maar acht het nu noodzakelijk om nadere richtsnoeren en specifieke informatie op te stellen om een samenhangende en geharmoniseerde benadering te waarborgen.

Daarom heeft de Groep besloten om in dit advies – op eenzelfde wijze als in het advies over het begrip “persoonsgegevens”² – op een aantal punten verduidelijking te geven en concrete voorbeelden aan te dragen³ met betrekking tot de begrippen “voor de verwerking van gegevens verantwoordelijke” en “gegevensverwerker”.

II. Algemene opmerkingen en beleidspunten

In de richtlijn wordt in meerdere bepalingen uitdrukkelijk het begrip “voor de verwerking verantwoordelijke” gebruikt. De definities van “voor de verwerking verantwoordelijke” en “verwerker” uit artikel 2, onder d) en e), van Richtlijn 95/46/EG (hierna “de richtlijn” te noemen) luiden als volgt:

“voor de verwerking verantwoordelijke”, de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer het doel van en de middelen voor de verwerking worden vastgesteld bij nationale of communautaire wettelijke of bestuursrechtelijke bepalingen, kan in het nationale of communautaire recht worden bepaald wie de voor de verwerking verantwoordelijke is of volgens welke criteria deze wordt aangewezen;

“verwerker”, de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt.

Deze definities zijn tot stand gekomen tijdens de besprekingen die begin jaren negentig werden gevoerd over de ontwerp-tekst voor de richtlijn, en het begrip “voor de verwerking verantwoordelijke” was voor een belangrijk deel afkomstig uit Verdrag 108 van de Raad van Europa uit 1981. Tijdens deze besprekingen werd een aantal belangrijke wijzigingen doorgevoerd.

¹ Zie onder meer Advies 10/2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT), goedgekeurd op 22 november 2006 (WP 128), en meer recentelijk Advies 5/2009 over online sociale netwerken, goedgekeurd op 12 juni 2009 (WP 163).

² Advies 4/2007 over het begrip persoonsgegeven, goedgekeurd op 20 juni 2007 (WP 136).

³ Deze voorbeelden zijn gebaseerd op de huidige nationale of Europese praktijk en kunnen voor de duidelijkheid iets aangepast of bewerkt zijn.

Ten eerste werd voor de “verwerking van persoonsgegevens” het begrip “houder van een bestand” uit Verdrag 108 vervangen door “voor de verwerking verantwoordelijke”. “Verwerking van persoonsgegevens” is een breed begrip, dat in artikel 2, onder b), van de richtlijn wordt omschreven als “elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens”. Het begrip “houder” of “verantwoordelijke” werd daarmee niet langer gebruikt voor een statisch object (“bestand”) maar gekoppeld aan activiteiten die de levenscyclus van gegevens weerspiegelen, vanaf het verzamelen tot het vernietigen ervan, en dit moest zowel op detailniveau als voor het geheel (“bewerking of elk geheel van bewerkingen”) worden gezien. Hoewel het resultaat in veel gevallen hetzelfde was, kreeg het begrip hiermee een veel bredere en meer dynamische betekenis en werkingsfeer.

Andere veranderingen hadden betrekking op de invoering van de mogelijkheid van “gezamenlijke verantwoordelijkheid” (“alleen of tezamen met anderen”), de eis dat de voor de verwerking verantwoordelijke “het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt” en het begrip dat deze vaststelling door middel van nationale of communautaire wetgeving of op andere wijze kan plaatsvinden. Daarnaast werd in de richtlijn het begrip “verwerker” ingevoerd. Dit bestond niet in Verdrag 108. Deze en andere wijzigingen komen in dit advies nader aan de orde.

II.1. Rol van begrippen

Waar het begrip “houder van een bestand” een zeer beperkte rol vervult⁴ in Verdrag 108, is dit wat betreft de “voor de verwerking verantwoordelijke” in de richtlijn geheel anders. In artikel 6, lid 2 wordt uitdrukkelijk bepaald dat “op de voor de verwerking verantwoordelijke [...] de plicht [rust] om voor de naleving van het bepaalde in lid 1 zorg te dragen”. Dit is een verwijzing naar de belangrijkste beginselen met betrekking tot de kwaliteit van gegevens, waaronder het beginsel uit artikel 6, lid 1, onder a), dat “persoonsgegevens eerlijk en rechtmatig moeten worden verwerkt”. Dit betekent in feite dat alle bepalingen met voorwaarden voor een rechtmatige verwerking in wezen zijn gericht tot de voor de verwerking verantwoordelijke, ook wanneer dit niet altijd even duidelijk wordt aangegeven.

Bovendien zijn de bepalingen over de rechten van betrokkenen op informatieverstrekking, toegang, rectificatie, uitwissing en afscherming en op verzet tegen de verwerking van persoonsgegevens (de artikelen 10-12 en 14) zodanig geformuleerd dat er voor de voor de verwerking verantwoordelijke verplichtingen ontstaan. De voor de verwerking verantwoordelijke staat ook centraal in de bepalingen over aanmelding en voorafgaand onderzoek (de artikelen 18-21). Ten slotte mag het niet verbazen dat de voor de verwerking verantwoordelijke in beginsel ook aansprakelijk is voor schade ten gevolge van onrechtmatige verwerking (artikel 23).

⁴ Het wordt in geen van de materiële bepalingen gebruikt, behalve in artikel 8, onder a., over het recht op informatieverstrekking (transparantiebeginsel). De houder van een bestand komt als verantwoordelijke partij slechts in bepaalde delen van de toelichting voor.

Dit betekent dat met het begrip “voor de verwerking verantwoordelijke” allereerst wordt bepaald wie verantwoordelijk is voor de naleving van de regelgeving voor gegevensbescherming en de manier waarop betrokkenen de rechten in de praktijk kunnen uitoefenen⁵. Met andere woorden: het toekennen van verantwoordelijkheid.

Daarmee komen we bij de kern van de richtlijn, die immers als eerste doelstelling “de bescherming van personen in verband met de verwerking van persoonsgegevens” heeft. Dit doel kan alleen worden bereikt en in de praktijk gestalte krijgen wanneer de voor de verwerking van gegevens verantwoordelijken met wettelijke en andere middelen voldoende kunnen worden gestimuleerd om alle maatregelen te nemen die noodzakelijk zijn om deze bescherming in de praktijk tot stand te brengen. Dit wordt bevestigd in artikel 17, lid 1 van de richtlijn, waarin wordt bepaald dat de voor de verwerking verantwoordelijke *“passende technische en organisatorische maatregelen ten uitvoer dient te leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking.”*

De middelen om verantwoordelijkheid te stimuleren kunnen proactief en reactief zijn. In het eerste geval moeten zij waarborgen dat maatregelen voor gegevensbescherming daadwerkelijk worden uitgevoerd en voldoende middelen beschikbaar zijn om de voor de verwerking verantwoordelijke op zijn verantwoordelijkheid aan te spreken. In het tweede geval kan het gaan om civielrechtelijke aansprakelijkheid en sancties, om te waarborgen dat eventuele relevante schade wordt gecompenseerd en dat passende maatregelen worden genomen om fouten of overtredingen te herstellen.

Het begrip “voor de verwerking verantwoordelijke” is ook van wezenlijk belang wanneer moet worden vastgesteld welk nationaal recht van toepassing is op een verwerking of een geheel van verwerkingen. De hoofdregel voor het toepasselijke recht uit artikel 4, lid 1, onder a), van de richtlijn is dat elke lidstaat zijn nationale bepalingen toepast op *“de verwerking van persoonsgegevens indien [...] die wordt verricht in het kader van de activiteiten van een vestiging op het grondgebied van de lidstaat van de voor de verwerking verantwoordelijke”*. Deze bepaling gaat als volgt verder: *“wanneer dezelfde verantwoordelijke een vestiging heeft op het grondgebied van verscheidene lidstaten, dient hij de nodige maatregelen te treffen om ervoor te zorgen dat elk van die vestigingen voldoet aan de verplichtingen die worden opgelegd door de toepasselijke nationale wetgeving”*. Dit betekent dat de vestigingsplaats(en) van de voor de verwerking verantwoordelijke ook bepaalt (bepalen) welk nationaal recht van toepassing is, en mogelijk ook welke nationale wetten en welke verbanden daartussen relevant zijn.⁶

⁵ Zie ook overweging 25 van Richtlijn 95/46/EG: *“Overwegende dat de beginselen van de bescherming enerzijds tot uiting moeten komen in de verplichtingen die aan de personen, overheidsinstanties, ondernemingen of andere lichamen die de verwerkingen uitvoeren, worden opgelegd, verplichtingen die met name betrekking hebben op de kwaliteit van de gegevens, de technische beveiliging, de aanmelding bij de toezichthoudende autoriteit en de omstandigheden waarin de verwerking kan worden uitgevoerd, en anderzijds in het feit dat aan personen wier gegevens het voorwerp van verwerkingen zijn, het recht wordt verleend om daarvan in kennis te worden gesteld, tot die gegevens toegang te krijgen, de rectificatie ervan te verlangen en zelfs om zich in bepaalde omstandigheden tegen verwerking te verzetten.”*

⁶ De Groep heeft het voornemen om in de loop van 2010 een afzonderlijk advies over het “toepasselijk recht” uit te brengen. Wanneer instellingen van de Gemeenschap en instanties persoonsgegevens verwerken, is de beoordeling van de verantwoordelijkheid ook relevant voor de mogelijke toepassing van Verordening (EG) nr. 45/2001 of andere relevante rechtsinstrumenten van de EU.

Tot slot dient te worden opgemerkt dat het begrip “voor de verwerking verantwoordelijke” in een groot aantal bepalingen van de richtlijn wordt gebruikt om de werkingssfeer van die bepalingen of van een specifieke voorwaarde daaruit aan te geven. Zo wordt in artikel 7 bepaald dat persoonsgegevens uitsluitend mogen worden verwerkt indien: “(c) *de verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is, (e) de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, drager is opgedragen, of (f) de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden [...] niet prevaleren*”. De identiteit van de voor de verwerking verantwoordelijke is ook een belangrijk onderdeel van de informatieverstrekking aan de betrokkene die in de artikelen 10 en 11 wordt voorgeschreven.

Het begrip “verwerker” speelt een belangrijke rol in het kader van de vertrouwelijkheid en de beveiliging van de verwerking (artikelen 16-17) omdat het wordt gebruikt om de verantwoordelijkheden te bepalen van degenen die nauwer betrokken zijn bij de verwerking van persoonsgegevens, onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of elders, ten behoeve van hem. Het onderscheid tussen “voor de verwerking verantwoordelijke” en “verwerker” dient met name om een onderscheid te maken tussen partijen met de hoedanigheid van voor de verwerking verantwoordelijke en degenen die uitsluitend namens hen handelen. Ook hier gaat het hoofdzakelijk om het beleggen van de verantwoordelijkheid. Andere gevolgen, met betrekking tot het toepasselijk recht of anderszins, kunnen hieruit voortvloeien.

In het geval van een verwerker is er echter een ander gevolg – voor zowel de voor de verwerking verantwoordelijke als de verwerker – namelijk dat op grond van artikel 17 van de richtlijn het toepasselijk recht voor de beveiliging van de verwerking het nationale recht is van de lidstaat waar de verwerker is gevestigd⁷.

Ten slotte wordt in artikel 2, onder f), een “derde” omschreven als “de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam, niet zijnde de betrokkene, noch de voor de verwerking verantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of de verwerker gemachtigd zijn om de gegevens te verwerken.” Derhalve worden de voor de verwerking verantwoordelijke en de verwerker beschouwd als de meest bij de gegevensverwerking betrokken partijen en vallen zij niet onder bijzondere bepalingen voor derden.

II.2. Relevante context

Verskillende ontwikkelingen in de relevante omgeving hebben deze zaken urgenter en ook gecompliceerder dan in het verleden gemaakt. Bij de ondertekening van Verdrag 108, en voor een groot deel ook op het moment dat Richtlijn 95/46/EG werd aangenomen, was het kader van gegevensverwerking nog relatief duidelijk en eenvoudig, maar dat is nu niet meer het geval.

⁷ Zie artikel 17, lid 3, tweede aandachtstreepje: de [...] verplichtingen, zoals gedefinieerd door de wetgeving van de lidstaat waarin de verwerker is gevestigd, eveneens op deze persoon rusten.

Allereerst is dit een gevolg van een toenemende tendens naar organisatiedifferentiatie in de meeste relevante sectoren. In de private sector heeft de spreiding van financiële of andere risico's geleid tot een voortdurende diversificatie van ondernemingen, die nog verder wordt versterkt door fusies en overnames. In de publieke sector is sprake van een vergelijkbare differentiatie in het kader van de decentralisatie of splitsing van beleidsafdelingen en uitvoerende instanties. In beide sectoren komt steeds meer nadruk te liggen op de ontwikkeling van leveringsketens of organisatiebrede dienstverlening, en op het gebruik van onderaannemers of het uitbesteden van diensten om te kunnen profiteren van specialisatie en mogelijke schaalvoordelen. Als gevolg hiervan groeit het aanbod van dienstverleners, die zichzelf niet altijd als verantwoordelijk of verantwoordingsplichtig beschouwen. Door organisatorische keuzes van ondernemingen (en hun aannemers of onderaannemers) kunnen de desbetreffende gegevensbestanden worden ondergebracht in een of meer landen binnen of buiten de Europese Unie.

De ontwikkeling van Informatie- en Communicatietechnologie (ICT) heeft deze organisatorische veranderingen sterk bevorderd en is zelf ook verantwoordelijk voor een aantal veranderingen. Verantwoordelijkheden op verschillende niveaus – die vaak voortvloeien uit een differentiatie van organisaties – vereisen en bevorderen doorgaans een uitgebreid gebruik van ICT. De ontwikkeling en toepassing van ICT-producten en -diensten leiden op zichzelf ook tot nieuwe rollen en verantwoordelijkheden, die niet altijd duidelijk aansluiten bij bestaande of zich ontwikkelende verantwoordelijkheden in de afnemende organisaties. Daarom is bewustzijn van relevante verschillen van belang en moeten verantwoordelijkheden waar nodig worden verduidelijkt. Ook bij de invoering van microtechnologie – bijvoorbeeld RFID-chips in consumentenproducten – ontstaan vergelijkbare vraagstukken met betrekking tot verschuivingen in verantwoordelijkheden. Aan de andere kant spelen er ook nieuwe en moeilijke vraagstukken bij het gebruik van zogenoemd gedistribueerd computergebruik, waaronder met name “*cloud computing*” en “*grids*”⁸.

Mondialisering is een andere complicerende factor. Waar bij organisatiedifferentiatie en de ontwikkeling van ICT meerdere rechtsstelsels een rol spelen, zoals vaak het geval is op internet, rijzen ook vaak problemen over het toepasselijk recht, niet alleen binnen de EU of de EER, maar ook met derde landen. Een voorbeeld is te vinden bij de strijd tegen doping, waarin het in Zwitserland gevestigde Wereldantidopingagentschap (WADA) een database met informatie over atleten (ADAMS) heeft, die vanuit Canada wordt beheerd in samenwerking met nationale instanties voor dopingbestrijding van over de hele wereld. Bij het verdelen van verantwoordelijkheden en het vaststellen wie voor de verwerking verantwoordelijk is, ontstaat volgens WP29 een aantal specifieke problemen⁹.

Dit betekent dat de kernpunten uit dit advies een grote praktische relevantie hebben en grote gevolgen kunnen hebben.

⁸ “*Cloud computing*” is een vorm van computergebruik waarbij schaalbare en flexibele IT-faciliteiten als dienst worden aangeboden aan grote aantallen klanten die internettechnologie gebruiken. Veel voorkomende diensten met “*cloud computing*” zijn het online aanbieden van standaard zakelijke toepassingen die met een webbrowser toegankelijk zijn en waarbij software en data op de servers staan. In deze zin is de “*cloud*” geen eiland maar een wereldwijde schakel tussen informatie en gebruikers. Voor meer informatie over “*grids*” wordt verwezen naar onderstaand voorbeeld 19.

⁹ Advies 3/2008 van 1 augustus 2008 over het ontwerp voor een internationale standaard inzake de bescherming van de persoonlijke levenssfeer in het kader van de wereldantidopingcode, WP156

II.3. Enkele centrale uitdagingen

Waar het gaat om de doelstellingen van de richtlijn moet met name worden gewaarborgd dat de verantwoordelijkheid voor de verwerking van gegevens duidelijk wordt omschreven en effectief kan worden toegepast.

Wanneer niet voldoende duidelijk is wie wat moet doen – bijvoorbeeld wanneer niemand verantwoordelijk is of er juist heel veel mogelijke verantwoordelijken zijn – bestaat uiteraard het risico dat er te weinig (of zelfs niets) gebeurt en dat de wettelijke bepalingen een dode letter blijven. Ook kunnen uiteenlopende interpretaties leiden tot strijdige aanspraken en andere controverses. In dat geval blijven de positieve effecten achter bij de verwachtingen of kunnen zij worden beperkt of opgeheven door onverwachte negatieve gevolgen.

In al deze gevallen is de belangrijkste uitdaging dus om voldoende duidelijkheid te scheppen, zodat effectieve toepassing en naleving in de praktijk mogelijk zijn en dan ook kunnen worden gewaarborgd. In geval van twijfel verdient het wellicht aanbeveling de oplossing te kiezen die hiervoor de beste mogelijkheden biedt.

De criteria die voldoende duidelijkheid scheppen, kunnen de zaken echter ook gecompliceerder maken en ongewenste gevolgen hebben. Zo kan bijvoorbeeld een differentiatie van de verantwoordelijkheid, aansluitend bij de realiteit in organisaties, tot gevolg hebben dat in situaties waarbij sprake is van meerdere rechtsstelsels meer onduidelijkheid ontstaat over de vraag welk nationaal recht van toepassing is.

Bij de analyse moet daarom goed worden gekeken naar het verschil tussen aanvaardbare gevolgen onder de huidige regelgeving en de mogelijk noodzakelijke aanpassing van bestaande regels om te zorgen dat deze effectief blijven en om ongewenste gevolgen bij veranderende omstandigheden te voorkomen.

Dit betekent dat deze analyse van groot strategisch belang is, en zorgvuldig moet worden uitgevoerd, in het volle besef dat er tussen verschillende problemen wellicht raakvlakken bestaan.

III. Analyse van definities

III.1. Definitie van “voor de verwerking verantwoordelijke”

In de richtlijn is de definitie van de voor de verwerking verantwoordelijke opgebouwd uit drie hoofdonderdelen, die in dit advies afzonderlijk worden onderzocht. Het betreft de volgende onderdelen:

- “de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam”
- “die, respectievelijk dat, alleen of tezamen met anderen”
- “het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt”.

Het eerste onderdeel heeft betrekking op het personele aspect van de definitie. Het derde onderdeel bevat de kernaspecten waarmee de voor de verwerking verantwoordelijke kan worden onderscheiden van andere partijen, terwijl het tweede onderdeel voorziet in de mogelijkheid van “gezamenlijke verantwoordelijkheid”. Deze onderdelen zijn onderling nauw verweven. Met het oog op de in dit advies te volgen methodiek zullen ze echter afzonderlijk worden besproken.

Om praktische redenen is het zinvol om te beginnen met het *eerste element* van het derde onderdeel, dus de betekenis van het woord “vaststelt”, en om dan verder te gaan met de rest van het derde onderdeel en pas daarna het eerste en tweede onderdeel te behandelen.

III.1.a) Inleidend element: “vaststelt”

Zoals reeds gezegd, speelde het begrip “houder van een bestand” een beperkte rol in Verdrag 108. In artikel 2 van dat verdrag werd de “houder van een bestand” omschreven als de instantie “die de bevoegdheid heeft te beslissen”. Verdrag 108 benadrukt de noodzaak van een bevoegdheid, die wordt vastgesteld “volgens het nationale recht”. Daarom verwees het verdrag terug naar nationale wetgeving over gegevensbescherming, waarin volgens de toelichting “nauwkeurig omschreven criteria” zouden zijn opgenomen om vast te stellen wie bevoegd is.

Hoewel deze bepaling terugkomt in het eerste voorstel van de Commissie, wordt in haar gewijzigde voorstel in plaats daarvan gesproken over de “beslissende” instantie, waarmee de eis komt te vervallen dat die beslissingsbevoegdheid wettelijk geregeld is: de vaststelling bij wet is nog wel mogelijk maar niet noodzakelijk. Dit wordt vervolgens bevestigd in het gemeenschappelijke standpunt van de Raad en in de goedgekeurde tekst, die beide spreken over de “vaststellende” instantie.

Tegen deze achtergrond kunnen in de ontstaansgeschiedenis twee belangrijke elementen worden onderscheiden: ten eerste kan een partij voor de verwerking verantwoordelijk zijn, ongeacht of er een specifieke wettelijke bevoegdheid bestaat voor de hoedanigheid van voor de verwerking van gegevens verantwoordelijke. In de tweede plaats wordt het vaststellen wie voor de verwerking verantwoordelijk is in de loop van het goedkeuringsproces van Richtlijn 95/46 een *communautair* begrip, met een vaste eigen betekenis in het Gemeenschapsrecht, onafhankelijk van – mogelijk uiteenlopende – bepalingen in het nationale recht. Dit laatste element is van wezenlijk belang voor een effectieve toepassing van de richtlijn en een goede bescherming in de lidstaten. Dat vereist een uniforme en dus autonome interpretatie van het kernbegrip “voor de verwerking verantwoordelijk”, dat in de richtlijn belangrijker wordt dan “houder van een bestand” in Verdrag 108.

Zo bezien vormt de richtlijn het sluitstuk van deze ontwikkeling, omdat in de richtlijn wordt bepaald dat de bevoegdheid om “vast te stellen” weliswaar specifiek bij wet geregeld kan zijn, maar doorgaans blijkt uit een analyse van feiten of omstandigheden: gekeken moet worden naar de desbetreffende specifieke verwerkingen en duidelijk moet worden wie deze vaststelt. Daarvoor moet in eerste instantie een antwoord worden gevonden op de vragen “Waarom vindt deze verwerking plaats?” en “Wie heeft deze geïnitieerd?”.

De hoedanigheid van voor de verwerking verantwoordelijke is primair het gevolg van de feitelijke omstandigheid dat een entiteit heeft besloten persoonsgegevens voor eigen doeleinden te verwerken. Een zuiver formeel criterium zou namelijk om ten minste twee redenen niet toereikend zijn: in bepaalde gevallen zou een formele aanstelling van een voor de verwerking verantwoordelijke – bijvoorbeeld in een wet, contract of aanmelding bij de autoriteit voor gegevensbescherming – gewoonweg ontbreken. In andere gevallen kan het voorkomen dat de formele aanstelling niet de realiteit weergeeft, bijvoorbeeld wanneer de rol van voor de verwerking verantwoordelijke formeel wordt toegekend aan een instantie die feitelijk niet in een positie verkeert om “vast te stellen”.

De relevantie van de feitelijke invloed is ook te zien in de SWIFT-zaak¹⁰, waarin SWIFT formeel werd beschouwd als gegevensverwerker maar in feite – in ieder geval in zekere mate – fungeerde als de voor de verwerking van gegevens verantwoordelijke. In deze zaak werd duidelijk dat de contractuele aanstelling van een partij als voor de verwerking van gegevens verantwoordelijke of als verwerker weliswaar relevante informatie kan bieden over de wettelijke hoedanigheid van die partij, maar dat een dergelijke contractuele aanstelling toch niet doorslaggevend is voor het vaststellen van de daadwerkelijke hoedanigheid van die partij, die uit concrete omstandigheden moet blijken.

Deze feitelijke benadering wordt ook gesteund door het gegeven dat de richtlijn bepaalt dat de voor de verwerking verantwoordelijke degene is die doel en middelen “vaststelt” en niet “rechtmatig vaststelt”. Alles draait om de vaststelling wie feitelijk voor de verwerking verantwoordelijk is, zelfs wanneer de aanstelling onrechtmatig lijkt of de verwerking van gegevens onrechtmatig plaatsvindt. Het is niet relevant of het besluit om gegevens te verwerken “rechtmatig” was in die zin dat de entiteit die een dergelijk besluit nam daartoe juridisch bevoegd was, of dat een voor de verwerking verantwoordelijke formeel werd aangesteld volgens een specifieke procedure. De vraag van de rechtmatigheid van de verwerking van persoonsgegevens is nog wel relevant in een ander stadium en zal worden bezien in het licht van andere artikelen (waaronder met name artikel 6-8) van de richtlijn. Met andere woorden: ook wanneer gegevens onrechtmatig worden verwerkt, moet de voor de verwerking verantwoordelijke eenvoudig kunnen worden gevonden en voor de verwerking verantwoordelijk worden gesteld.

Een laatste eigenschap van het begrip “voor de verwerking verantwoordelijke” is de autonomie daarvan, in die zin dat externe juridische bronnen weliswaar kunnen helpen om vast te stellen wie voor de verwerking verantwoordelijk is, maar dat het vooral moet worden geïnterpreteerd volgens de wetgeving voor gegevensbescherming¹¹. Aan het begrip “voor de verwerking verantwoordelijke” mag geen afbreuk worden gedaan door andere – soms strijdige of overlappende – begrippen uit andere rechtsgebieden, bijvoorbeeld dat van de maker of de rechthebbende in het intellectuele eigendomsrecht. Wie rechthebbende voor het intellectuele eigendom is, kan ook als “voor de verwerking verantwoordelijke” worden aangemerkt en dus moeten voldoen aan de verplichtingen uit de wetgeving voor gegevensbescherming.

¹⁰ In deze zaak worden bankgegevens die door SWIFT namens banken en financiële instellingen voor financiële transacties zijn verzameld aan de Amerikaanse autoriteiten overgedragen om de financiering van terrorisme te kunnen aanpakken.

¹¹ De raakvlakken met begrippen uit andere rechtsgebieden (bijvoorbeeld het begrip “rechthebbende” voor intellectueel eigendom of wetenschappelijk onderzoek, of aansprakelijkheid volgens het burgerlijk recht) worden hierna behandeld.

Noodzakelijke typologie

Het begrip “voor de verwerking verantwoordelijke” is een functioneel begrip, dat is bedoeld om verantwoordelijkheden te leggen op de plaats waar de feitelijke invloed ligt. Het is dus meer op een feitelijke dan op een formele analyse gebaseerd. Voor het bepalen van de verantwoordelijkheid kan dus soms een diepgaand en langdurig onderzoek noodzakelijk zijn. Met het oog op de effectiviteit moet echter worden gekozen voor een pragmatische benadering, om de voorspelbaarheid met betrekking tot de verantwoordelijkheid te waarborgen. Vanuit dit oogpunt zijn vuistregels en praktische aannames nodig om de toepassing van wetgeving voor gegevensbescherming te sturen en te vereenvoudigen.

Daarom moet de richtlijn zodanig worden geïnterpreteerd dat de “vaststellende instantie” in de meeste situaties eenvoudig en duidelijk kan worden aangegeven onder verwijzing naar de – juridische en/of feitelijke – omstandigheden waaruit feitelijke invloed normaal gesproken kan worden afgeleid, tenzij uit andere feiten het tegendeel blijkt.

Deze omstandigheden kunnen worden geanalyseerd en ingedeeld volgens onderstaande drie categorieën van situaties, die een systematische benadering van deze zaken mogelijk maken:

1) Verantwoordelijkheid op grond van een uitdrukkelijke juridische bevoegdheid. Hierover gaat het onder andere in het tweede deel van de definitie, dus wanneer de voor de verwerking verantwoordelijke of de specifieke criteria voor zijn aanstelling zijn vastgelegd in nationale of communautaire wetgeving. Het gebeurt niet vaak dat de aanstelling van de voor de verwerking verantwoordelijke uitdrukkelijk bij wet is geregeld. Wanneer dat wel het geval is, ontstaan doorgaans geen grote problemen. In sommige landen is in de nationale wetgeving vastgelegd dat overheidsdiensten in het kader van de hun opgedragen taken verantwoordelijk zijn voor de verwerking van persoonsgegevens.

Het komt echter vaker voor dat de voor de verwerking verantwoordelijke of de criteria voor zijn aanstelling niet rechtstreeks bij wet wordt (worden) benoemd of vastgesteld maar dat in die wet iemand wordt belast met het verzamelen en verwerken van bepaalde gegevens. Dit zou bijvoorbeeld het geval zijn wanneer een entiteit wordt belast met de uitvoering van bepaalde overheidstaken (bijvoorbeeld de sociale zekerheid) waarbij altijd persoonsgegevens worden vastgelegd, en dan een register opzet om deze taken te kunnen uitvoeren. In dat geval blijkt uit de wet wie voor de verwerking verantwoordelijk is. In meer algemene zin kan de wet publieke of private entiteiten verplichten bepaalde gegevens te bewaren of te verstrekken. Deze entiteiten zouden in dat verband dan normaliter worden beschouwd als de voor een verwerking van persoonsgegevens verantwoordelijke.

2) Verantwoordelijkheid op grond van een impliciete bevoegdheid. Dit is het geval wanneer de bevoegdheid tot vaststelling niet uitdrukkelijk bij wet is geregeld en evenmin rechtstreeks voortvloeit uit expliciete wettelijke bepalingen, maar wel stoelt op gemeenrechtelijke bepalingen of vaste juridische praktijken op verschillende gebieden (civiel recht, handelsrecht, arbeidsrecht enz.). In dit geval kan mede aan de hand van bestaande traditionele rollen, die doorgaans een bepaalde verantwoordelijkheid inhouden, worden vastgesteld wie voor de verwerking verantwoordelijk is, bijvoorbeeld een werkgever waar het gaat om gegevens van zijn werknemers, een uitgever waar het gaat om gegevens van abonnees of een vereniging waar het gaat om gegevens van leden of donateurs.

In al deze gevallen kan worden aangenomen dat de bevoegdheid om verwerkingsactiviteiten vast te stellen uit de aard der zaak gekoppeld is aan de functionele rol van een (private) organisatie waaraan uiteindelijk bepaalde verantwoordelijkheden zijn verbonden, ook vanuit een oogpunt van gegevensbescherming. Dit zou juridisch gezien het geval zijn, ongeacht of de bevoegdheid tot vaststelling bij de genoemde rechtspersonen zou liggen, zou worden uitgeoefend door de geëigende zelfstandig handelende organen of door een natuurlijke persoon met eenzelfde rol (zie hierna over het eerste element in punt c). Hetzelfde zou echter ook het geval zijn voor een overheidsdienst met bepaalde administratieve taken, in een land waar de verantwoordelijkheid van die dienst voor gegevensbescherming niet uitdrukkelijk bij wet is geregeld.

Voorbeeld 1: Telecombedrijven

Een interessant voorbeeld van wettelijke richtsnoeren voor de private sector heeft betrekking op de rol van telecombedrijven: in overweging 47 van Richtlijn 95/46/EG wordt verduidelijkt dat *“wanneer een bericht dat persoonsgegevens bevat, wordt verzonden via een telecommunicatie- of elektronische postdienst waarvan het enige doel is dit soort berichten door te geven, het de persoon is van wie het bericht uitgaat, en niet degene die de dienst aanbiedt, die normaliter zal worden beschouwd als verantwoordelijk voor de verwerking van de in het bericht vervatte persoonsgegevens; (...) dat evenwel de personen die deze diensten aanbieden normaliter zullen worden beschouwd als verantwoordelijk voor de verwerking van de aanvullende persoonsgegevens die noodzakelijk zijn voor de werking van de dienst”*. De aanbieder van telecommunicatiediensten behoort derhalve in beginsel alleen als voor de verwerking verantwoordelijke te worden beschouwd voor verkeers- en factureringsgegevens, en niet voor verzonden gegevens¹². Dit juridische richtsnoer van de communautaire wetgever sluit volledig aan bij de functionele benadering die in dit advies wordt gevolgd.

3) Verantwoordelijkheid door feitelijke invloed. In dit geval wordt de verantwoordelijkheid voor de verwerking toegewezen op basis van een beoordeling van de feitelijke omstandigheden. In veel gevallen wordt hiervoor een beoordeling gemaakt van de contractuele verhoudingen tussen de verschillende betrokken partijen. Op grond van deze beoordeling kunnen externe conclusies worden getrokken, waarbij de rol en verantwoordelijkheden van de voor de verwerking verantwoordelijke bij een of meer partijen worden neergelegd. Dit kan bijzonder nuttig zijn in gecompliceerde omgevingen, waar vaak gebruik wordt gemaakt van nieuwe informatietechnologie en relevante partijen vaak de neiging hebben zichzelf als “faciliterend” te beschouwen, en niet als voor de verwerking verantwoordelijk.

¹² Een gegevensbeschermingsautoriteit oordeelde over de verantwoordelijkheid in een zaak die aanhangig werd gemaakt door een betrokkene die klaagde over ongewenste reclame per e-mail. In zijn klacht verzocht betrokkene de aanbieder van het communicatienetwerk te bevestigen of te ontkennen dat e-mail met reclame vanuit dat netwerk was verzonden. De gegevensbeschermingsautoriteit verklaarde dat de onderneming, die slechts zijn klanten toegang tot een communicatienetwerk aanbiedt, dus de verzending van gegevens niet initieert en evenmin de geadresseerden selecteert of de informatie in het bericht wijzigt, niet als voor de verwerking van gegevens verantwoordelijk kan worden beschouwd.

Mogelijk wordt in een contract niets gezegd over de verantwoordelijkheid voor de verwerking, maar bevat het wel voldoende gegevens om de verantwoordelijkheid voor de verwerking te leggen bij een partij die klaarblijkelijk in dit opzicht een leidende rol vervult. In andere gevallen is een contract duidelijker over de verantwoordelijkheid voor de verwerking. Wanneer er geen aanleiding bestaat om te betwijfelen of hiermee de werkelijkheid op een juiste wijze wordt weergegeven, is er niets op tegen om aan te sluiten bij de contractbepalingen. De bepalingen van een contract zijn echter niet altijd doorslaggevend, omdat contractpartijen dan de verantwoordelijkheid naar eigen goeddunken zouden kunnen beleggen.

Het enkele feit dat iemand bepaalt op welke manier persoonsgegevens worden verwerkt, kan ertoe leiden dat hij wordt aangemerkt als voor de verwerking van de gegevens verantwoordelijk, hoewel deze kwalificatie buiten de werkingssfeer van een contractuele verhouding ontstaat of uitdrukkelijk door een contract wordt uitgesloten. Een duidelijk voorbeeld hiervan was de SWIFT-zaak, waarin deze onderneming het besluit nam om bepaalde persoonsgegevens – die oorspronkelijk namens financiële instellingen voor commerciële doeleinden werden verwerkt – ook beschikbaar te stellen met het oog op de bestrijding van de financiering van terrorisme, zoals verzocht in dagvaardingen van het Amerikaanse ministerie van Financiën.

Bij twijfel kunnen naast de bepalingen van een contract ook andere feiten nuttig zijn om vast te stellen wie voor de verwerking verantwoordelijk is, bijvoorbeeld de mate van feitelijke zeggenschap van een partij, het beeld dat aan betrokkenen wordt geschetst en redelijke verwachtingen van betrokkenen op basis van deze zichtbaarheid (zie ook hierna over het derde element in punt b). Deze categorie is bijzonder belangrijk omdat hiermee ook bij onrechtmatige gedragingen verantwoordelijkheden kunnen worden belegd en toegewezen, dus in gevallen waarin de feitelijke verwerkingsactiviteiten zelfs kunnen worden uitgeoefend in strijd met de belangen en tegen de wil van sommige partijen.

Voorlopige conclusie

Met de eerste twee van deze categorieën kan in beginsel beter worden bepaald wie de ‘vaststellende partij’ is. In de praktijk valt wellicht meer dan 80% van de relevante situaties in deze twee categorieën. Een formeel juridische aanstelling behoort echter in overeenstemming met de regelgeving voor gegevensbescherming te zijn, en te waarborgen dat de aangewezen instantie ook daadwerkelijk zeggenschap heeft over de verwerkingen. Anders gezegd: de juridische aanstelling moet in overeenstemming met de werkelijkheid zijn.

Voor categorie 3 is een diepgaande analyse vereist. In deze categorie kunnen sneller uiteenlopende interpretaties ontstaan. Vaak geven de bepalingen in een contract meer duidelijkheid, maar zij zijn niet altijd doorslaggevend. Steeds vaker menen betrokken partijen dat zij de verwerkingen niet vaststellen en er dus niet verantwoordelijk voor zijn. Een conclusie op basis van de feitelijke invloed is in die gevallen de enige haalbare mogelijkheid. De rechtmatigheid van deze verwerking wordt altijd nog getoetst aan andere artikelen (6-8).

Wanneer geen van bovengenoemde categorieën van toepassing is, moet de aanstelling van een voor de verwerking verantwoordelijke als nietig worden beschouwd. Een partij die geen juridische of feitelijke invloed heeft op de vaststelling van de wijze waarop persoonsgegevens worden verwerkt kan namelijk niet als voor de verwerking verantwoordelijk worden beschouwd.

Formeel gezien wordt deze benadering bevestigd door de overweging dat de definitie van de voor de verwerking van gegevens verantwoordelijke behoort te worden beschouwd als een bindende wettelijke bepaling, die partijen niet eenvoudigweg naast zich neer kunnen leggen of omzeilen. Vanuit strategisch oogpunt zou een dergelijke aanstelling strijdig zijn met een effectieve toepassing van de wetgeving inzake gegevensbescherming en de verantwoordelijkheid voor de gegevensverwerking teniet doen.

III.1.b) Derde element: “het doel van, en de middelen voor de verwerking”

Het derde element vertegenwoordigt het materiële deel van de toets: wat een partij moet vaststellen om als voor de verwerking verantwoordelijk te worden aangemerkt.

In de loop der tijd is deze bepaling aanzienlijk gewijzigd. In Verdrag 108 werd gesproken over het doel van de geautomatiseerde gegevensbestanden, de categorieën persoonsgegevens en de op die gegevens uit te voeren bewerkingen. De Commissie nam deze materiële elementen met kleine taalkundige aanpassingen over en voegde er de bevoegdheid aan toe om te besluiten welke derden toegang tot de gegevens hebben. Het gewijzigde voorstel van de Commissie ging van “de doelen van het gegevensbestand” meer in de richting van “de doelen en het oogmerk van de verwerking”, dus van een statische definitie (gekoppeld aan een gegevensbestand) naar een dynamische definitie (gekoppeld aan de verwerkingsactiviteit). In het gewijzigde voorstel werden nog steeds vier elementen onderscheiden (doelen/oogmerk, persoonsgegevens, bewerkingen en toegang van derden tot gegevens), die pas in het gemeenschappelijke standpunt van de Raad werden teruggebracht tot twee (“doelen en middelen”).

In woordenboeken wordt “doel” omschreven als “datgene waarnaar men streeft, dat men probeert te bereiken, te verwezenlijken” en “middel” als “datgene wat gebezigd wordt om een doel te bereiken, om ergens toe te komen”.

Anderzijds wordt in de richtlijn bepaald dat gegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Het is daarom van bijzonder groot belang om te bepalen wat de “doelen” van de verwerking zijn en welke “middelen” worden ingezet om die doelen te bereiken.

Verder is het zo dat degene die doelen en middelen vaststelt ook respectievelijk het “waarom” en het “hoe” van bepaalde verwerkingsactiviteiten bepaalt. Zo bezien, en omdat deze twee aspecten gekoppeld zijn, bestaat er behoefte aan richtsnoeren over de vraag hoeveel invloed een entiteit op het “waarom” en het “hoe” moet hebben om als voor de verwerking verantwoordelijk te worden beschouwd.

Wanneer moet worden beoordeeld wie doelen en middelen vaststelt, om zo te kunnen bepalen wie voor de verwerking verantwoordelijk is, staat daarom de vraag centraal hoe gedetailleerd iemand doelen en middelen moet vaststellen om als voor de verwerking verantwoordelijk te worden aangemerkt. Ook moet duidelijk worden hoeveel vrijheid van handelen een gegevensverwerker volgens de richtlijn mag hebben. Deze definities worden met name relevant wanneer meerdere partijen betrokken zijn bij de verwerking van persoonsgegevens en vastgesteld moet worden welke van deze partijen (alleen of samen met anderen) voor de verwerking van gegevens verantwoordelijk zijn en welke in plaats daarvan eventueel moeten worden beschouwd als gegevensverwerkers.

Het gewicht dat aan doelen of middelen moet worden toegekend, kan afhangen van de specifieke situatie waarbinnen de verwerking plaatsvindt.

Dit vraagt om een pragmatische benadering, waarin een groter gewicht wordt toegekend aan de vrijheid van handelen bij het vaststellen van doelen en aan de manoeuvreerruimte bij het nemen van beslissingen. In deze gevallen is het de vraag waarom de verwerking plaatsvindt en wat de rol is van mogelijk betrokken partijen, bijvoorbeeld van bedrijven waaraan werkzaamheden worden uitbesteed: zouden dergelijke bedrijven gegevens hebben verwerkt wanneer dat niet door de voor de verwerking verantwoordelijke zou zijn gevraagd, en onder welke voorwaarden? Verder kan een verwerker opereren op basis van algemene richtsnoeren waarin met name de doelen worden omschreven en niet uitvoerig wordt ingegaan op details met betrekking tot de middelen.

Voorbeeld 2: Mailings

Onderneming ABC sluit met een aantal organisaties contracten voor de uitvoering van zijn mailingcampagnes en voor zijn salarisverwerking. Hij geeft duidelijke aanwijzingen (welk marketingmateriaal moet worden verzonden en aan wie, en wie hoeveel betaald moet krijgen op welke datum enz.). Hoewel de organisaties enige vrijheid van handelen hebben (onder meer ten aanzien van de te gebruiken software) zijn hun taken tamelijk duidelijk en strak omschreven en hoewel het mailingbedrijf adviezen kan geven (bijvoorbeeld om geen mailings in augustus te versturen) is het duidelijk dat het volgens de aanwijzingen van ABC te werk moet gaan. Bovendien mag slechts één partij (onderneming ABC) de verwerkte gegevens gebruiken. Alle andere partijen moeten aannemen dat ABC deze gegevens rechtmatig gebruikt wanneer vragen worden gesteld over hun juridische bevoegdheid om de gegevens te verwerken. In dit geval is het duidelijk dat onderneming ABC voor de verwerking van gegevens verantwoordelijk is en dat alle afzonderlijke organisaties als verwerkers kunnen worden beschouwd voor de specifieke verwerking van gegevens die namens de onderneming plaatsvindt.

Waar het gaat om het vaststellen van middelen is het begrip “middelen” natuurlijk erg breed, zoals ook blijkt uit de ontstaansgeschiedenis van deze definitie. In het oorspronkelijke voorstel is iemand voor de verwerking verantwoordelijk wanneer hij vier dingen vaststelt (doelen/oogmerk, persoonsgegevens, bewerkingen en de toegang van derden). De uiteindelijke formulering van de bepaling, waarin alleen “doelen en middelen” zijn overgebleven, kan niet als strijdig met de oudere versie worden beschouwd omdat het geen enkele twijfel lijdt dat de voor de verwerking verantwoordelijke bijvoorbeeld moet vaststellen welke gegevens moeten worden verwerkt voor het beoogde doel. Daarom moet de uiteindelijke definitie veeleer worden opgevat als een ingekorte versie, waarin toch de geest van de oudere versie bewaard is gebleven. Met andere woorden: “middelen” slaat niet alleen op de technische wijzen waarop persoonsgegevens worden verwerkt, maar ook op het “hoe” van de verwerking, waartoe ook vragen behoren als “Welke gegevens moeten worden verwerkt?”, “Welke derden moeten toegang tot deze gegevens hebben?”, “Wanneer moeten gegevens worden gewist?” enz.

Bij het vaststellen van de “middelen” gaat het dus niet alleen om technische en organisatorische vragen, die heel goed aan verwerkers kunnen worden gedelegeerd (bijvoorbeeld de vraag welke hard- of software moet worden gebruikt), maar ook om wezenlijke aspecten, die gewoonlijk door de voor de verwerking verantwoordelijke

worden vastgesteld, waaronder “Welke gegevens moeten worden verwerkt?”, “Hoe lang moeten zij worden verwerkt?”, “Voor wie moeten zij toegankelijk zijn?” enzovoort.

Wie het doel van de verwerking vaststelt, wordt tegen deze achtergrond dan in ieder geval als voor de verwerking verantwoordelijk aangemerkt, terwijl bij het vaststellen van de middelen alleen van verantwoordelijkheid sprake is wanneer die vaststelling betrekking heeft op de wezenlijke aspecten van de middelen.

Zo bezien kunnen technische en organisatorische middelen zeer wel alleen door de gegevensverwerker worden vastgesteld.

In deze gevallen – waarin doelen goed zijn omschreven, maar weinig of geen aanwijzingen worden gegeven over technische en organisatorische middelen – moeten de gestelde doelen redelijkerwijs met de middelen kunnen worden bereikt en behoort de voor de verwerking van de gegevens verantwoordelijke volledig op de hoogte te zijn van de gebruikte middelen. Wanneer een aannemer invloed heeft op het doel en gegevens (ook) voor eigen doeleinden kan verwerken, bijvoorbeeld door de ontvangen persoonsgegevens te gebruiken voor het ontwikkelen van diensten met toegevoegde waarde, dan zou hij verantwoordelijk (of mogelijk mede verantwoordelijk) voor een andere verwerking zijn en zouden alle verplichtingen van de toepasselijke wetgeving voor gegevensbescherming voor hem gelden.

Voorbeeld 3: Een onderneming wordt aangemerkt als gegevensverwerker maar handelt als voor de verwerking verantwoordelijke

Onderneming MarketinZ verricht voor meerdere ondernemingen diensten op het gebied van reclame en direct marketing. Onderneming GoodProductZ sluit een contract met MarketinZ, waarin wordt overeengekomen dat laatstgenoemd bedrijf reclame gaat maken bij klanten van GoodProductZ en als gegevensverwerker wordt aangemerkt. MarketinZ besluit echter om de klantgegevens van GoodProductZ ook te gebruiken om reclame te maken voor producten van andere klanten. Dit besluit, dus om de persoonsgegevens naast het doel waarvoor zij werden overgedragen nog voor een ander doel te gebruiken, maakt MarketinZ voor deze verwerking een voor de verwerking van gegevens verantwoordelijke. De rechtmatigheid van deze verwerking wordt altijd nog getoetst aan andere artikelen (6-8).

In sommige rechtsstelsels zijn beslissingen over beveiligingsmaatregelen bijzonder belangrijk omdat beveiligingsmaatregelen uitdrukkelijk worden beschouwd als een wezenlijk kenmerk, dat wordt vastgesteld door degene die voor de verwerking verantwoordelijk is. Hierbij rijst de vraag welke beslissingen over beveiliging ertoe leiden dat een onderneming waaraan de verwerking is uitbesteed als voor de verwerking verantwoordelijk wordt aangemerkt.

Voorlopige conclusie

Het vaststellen van het “doel” van de verwerking is voorbehouden aan de “voor de verwerking verantwoordelijke”. Degene die in dezen beslist is derhalve (de facto) voor de verwerking verantwoordelijk. Het vaststellen van de “middelen” voor de verwerking kan door de voor de verwerking verantwoordelijke worden gedelegeerd wanneer het gaat om technische of organisatorische zaken. Kernvragen met betrekking tot de

rechtmatigheid van de verwerking vallen onder de bevoegdheid van de voor de verwerking verantwoordelijke. De persoon of entiteit die bijvoorbeeld besluit hoe lang gegevens moeten worden opgeslagen of voor wie de verwerkte gegevens toegankelijk moeten zijn, handelt voor dit deel van het gebruik van de gegevens als “voor de verwerking verantwoordelijke” en moet derhalve voldoen aan alle verplichtingen die voor een voor de verwerking verantwoordelijke gelden.

III.1.c) Eerste element: “de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam”

Het eerste element van de definitie verwijst naar het personele aspect: wie kan voor de verwerking verantwoordelijk zijn en dus uiteindelijk verantwoordelijk worden gehouden voor de naleving van de verplichtingen uit de richtlijn? De definitie komt volledig overeen met de formulering van artikel 2 van Verdrag 108 en leidde bij de totstandkoming van de richtlijn niet tot specifieke discussie. Volgens de definitie kunnen vele partijen de rol van voor de verwerking verantwoordelijke vervullen, uiteenlopend van natuurlijke tot rechtspersonen, maar ook “enig ander lichaam”.

Aan de hand van dit aspect moet de richtlijn zodanig kunnen worden geïnterpreteerd dat een effectieve toepassing ervan mogelijk is. Daarvoor moet worden bevorderd dat altijd duidelijk en ondubbelzinnig kan worden vastgesteld wie voor de verwerking verantwoordelijk is, ongeacht of een formele aanstelling al dan niet heeft plaatsgevonden en openbaar is gemaakt.

Allereerst is het van belang om zo weinig mogelijk af te wijken van de praktijk die zowel in de publieke als de private sector is ontstaan op andere rechtsgebieden, waaronder civiel recht, bestuursrecht en strafrecht. In de meeste gevallen blijkt uit deze bepalingen welke personen of instanties verantwoordelijk moeten worden gehouden en maken zij het in beginsel mede mogelijk om vast te stellen wie voor de verwerking van gegevens verantwoordelijk is.

Vanuit het strategische oogpunt van het beleggen van verantwoordelijkheden, en om betrokkenen stelselmatig duidelijkheid te bieden over de vraag waar zij hun rechten op grond van de richtlijn kunnen uitoefenen, moet bij voorkeur de onderneming of instantie zelf als voor de verwerking verantwoordelijk worden beschouwd, en niet een specifieke persoon binnen de onderneming of instantie. De onderneming of instantie zal uiteindelijk worden beschouwd als de partij die verantwoordelijk is voor de verwerking van gegevens en de naleving van de wettelijke verplichtingen voor gegevensbescherming, tenzij duidelijk blijkt dat een natuurlijke persoon verantwoordelijk is. In algemene zin moet worden aangenomen dat een onderneming of instantie als zodanig verantwoordelijk is voor de verwerkingen die plaatsvinden in het kader van de activiteiten en risico's van die onderneming of instantie.

Soms stellen ondernemingen en overheidsorganen een specifieke persoon aan als verantwoordelijke voor de uitvoering van de verwerkingen. Ook in dergelijke gevallen, wanneer een specifieke natuurlijke persoon wordt aangesteld om de naleving van de beginselen voor gegevensbescherming te waarborgen of om persoonsgegevens te verwerken, is deze persoon echter niet de voor de verwerking verantwoordelijke maar handelt hij/zij namens de rechtspersoon (onderneming of overheidsorgaan), die in zijn hoedanigheid van voor de verwerking verantwoordelijke aansprakelijk blijft voor inbreuken op de beginselen¹³.

¹³ Een vergelijkbare redenering wordt gevolgd met betrekking tot Verordening (EG) nr. 45/2001, waarin in artikel 2 onder (d) sprake is van “de communautaire instelling of het communautaire orgaan, het

Met name voor grote en complexe organisaties is het voor het beheer van de gegevensbescherming van cruciaal belang om zowel de verantwoordelijkheid van de natuurlijke persoon die de onderneming vertegenwoordigt als de concrete functionele verantwoordelijkheden binnen de organisatie duidelijk te regelen, bijvoorbeeld door andere personen aan te stellen als vertegenwoordigers of contactpersonen voor betrokkenen.

Nader onderzoek is noodzakelijk wanneer een natuurlijke persoon die binnen een rechtspersoon handelt gegevens gebruikt voor eigen doeleinden, die buiten het kader van de activiteiten van de rechtspersoon en het toezicht daarop vallen. In dat geval zou de betrokken natuurlijke persoon verantwoordelijk zijn voor de vastgestelde verwerking, en daarnaast ook verantwoordelijk voor dit gebruik van persoonsgegevens. Degene die oorspronkelijk voor de verwerking verantwoordelijk was, zou niettemin enige verantwoordelijkheid kunnen behouden wanneer de nieuwe verwerking kan plaatsvinden als gevolg van ontoereikende beveiligingsmaatregelen.

Zoals reeds aangegeven, is de rol van de voor de verwerking verantwoordelijke van cruciaal belang en bijzonder relevant wanneer aansprakelijkheid moet worden vastgesteld en sancties moeten worden opgelegd. Hoewel aansprakelijkheid en sancties per lidstaat verschillen, omdat zij volgens nationaal recht worden opgelegd, lijkt het geen twijfel dat de noodzaak om duidelijk vast te stellen welke natuurlijke of rechtspersoon verantwoordelijk is voor inbreuken op de wetgeving inzake gegevensbescherming een wezenlijke randvoorwaarde is voor een effectieve toepassing van de richtlijn.

Vaststellen wie voor de verwerking verantwoordelijk is, zal vanuit een oogpunt van gegevensbescherming in de praktijk nauw verweven zijn met de voor natuurlijke of rechtspersonen geldende regels uit het civiel recht, bestuursrecht of strafrecht voor het toewijzen van verantwoordelijkheden of het opleggen van sancties¹⁴.

De civielrechtelijke aansprakelijkheid zou in dit verband niet tot specifieke problemen behoren te leiden omdat deze in beginsel geldt voor zowel rechtspersonen als natuurlijke personen. Straf- en/of bestuursrechtelijke aansprakelijkheid is, afhankelijk van het nationale recht, in sommige gevallen wel mogelijk, maar dan alleen waar het gaat om natuurlijke personen. Wanneer het desbetreffende nationale recht voorziet in strafrechtelijke of bestuursrechtelijke sancties voor inbreuk op de regels voor gegevensbescherming, wordt in dat recht doorgaans ook bepaald wie verantwoordelijk is: wanneer de strafrechtelijke of bestuursrechtelijke aansprakelijkheid van rechtspersonen niet wordt erkend, zouden functionarissen van rechtspersonen volgens de specifieke regels van het nationale recht aansprakelijk kunnen worden gesteld¹⁵.

directoraat-generaal, de eenheid of enig andere organisatieafdeling". In de toezichtspraktijk is voldoende duidelijk geworden dat ambtenaren van instellingen en organen van de EU die als "voor de verwerking verantwoordelijke" zijn aangesteld, optreden namens het orgaan waarvoor zij werkzaam zijn.

¹⁴ Zie van de Commissie de Vergelijkende studie naar de situatie in de 27 lidstaten met betrekking tot de wetgeving inzake niet-contractuele verplichtingen voortvloeiend uit inbreuken op de persoonlijke levenssfeer en aan persoonlijkheid verbonden rechten van februari 2009, verkrijgbaar op http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

¹⁵ Dit laat onverlet dat nationale wetten kunnen voorzien in strafrechtelijke of bestuursrechtelijke aansprakelijkheid, niet alleen van de voor de verwerking verantwoordelijke, maar ook van eenieder die de wetgeving inzake gegevensbescherming overtreedt.

In de Europese wetgeving bestaan nuttige voorbeelden van criteria voor de strafrechtelijke verantwoordelijkheid¹⁶, met name wanneer een overtreding wordt begaan ten voordele van de rechtspersoon: in dergelijke gevallen kan eenieder aansprakelijk worden gesteld die “individueel of als onderdeel van een orgaan van de rechtspersonen handelt, die een leidinggevende functie binnen de rechtspersoon bekleedt, blijkend uit een of meer van de onderstaande punten:

- (a) de bevoegdheid om de rechtspersoon te vertegenwoordigen,
- (b) de bevoegdheid om namens de rechtspersoon besluiten te nemen,
- (c) de bevoegdheid om binnen de rechtspersoon zeggenschap uit te oefenen.”

Voorlopige conclusie

Samenvattend kan uit bovenstaande overwegingen worden geconcludeerd dat voor overtredingen op het gebied van gegevensbescherming altijd de voor de verwerking verantwoordelijke aansprakelijk is, dus de rechtspersoon (onderneming of overheidsorgaan) of de natuurlijke persoon die formeel volgens de criteria van de richtlijn is geïdentificeerd. Wanneer een natuurlijke persoon die werkzaam is bij een onderneming of overheidsinstantie gegevens voor eigen doeleinden gebruikt buiten het kader van de activiteiten van de onderneming, wordt deze persoon als de facto voor de verwerking verantwoordelijk beschouwd en is hij als zodanig aansprakelijk.

Voorbeeld 4: Heimelijk toezicht op werknemers

Een directielid van een onderneming besluit om heimelijk toezicht te houden op de werknemers van de onderneming, hoewel dit besluit niet formeel door de directie is bekrachtigd. De onderneming dient als voor de verwerking verantwoordelijke te worden beschouwd en is aansprakelijk jegens de werknemers van wie de persoonsgegevens zijn misbruikt.

De aansprakelijkheid van de onderneming vloeit met name voort uit het feit dat deze als voor de verwerking verantwoordelijke verplicht is om de naleving van de regelgeving met betrekking tot beveiliging en vertrouwelijkheid te waarborgen. Misbruik door een functionaris van de onderneming of een werknemer kan worden beschouwd als een gevolg van ontoereikende beveiligingsmaatregelen. Dit staat los van een eventuele aansprakelijkheidsstelling in een later stadium van het directielid of andere natuurlijke personen binnen de onderneming, zowel vanuit civielrechtelijk – ook jegens de onderneming – als vanuit strafrechtelijk oogpunt. Dat kan bijvoorbeeld het geval zijn wanneer het directielid de verzamelde gegevens gebruikt om persoonlijke gunsten van werknemers te verkrijgen: het moet dan als “voor de verwerking verantwoordelijke” worden beschouwd en is aansprakelijk voor dit specifieke gebruik van gegevens.

¹⁶ Zie onder meer Richtlijn 2008/99/EG van 19 november 2008 inzake de bescherming van het milieu door middel van het strafrecht, kaderbesluit van de Raad van 13 juni 2002 over de bestrijding van terrorisme. Rechtsinstrumenten stoelen ofwel op artikel 29, artikel 31 onder (e) en artikel 34, lid 2 onder (b) VEU of zijn in overeenstemming met de rechtsgrondslag van instrumenten die in de eerste pijler worden gebruikt en voortvloeien uit de jurisprudentie van het HvJ in de zaken C-176/03, COM/Raad, [Jurispr.] 2005, I-7879 en C-440/05, COM/Raad, [Jurispr.] 2007, I-9097. Zie ook de mededeling van de Commissie, COM (2005) 583 def.).

III.1.d) Tweede element: “die, respectievelijk dat, alleen of tezamen met anderen”

Deze paragraaf sluit aan bij bovenstaande analyse van de standaardkenmerken van een voor de verwerking verantwoordelijke en behandelt gevallen waarin meerdere partijen betrokken zijn bij de verwerking van persoonsgegevens. In steeds meer gevallen treden namelijk verschillende partijen op als voor de verwerking verantwoordelijke, en de definitie in de richtlijn houdt hier rekening mee.

De mogelijkheid dat de voor de verwerking verantwoordelijke “alleen of tezamen met anderen” handelt, kwam niet voor in Verdrag 108 en werd eigenlijk pas door het Europees Parlement ingebracht vóór de goedkeuring van de richtlijn. In het advies van de Commissie over het amendement van het EP verwijst de Commissie naar de mogelijkheid dat “voor één verwerking een aantal partijen gezamenlijk het doel van, en de middelen voor de te verrichten verwerking vaststelt” en dat daarom in een dergelijk geval “*elk van de voor de verwerking mede verantwoordelijken moet worden geacht onderworpen te zijn aan de verplichtingen van de richtlijn ter bescherming van de natuurlijke personen van wie de gegevens worden verwerkt*”.

Het advies van de Commissie ging deels voorbij aan de huidige complexe realiteit van de gegevensverwerking omdat het slechts betrekking had op een situatie waarin alle voor de verwerking verantwoordelijken een even grote invloed hebben bij de vaststelling van één enkele verwerking en daar in gelijke mate verantwoordelijk voor zijn. In werkelijkheid blijkt dat dit slechts een van de verschillende mogelijke soorten “gezamenlijke verantwoordelijkheid” is. In dit verband moet “tezamen” worden geïnterpreteerd als “samen met” of “niet alleen” in verschillende vormen en combinaties.

Allereerst moet worden opgemerkt dat de kans dat meerdere partijen betrokken zijn bij de verwerking van persoonsgegevens uiteraard afhangt van de vele soorten activiteiten die volgens de richtlijn kunnen neerkomen op de “verwerking” waarop de “gezamenlijke verantwoordelijkheid” uiteindelijk betrekking heeft. De definitie van verwerking uit artikel 2, onder b), van de richtlijn sluit niet uit dat verschillende partijen betrokken kunnen zijn bij verschillende bewerkingen of gehelen van bewerkingen op persoonsgegevens. Deze bewerkingen kunnen gelijktijdig of in verschillende fasen plaatsvinden.

In een dergelijke complexe omgeving is het nog belangrijker dat rollen en verantwoordelijkheden eenvoudig kunnen worden toegewezen, om te waarborgen dat de complexiteit van een gezamenlijke verantwoordelijkheid niet leidt tot een onwerkbare spreiding van verantwoordelijkheden die de wetgeving voor gegevensbescherming minder effectief zou maken. Door de vele mogelijke constructies kan echter helaas geen volledige en “afgeronde” lijst of classificatie van de verschillende soorten “gezamenlijke verantwoordelijkheid” worden opgesteld. Het is echter wel nuttig om ook in dit verband richtsnoeren te geven, zowel in de vorm van een aantal categorieën en voorbeelden van gezamenlijke verantwoordelijkheid als aan de hand van feitelijke omstandigheden waaruit gezamenlijke verantwoordelijkheid kan worden afgeleid of verondersteld.

In algemene zin behoort een gezamenlijke verantwoordelijkheid op dezelfde wijze te worden beoordeeld als een “individuele” verantwoordelijkheid, zoals hierboven omschreven in paragraaf III.1.a tot en met c. Zo moet ook bij het beoordelen van gezamenlijke verantwoordelijkheid een uitvoerige en functionele benadering worden gevolgd, zoals hierboven omschreven, gericht op de vraag of de doelen en middelen door meer dan één partij worden vastgesteld.

Voorbeeld 5: Aanbrengen van videobewakingscamera's

De eigenaar van een gebouw sluit een contract met een beveiligingsbedrijf, waarin wordt overeengekomen dat het beveiligingsbedrijf namens de voor de verwerking verantwoordelijke in delen van het gebouw enkele camera's plaatst. De doelen van de videobewaking en de wijze waarop de beelden worden verzameld en opgeslagen worden uitsluitend door de eigenaar van het gebouw vastgesteld. Deze dient daarom te worden beschouwd als de enige die voor deze verwerking verantwoordelijk is.

In dit verband kunnen contractbepalingen ook nuttig zijn bij het beoordelen van een gezamenlijke verantwoordelijkheid. Zij dienen echter altijd te worden getoetst aan de feitelijke omstandigheden van de relatie tussen de partijen

Voorbeeld 6: Headhunters

Headhunterz B.V. ondersteunt Enterprize N.V. bij de werving van nieuw personeel. In het contract wordt duidelijk bepaald dat "Headhunterz B.V. namens Enterprize optreedt en bij het verwerken van persoonsgegevens als gegevensverwerker handelt. Enterprize is als enige voor de verwerking van gegevens verantwoordelijk". Headhunterz B.V. verkeert echter in een onduidelijke positie: enerzijds vervult het naar werkzoekenden de rol van voor de verwerking verantwoordelijke, terwijl het anderzijds veronderstelt dat het verwerker is, die handelt namens de voor de verwerking verantwoordelijken, waaronder Enterprize B.V. en andere ondernemingen waarvoor het personeel werft. Verder zoekt Headhunterz – met zijn bekende toegevoegde-waarde-dienst "Global match" – naar geschikte kandidaten in zowel de cv's die rechtstreeks bij Enterprize binnenkomen als in de cv's die het reeds in zijn uitgebreide database heeft opgeslagen. Zo kan Headhunterz, dat volgens het contract alleen wordt betaald voor daadwerkelijk getekende arbeidsovereenkomsten, vraag en aanbod van banen beter op elkaar afstemmen en dus meer inkomsten genereren. Op grond van het bovenstaande kan worden gezegd dat Headhunterz B.V., in tegenstelling tot hetgeen in het contract is bepaald, moet worden beschouwd als een voor de verwerking verantwoordelijke, en samen met Enterprize B.V. als gezamenlijk verantwoordelijke voor in ieder geval de bewerkingen die verband houden met de werving voor Enterprize.

Zo gezien is van gezamenlijke verantwoordelijkheid sprake wanneer verschillende partijen voor specifieke verwerkingen het doel, de wezenlijke onderdelen of de middelen vaststellen die een voor de verwerking verantwoordelijke kenmerken (zie bovenstaande paragraaf III.1.a tot en met c).

Bij een gezamenlijke verantwoordelijkheid kunnen de partijen in verschillende mate betrokken zijn bij de gezamenlijke vaststelling en hoeft hun inbreng niet even groot te zijn. Wanneer er namelijk sprake is van meerdere partijen, kunnen zij zeer nauwe banden hebben (en bijvoorbeeld alle doelen en middelen van een verwerking delen) of een lossere relatie hebben (en bijvoorbeeld alleen doelen of middelen delen). Daarom moet een breed scala van typologieën voor gezamenlijke verantwoordelijkheid worden onderzocht en moeten hun juridische gevolgen worden beoordeeld. Daarbij dient enige souplesse te worden betracht, om rekening te houden met de toenemende complexiteit van de huidige realiteit van de gegevensverwerking.

Tegen deze achtergrond moet een oplossing worden gezocht voor de uiteenlopende mate waarin meerdere partijen bij de verwerking van persoonsgegevens contact of onderlinge relaties kunnen hebben.

Allereerst betekent het enkele feit dat meerdere betrokkenen samenwerken bij de verwerking van persoonsgegevens, bijvoorbeeld in een keten, niet dat zij in alle gevallen gezamenlijk verantwoordelijk zijn omdat de uitwisseling van gegevens tussen twee partijen zonder dat daarbij doelen of middelen worden gedeeld in een gemeenschappelijk geheel van verwerkingen alleen moet worden beschouwd als een overdracht van gegevens tussen afzonderlijke voor de verwerking verantwoordelijken.

Voorbeeld 7: Reisbureau (1)

Een reisbureau stuurt bij reserveringen voor pakketreizen de persoonsgegevens van zijn klanten naar de luchtvaartmaatschappijen en een hotelketen. De luchtvaartmaatschappij en het hotel bevestigen de beschikbaarheid van de aangevraagde stoelen en kamers. Het reisbureau stelt de reisdocumenten en vouchers voor zijn klanten op. In dit geval zijn het reisbureau, de luchtvaartmaatschappij en het hotel drie verschillende voor de verwerking verantwoordelijken, die alle drie voor hun eigen verwerking van persoonsgegevens moeten voldoen aan de verplichtingen met betrekking tot gegevensbescherming.

De beoordeling kan echter anders uitvallen wanneer verschillende partijen zouden besluiten om een gezamenlijke infrastructuur op te zetten om hun eigen individuele doelen te bereiken. Wanneer deze partijen bij het opzetten van die infrastructuur de wezenlijke aspecten van de te gebruiken middelen vaststellen, moeten zij als gezamenlijk voor de verwerking van gegevens verantwoordelijk worden aangemerkt – in ieder geval in die mate – ook wanneer zij niet noodzakelijkerwijs dezelfde doelen nastreven.

Voorbeeld 8: Reisbureau (2)

Het reisbureau, de hotelketen en de luchtvaartmaatschappij besluiten om een gemeenschappelijk online platform te ontwikkelen om beter te kunnen samenwerken bij reserveringen. Zij bereiken overeenstemming over belangrijke aspecten van de te gebruiken middelen, waaronder welke gegevens zullen worden opgeslagen, de wijze waarop reserveringen worden toegewezen en bevestigd en wie toegang tot de opgeslagen informatie heeft. Daarnaast besluiten zij de gegevens van hun klanten te delen om hun marketingactiviteiten te kunnen integreren.

In dit geval zijn het reisbureau, de luchtvaartmaatschappij en de hotelketen gezamenlijk verantwoordelijk voor de wijze waarop persoonsgegevens van hun respectieve klanten worden verwerkt en zijn zij daarom gezamenlijk voor de verwerking verantwoordelijk waar het gaat om de verwerkingen voor het gemeenschappelijke online boekingsplatform. Elk van hen zou echter individueel verantwoordelijk blijven voor andere verwerkingen, bijvoorbeeld in verband met hun personeelsbeheer.

In sommige gevallen verwerken meerdere partijen dezelfde persoonsgegevens na elkaar. Waarschijnlijk lijken de verschillende verwerkingen in de keten op microniveau dan los van elkaar te staan omdat zij elk een verschillend doel hebben. Op macroniveau moet

echter extra worden nagegaan of deze verwerkingen niet moeten worden beschouwd als een “geheel van verwerkingen” met een gezamenlijk doel of met gebruikmaking van gezamenlijk vastgestelde middelen.

De volgende twee voorbeelden verduidelijken dit aan de hand van twee mogelijke verschillende scenario's.

Voorbeeld 9: Overdracht van personeelsgegevens aan de belastingdienst

Onderneming XYZ verzamelt en verwerkt persoonsgegevens van zijn werknemers voor het beheer van salarissen, dienstreizen, zorgverzekeringen enz.. De onderneming is echter ook wettelijk verplicht om alle salarisgegevens aan de belastingdienst op te geven, met het oog op een betere belastingcontrole.

Hoewel onderneming XYZ en de belastingdienst in dit geval dezelfde salarisgegevens verwerken, zullen de twee entiteiten als twee afzonderlijke voor de verwerking verantwoordelijken worden aangemerkt omdat er in onvoldoende mate sprake is van een gezamenlijk doel of gezamenlijke middelen voor deze gegevensverwerking.

Voorbeeld 10: Financiële transacties

Laten we nu eens kijken naar een bank, die voor zijn financiële transacties gebruikmaakt van de diensten van een aanbieder van financieel berichtenverkeer. De bank en de aanbieder zijn het eens over de middelen voor de verwerking van financiële gegevens. De persoonsgegevens voor financiële transacties worden in eerste instantie door de financiële instelling verwerkt en pas later door de aanbieder van het financiële berichtenverkeer. Hoewel deze betrokkenen op microniveau elk hun eigen doelen hebben, zijn de verschillende fasen, doelen en middelen van de verwerking op macroniveau nauw met elkaar verbonden. In dit geval kunnen zowel de bank als de aanbieder van het berichtenverkeer als gezamenlijk voor de verwerking verantwoordelijk worden beschouwd.

In andere gevallen stellen de diverse betrokken partijen gezamenlijk, en in sommige gevallen in verschillende mate, de doelen en/of middelen van een verwerkingsbewerking vast.

Soms is elke partij slechts voor een deel van de verwerking verantwoordelijk, maar wordt de informatie via een platform samengebracht en verwerkt.

Voorbeeld 11: Portalen voor eOverheid

Portalen voor eOverheid fungeren als schakel tussen de burger en overheidsdiensten: het portaal zendt verzoeken van burgers door en plaatst de documenten van de overheidsdienst zodat zij door de burger kunnen worden opgevraagd. Elke overheidsdienst blijft verantwoordelijk voor de verwerking van de gegevens voor de eigen doeleinden. Toch kan ook het portaal zelf als voor de verwerking verantwoordelijk worden beschouwd. Het verwerkt namelijk zowel aanvragen van burgers (deze worden verzameld en doorgestuurd naar de bevoegde dienst) als overheidsdocumenten (deze worden op het portaal geplaatst en ontsloten, bijvoorbeeld voor burgers die ze kunnen downloaden) voor andere doeleinden (bevorderen van eOverheidsdiensten) dan waarvoor de gegevens oorspronkelijk door elke overheidsdienst werden verwerkt.

Deze voor de verwerking verantwoordelijken moeten onder meer waarborgen dat persoonsgegevens van de gebruiker veilig naar het systeem van de overheidsdienst worden verzonden, omdat deze overdracht op macroniveau een wezenlijk onderdeel is van het geheel van verwerkingen dat via het portaal plaatsvindt.

Een andere mogelijke opzet is de “herkomstgebaseerde benadering”, waarvan sprake is wanneer elke voor de verwerking verantwoordelijke kan worden aangesproken op de gegevens die hij in het systeem inbrengt. Dit is het geval bij sommige EU-brede databases, waar de verantwoordelijkheid – en dus de verplichting om te reageren op verzoeken om toegang en rectificatie – wordt belegd op basis van de nationale herkomst van persoonsgegevens.

Een ander interessant scenario houdt verband met sociale netwerken op internet:

Voorbeeld 12: Sociale netwerken

Aanbieders van sociale netwerken bieden online communicatieplatforms aan, waarop gebruikers informatie kunnen publiceren en met andere gebruikers kunnen uitwisselen. Deze aanbieders zijn voor de verwerking van de gegevens verantwoordelijk, omdat zij zowel de doelen van, als de middelen voor de verwerking van dergelijke informatie vaststellen. De gebruikers van deze netwerken, die ook van derden persoonsgegevens uploaden, zouden moeten worden aangemerkt als voor de verwerking verantwoordelijken voor zover hun activiteiten niet onder de zogenoemde “vrijstelling voor huishoudelijk gebruik” vallen¹⁷.

Na onderzoek van gevallen waarin de verschillende betrokkenen gezamenlijk slechts een deel van de doelen en middelen vaststellen is de volgende situatie glashelder en eenvoudig: meerdere betrokkenen stellen gezamenlijk alle doelen van, en middelen voor verwerkingsactiviteiten vast en delen deze, zodat een volledig gezamenlijke verantwoordelijkheid ontstaat.

In dit laatste geval kan eenvoudig worden vastgesteld wie bevoegd is en in de positie verkeert om de rechten van betrokkenen te waarborgen en tegelijkertijd te voldoen aan de verplichtingen met betrekking tot gegevensbescherming. Wanneer de diverse gezamenlijk verantwoordelijken echter niet allen evenveel gewicht in de schaal leggen bij het vaststellen van doelen en middelen van de verwerking is het is echter veel moeilijker om vast te stellen welke voor de verwerking verantwoordelijke bevoegd – en aansprakelijk – is voor welke rechten en plichten van betrokkenen.

Verdeling van verantwoordelijkheid verduidelijken

Allereerst moet er op gewezen worden dat, met name wanneer van gezamenlijke verantwoordelijkheid sprake is, het feit dat een partij niet rechtstreeks alle verplichtingen van de voor de verwerking verantwoordelijke kan nakomen (waarborgen van informatievoorziening, recht van toegang enz.) niet uitsluit dat deze partij de voor de verwerking verantwoordelijke is. Mogelijk kan in de praktijk gemakkelijk – namens de voor de verwerking verantwoordelijke – aan deze verplichting worden voldaan door andere partijen, die soms dichter bij de betrokkenen staan. Wel blijft een voor de

¹⁷ Voor nadere bijzonderheden en voorbeelden wordt verwezen naar Advies 5/2009 van de Groep Gegevensbescherming artikel 29 van 12 juni 2009 (WP 163).

verwerking verantwoordelijke altijd uiteindelijk verantwoordelijk voor de nakoming van zijn verplichtingen en aansprakelijk wanneer de nakoming van deze verplichtingen eventueel uitblijft.

Volgens een vorige tekst die door de Commissie werd gepresenteerd gedurende het goedkeuringsproces van de richtlijn zou het feit dat men toegang heeft tot bepaalde persoonsgegevens betekenen dat men (gezamenlijk) voor de verwerking van deze gegevens verantwoordelijk is. Deze formulering is in de uiteindelijke tekst echter komen te vervallen, en de ervaring leert dat enerzijds het hebben van toegang tot gegevens op zichzelf niet wil zeggen dat men voor de verwerking verantwoordelijk is, terwijl anderzijds het feit dat men toegang tot gegevens heeft geen harde voorwaarde is voor de hoedanigheid van voor de verwerking verantwoordelijke. In complexe constructies met meerdere partijen kunnen de toegang tot persoonsgegevens en andere rechten van betrokkenen op verschillende niveaus door verschillende partijen worden gewaarborgd.

Onderdeel van de juridische gevolgen is ook de aansprakelijkheid van voor de verwerking verantwoordelijken, waarbij met name de vraag rijst of “gezamenlijke verantwoordelijkheid” in de zin van de richtlijn ook altijd betekent dat sprake is van gezamenlijke en hoofdelijke aansprakelijkheid. Artikel 26 over aansprakelijkheid gebruikt het enkelvoud “voor de verwerking verantwoordelijke”, wat zou betekenen dat het antwoord bevestigend luidt. Zoals echter reeds aangegeven kan “tezamen met” diverse vormen van gezamenlijk handelen inhouden, dus “samen met”. Onder bepaalde omstandigheden kan dit leiden tot een gezamenlijke en hoofdelijke aansprakelijkheid, maar dit is geen ijzeren regel: in veel gevallen kunnen de diverse voor de verwerking verantwoordelijken verantwoordelijk – en dus aansprakelijk – zijn voor de verwerking van persoonsgegevens in diverse fasen en in verschillende mate.

Ook wanneer gegevens worden verwerkt in complexe omgevingen, waarin verschillende voor de verwerking verantwoordelijken betrokken zijn bij de verwerking van persoonsgegevens, moet uiteindelijk worden gewaarborgd dat de naleving van de regelgeving voor gegevensbescherming en de verantwoordelijkheden voor mogelijke overtredingen van deze regels duidelijk zijn geregeld, om te voorkomen dat persoonsgegevens minder goed worden beschermd of dat een “negatief bevoegdheidsconflict” en mazen in de wet ontstaan, waardoor sommige verplichtingen of rechten uit de richtlijn door een partij niet worden nageleefd.

In deze gevallen is het meer dan ooit van belang dat aan betrokkenen duidelijke informatie wordt verstrekt, met een toelichting op de diverse fasen van de verwerking en de verschillende partijen die daarbij zijn betrokken. Bovendien moet duidelijk worden gemaakt of elke voor de verwerking verantwoordelijke bevoegd is om alle rechten van betrokkenen te waarborgen of welke verantwoordelijke voor welk recht bevoegd is.

Voorbeeld 13: Banken en informatiecentra voor klanten met betalingsachterstanden

Een aantal banken kan gezamenlijk een “informatiecentrum” oprichten – voor zover dit op grond van nationale wetgeving is toegestaan – waaraan elk van hen informatie (gegevens) aanlevert over klanten met betalingsachterstanden, waarna zij alle toegang hebben tot de volledige informatie. Soms wordt in wetgeving bepaald dat verzoeken van betrokkenen, bijvoorbeeld om toegang tot gegevens of uitwissing daarvan, altijd maar aan één “loket” behoeven te worden gericht, te weten de aanbieder. De aanbieder is verantwoordelijk voor het vinden van de desbetreffende voor de verwerking verantwoordelijke en moet waarborgen dat de betrokkene naar behoren wordt geantwoord.

De identiteit van de aanbieder wordt openbaar gemaakt in het gegevensverwerkingsregister. In andere rechtsstelsels kunnen dergelijke informatiecentra worden geëxploiteerd door aparte rechtspersonen die als voor de verwerking verantwoordelijke fungeren, terwijl verzoeken om toegang van betrokkenen worden behandeld door de deelnemende banken, die dan als tussenpersoon optreden.

Voorbeeld 14: Reclame op basis van surfgedrag

Bij deze vorm van reclame wordt gebruikgemaakt van informatie die is verzameld over het surfgedrag van een internetgebruiker, bijvoorbeeld over de pagina's die hij heeft bezocht of de zoekwoorden die hij heeft opgegeven. Op basis van deze informatie worden de advertenties geselecteerd die aan die persoon worden getoond. Zowel uitgevers, die vaak advertentieruimte op hun websites verhuren, als aanbieders van advertentienetwerken, die deze ruimte met gerichte reclame vullen, kunnen – afhankelijk van specifieke contractuele regelingen – informatie over gebruikers verzamelen en uitwisselen.

Vanuit een oogpunt van gegevensbescherming moet de uitgever worden beschouwd als een autonome voor de verwerking verantwoordelijke wanneer hij persoonsgegevens van de gebruiker (gebruikersprofiel, IP-adres, plaats, taal of besturingssysteem enz.) voor eigen doeleinden verzamelt. De aanbieder van het advertentienetwerk is ook voor de verwerking verantwoordelijk voor zover hij de doelen van (het volgen van gebruikers op verschillende websites), of de belangrijkste middelen voor de verwerking van gegevens vaststelt. Afhankelijk van de voorwaarden voor de samenwerking tussen de uitgever en de aanbieder van het advertentienetwerk, bijvoorbeeld wanneer de uitgever de doorgifte van persoonsgegevens aan de aanbieder van het advertentienetwerk mogelijk maakt, ook bijvoorbeeld door het doorsturen van de gebruiker naar de webpagina van de aanbieder van het advertentienetwerk, kunnen zij gezamenlijk voor de verwerking verantwoordelijk zijn voor het geheel van verwerkingen dat ten grondslag ligt aan op surfgedrag gebaseerde reclame.

In alle gevallen dienen de (gezamenlijk) voor de verwerking verantwoordelijken te waarborgen dat de gecompliceerde aard en de technische eigenschappen van op surfgedrag gebaseerde reclame geen beletsel vormen voor passende oplossingen om te voldoen aan de verplichtingen van de voor de verwerking verantwoordelijken en voor het waarborgen van de rechten van betrokkenen. Dit betekent met name:

- *informatieverstrekking* aan de gebruiker over het feit dat een derde toegang heeft tot zijn/haar gegevens: het is doelmatiger om dit via de uitgever te laten verlopen, die het eerste aanspreekpunt voor de gebruiker is,
- en voorwaarden voor de *toegang* tot persoonsgegevens: het advertentiebedrijf zou moeten antwoorden op verzoeken van gebruikers over de wijze waarop het op basis van gebruikersgegevens gericht adverteert, en moeten ingaan op verzoeken om rectificatie en uitwissing.

Bovendien kunnen voor uitgevers en advertentiebedrijven andere verplichtingen uit het burgerlijk en consumentenrecht gelden, onder meer met betrekking tot onrechtmatige daden en oneerlijke handelspraktijken.

Voorlopige conclusie

Gezamenlijk handelende partijen hebben een zekere speelruimte bij het verdelen en beleggen van verplichtingen en verantwoordelijkheden, zolang zij maar een volledige naleving waarborgen. Voorschriften over de wijze waarop gezamenlijke verantwoordelijkheden moeten worden uitgeoefend, dienen in beginsel door voor de verwerking verantwoordelijken te worden vastgesteld. In dit geval moet echter ook naar de feitelijke omstandigheden worden gekeken, om te beoordelen of de regelingen de werkelijkheid van de onderliggende gegevensverwerking weerspiegelen.

Zo bezien moet bij de beoordeling van gezamenlijke verantwoordelijkheid enerzijds rekening worden gehouden met de noodzaak om volledige naleving van de regelgeving voor gegevensbescherming te waarborgen en anderzijds met het feit dat de aanwezigheid van meerdere voor de verwerking verantwoordelijken zaken ook ongewenst kan compliceren en mogelijk minder duidelijk maakt waar verantwoordelijkheden liggen. Hierdoor zou de volledige verwerking mogelijk onrechtmatig worden vanwege een gebrek aan transparantie en zou inbreuk worden gemaakt op het beginsel van eerlijke verwerking.

Voorbeeld 15: Platforms voor het beheren van gezondheidsgegevens

In een lidstaat stelt een overheidsinstantie een nationaal informatiecentrum in voor de uitwisseling van patiëntengegevens tussen zorgaanbieders. Door het grote aantal voor de verwerking verantwoordelijken – tienduizenden – ontstaat voor de betrokkenen (patiënten) een dermate onduidelijke situatie dat de bescherming van hun rechten in het geding komt. Voor betrokkenen is het namelijk onduidelijk tot wie zij zich kunnen richten met klachten, vragen en verzoeken om informatie, rectificatie en toegang tot persoonsgegevens. Bovendien is de overheidsinstantie verantwoordelijk voor de feitelijke opzet van de verwerking en de wijze waarop deze wordt gebruikt. Daarom moet worden geconcludeerd dat de overheidsinstantie die het datacentrum instelt als gezamenlijk voor de verwerking verantwoordelijk moet worden beschouwd, en tevens als aanspreekpunt voor verzoeken van betrokkenen.

Tegen deze achtergrond kan worden aangevoerd dat gezamenlijke en hoofdelijke aansprakelijkheid voor alle betrokken partijen zou moeten worden beschouwd als een manier om onduidelijkheid weg te nemen, en dat daar derhalve alleen vanuit kan worden gegaan wanneer de betrokken partijen verplichtingen en verantwoordelijkheden niet duidelijk en even effectief hebben belegd of dit niet duidelijk uit de feitelijke omstandigheden blijkt.

III.2. Definitie van verwerker

Het begrip “verwerker” kwam niet voor in Verdrag 108. De rol van de verwerker wordt voor het eerst erkend in het eerste voorstel van de Commissie, maar het begrip wordt dan niet ingevoerd, om “*situaties te voorkomen waarin verwerking door een derde namens de voor het gegevensbestand verantwoordelijke tot gevolg heeft dat de door de betrokkene genoten bescherming afneemt*”. Pas in het gewijzigde voorstel van de Commissie en naar aanleiding van een voorstel van het Europees Parlement werd het begrip “verwerker” uitdrukkelijk en zelfstandig uitgewerkt, als voorloper van de huidige formulering in het gemeenschappelijke standpunt van de Raad.

Net als in de definitie van de voor de verwerking verantwoordelijke kan volgens de definitie van verwerker een breed scala van partijen de rol van verwerker vervullen (“...een natuurlijke of rechtspersoon, overheidsinstantie, dienst of enig ander lichaam...”).

Het bestaan van een verwerker is afhankelijk van een besluit van de voor de verwerking verantwoordelijke, die kan besluiten gegevens binnen zijn eigen organisatie te verwerken, bijvoorbeeld door personeel dat wordt gemachtigd om gegevens onder zijn rechtstreekse gezag te verwerken (zie *a contrario* artikel 2, onder f)), of om de verwerkingen geheel of gedeeltelijk te delegeren aan een externe organisatie, dus – zoals aangegeven in de toelichting op het gewijzigde voorstel van de Commissie – door een “juridisch afzonderlijke persoon die namens hem handelt”.

De twee centrale voorwaarden om een partij als verwerker te kunnen aanmerken zijn dus enerzijds dat het een aparte rechtspersoon is, die los van de voor de verwerking verantwoordelijke staat, en anderzijds dat deze partij persoonsgegevens ten behoeve van die voor de verwerking verantwoordelijke verwerkt. Deze verwerking kan zich beperken tot een zeer specifieke taak of een zeer specifiek kader, of meer algemeen en uitgebreid zijn.

Bovendien is de rol van verwerker niet gekoppeld aan de aard van een entiteit die gegevens verwerkt maar vloeit hij voort uit haar concrete activiteiten in een specifiek kader. Met andere woorden: een en dezelfde entiteit kan tegelijkertijd voor sommige verwerkingen als voor de verwerking verantwoordelijke optreden en voor andere als verwerker, en bij de vraag of hij als verwerker of als voor de verwerking verantwoordelijke moet worden aangemerkt, moet worden gekeken naar specifieke gehelen van gegevens of verwerkingen.

Voorbeeld 16: Aanbieders van hostingdiensten op internet (Internet Service Providers – ISP)

Een ISP die hostingdiensten aanbiedt is in beginsel een verwerker van de persoonsgegevens die online worden gepubliceerd door zijn klanten, die deze ISP gebruiken voor hosting en onderhoud van hun website. Wanneer de ISP de gegevens van de websites echter verder verwerkt voor eigen doeleinden, is hij voor die specifieke verwerking de voor de verwerking verantwoordelijke. Anders ligt het bij een ISP die e-maildiensten of toegang tot internet aanbiedt (zie ook voorbeeld 1 over telecombedrijven).

Het belangrijkste is de eis dat de verwerker “...ten behoeve van de voor de verwerking verantwoordelijke...” handelt. “Handelen ten behoeve van” betekent dat in het belang van iemand anders wordt gehandeld, en verwijst naar het juridische begrip “delegatie”. In het kader van de wetgeving inzake gegevensbescherming dient een verwerker de aanwijzingen van de voor de verwerking verantwoordelijke op te volgen, in ieder geval waar het gaat om het doel van de verwerking en de wezenlijke aspecten van de middelen.

Vanuit dit oogpunt wordt de rechtmatigheid van de door de verwerker verrichte gegevensverwerking bepaald door de opdracht die hem daartoe door de voor de verwerking verantwoordelijk is verstrekt. Een verwerker die verder gaat dan zijn opdracht en een relevante rol krijgt bij het vaststellen van de doelen van, of de wezenlijke middelen voor de verwerking is eerder een (gezamenlijk) voor de verwerking

verantwoordelijke dan een verwerker. De rechtmatigheid van deze verwerking wordt altijd nog getoetst aan andere artikelen (6-8). Bij delegatie kan echter nog steeds sprake zijn van een bepaalde handelingsvrijheid voor wat betreft de wijze waarop de belangen van de voor de verwerking verantwoordelijke het best kunnen worden gediend, zodat de verwerker de meest geschikte technische en organisatorische middelen kan kiezen.

Voorbeeld 17: Uitbesteden van postdiensten

Particuliere dienstverleners verrichten postdiensten namens (overheids)instanties, bijvoorbeeld de verzending van kinderbijslag en moederschapstoelage namens de nationale instantie voor sociale zekerheid. In dit geval gaf een gegevensbeschermingsautoriteit aan dat de desbetreffende dienstverleners als verwerkers dienden te worden aangesteld omdat hun taak, die zij weliswaar met een zekere autonomie uitvoerden, zich beperkte tot slechts een deel van de verwerkingen die noodzakelijk zijn voor de doelen die waren vastgesteld door de voor de verwerking van de gegevens verantwoordelijke.

Om ook hier te waarborgen dat bij uitbesteden en delegeren de normen voor gegevensbescherming niet worden versoepeld, bevat de richtlijn twee bepalingen die specifiek op de verwerker betrekking hebben en waarin zijn verplichtingen met betrekking tot vertrouwelijkheid en beveiliging zeer nauwkeurig worden omschreven.

– In artikel 16 wordt bepaald dat zowel de verwerker zelf als eenieder die onder zijn gezag handelt en toegang tot persoonsgegevens heeft deze alleen in opdracht van de voor de verwerking verantwoordelijke mag verwerken.

– In artikel 17 over de beveiliging van de verwerking wordt bepaald dat de verhoudingen tussen de voor de verwerking van gegevens verantwoordelijke en de verwerker worden geregeld in een contract of een bindende rechtsakte. Met het oog op de bewaring van de bewijzen dient dit een schriftelijke overeenkomst te zijn, waarin in ieder geval een aantal zaken wordt geregeld, waaronder met name dat de gegevensverwerker uitsluitend in opdracht van de voor de verwerking verantwoordelijke handelt en technische en organisatorische maatregelen treft om persoonsgegevens adequaat te beveiligen. In het contract dient een voldoende uitgewerkte beschrijving van de opdracht aan de verwerker te worden opgenomen.

In dit verband moet worden opgemerkt dat in veel gevallen dienstverleners die zijn gespecialiseerd in bepaalde vormen van gegevensverwerking (bijvoorbeeld de uitbetaling van salarissen) standaarddiensten en -contracten zullen opstellen die door de voor de verwerking verantwoordelijke moeten worden ondertekend, waardoor in feite een bepaalde standaardwijze ontstaat voor de verwerking van persoonsgegevens¹⁸. Het feit echter dat het contract met zijn nauwkeurig omschreven bepalingen door de dienstverlener wordt opgesteld, en niet door de voor de verwerking verantwoordelijke, is *op zichzelf* nog onvoldoende reden om te concluderen dat de dienstverlener als een voor de verwerking verantwoordelijke moet worden beschouwd, omdat de voor de verwerking verantwoordelijke uit vrije wil heeft ingestemd met de contractbepalingen en er daarmee de volledige verantwoordelijkheid voor aanvaardt.

¹⁸ De formulering van de contractbepalingen door de dienstverlener laat onverlet dat wezenlijke aspecten van de verwerking, zoals omschreven in punt III.1.b, door de voor de verwerking verantwoordelijke worden vastgesteld.

Zo behoort ook de onevenwichtigheid in de contractuele macht van een kleine voor de verwerking verantwoordelijke ten opzichten van grote dienstverleners niet te worden beschouwd als een rechtvaardiging voor de voor de verwerking verantwoordelijke om contractbepalingen te accepteren die niet in overeenstemming met de wetgeving voor gegevensbescherming zijn.

Voorbeeld 18: E-mail platforms

De heer van Dalen zoekt een e-mail platform voor zichzelf en de vijf werknemers van zijn onderneming. Hij ontdekt dat een geschikt gebruikersvriendelijk platform – en ook het enige dat gratis is – persoonsgegevens buitensporig lang bewaart en zonder duidelijke waarborgen naar derde landen overbrengt. Bovendien komen de contractbepalingen neer op “*take it or leave it*”.

In dit geval moet de heer van Dalen uitzien naar een andere aanbieder of – wanneer sprake zou zijn van overtreding van de regelgeving voor gegevensbescherming of op de markt niet voldoende geschikte andere aanbieders beschikbaar zijn – de zaak aanhangig maken bij de bevoegde instanties, zoals gegevensbeschermingsautoriteiten, organisaties voor consumentenbescherming, mededingingsautoriteiten enz..

Het feit dat de richtlijn voor de beveiliging van de verwerking eist dat een schriftelijk contract wordt opgesteld, betekent niet dat er geen verhoudingen van het type verwerker-verantwoordelijke kunnen bestaan zonder voorafgaande contracten. Vanuit dit oogpunt is het contract wezenlijk noch doorslaggevend, hoewel het nuttig kan zijn voor een beter inzicht in de verhoudingen tussen de partijen¹⁹. Daarom moet ook in dit geval een functionele benadering worden gevolgd, waarbij wordt gekeken naar de feitelijke aspecten van de verhoudingen tussen de verschillende betrokkenen en de wijze waarop doelen van, en middelen voor de verwerking worden vastgesteld. Wanneer een verhouding tussen verantwoordelijke en verwerker blijkt te bestaan, zijn deze partijen wettelijk verplicht een contract te sluiten (zie artikel 17 van de richtlijn).

Meerdere verwerkers

Steeds vaker wordt de verwerking van persoonsgegevens door een voor de verwerking verantwoordelijke uitbesteed aan een aantal gegevensverwerkers. Deze verwerkers kunnen een rechtstreekse verhouding met de voor de verwerking verantwoordelijke hebben, of onderaannemers zijn, waaraan de verwerkers een deel van de hun opgedragen verwerkingen hebben uitbesteed.

Deze gecompliceerde (gelaagde of gespreide) constructies voor de verwerking van persoonsgegevens komen met de nieuwe technologieën vaker voor en worden in sommige nationale wetgevingen uitdrukkelijk genoemd. De richtlijn belet geenszins dat om organisatorische redenen meerdere entiteiten als gegevensverwerker of (sub-)verwerker worden aangewezen of dat de desbetreffende taken worden

¹⁹ In sommige gevallen kan het bestaan van een schriftelijk contract echter een noodzakelijke voorwaarde zijn om in bepaalde situaties automatisch als verwerker te worden aangemerkt. Zo worden in Spanje in het rapport over callcenters alle callcenters in derde landen als verwerkers aangemerkt zolang zij zich aan het contract houden. Dat is ook het geval wanneer het contract is opgesteld door de verwerker en de voor de verwerking verantwoordelijke het alleen maar “onderschrijft”.

onderverdeeld. Zij moeten zich echter allen bij de verwerking houden aan de opdrachten van de voor de verwerking verantwoordelijke.

Voorbeeld 19: Computergrids

Grootschalige researchinfrastructuur maakt steeds meer gebruik van decentrale computerfaciliteiten, waaronder met name de zogenoemde ‘grids’, om meer reken- en opslagcapaciteit te krijgen. *Grids* zijn geïnstalleerd in verschillende researchinfrastructuren die zijn gevestigd in verschillende landen. Zo kan een Europese *grid* bijvoorbeeld bestaan uit nationale *grids*, die op hun beurt onder de verantwoordelijkheid van een nationale instantie vallen. Mogelijk kent deze Europese *grid* echter geen centraal orgaan dat verantwoordelijk is voor zijn functioneren. Onderzoekers die een dergelijke *grid* gebruiken, kunnen doorgaans niet achterhalen waar hun gegevens precies worden verwerkt en dus ook niet wie de verantwoordelijke gegevensverwerker is (nog ingewikkelder wordt het wanneer *grid*-infrastructuur zich in derde landen bevindt). Wanneer *grid*-infrastructuur gegevens op een ongeoorloofde manier gebruikt, kan deze partij als voor de verwerking verantwoordelijke worden beschouwd indien hij niet ten behoeve van de onderzoekers handelt.

Het strategische punt is hier dat – wanneer meerdere partijen bij het proces betrokken zijn – de verplichtingen en verantwoordelijkheden uit de wetgeving voor gegevensbescherming duidelijk behoren te worden belegd en niet versnipperd mogen raken over de keten van uitbesteding/onderaanneming. Met andere woorden: voorkomen moet worden dat er ketens van (sub-)verwerkers ontstaan, waarbij een effectief toezicht en duidelijke verantwoordelijkheden voor verwerkingsactiviteiten versnipperd zouden raken of zelfs onmogelijk zouden worden, tenzij de verantwoordelijkheden van de verschillende partijen in de keten duidelijk worden vastgesteld.

Hoewel het niet noodzakelijk is dat de voor de verwerking verantwoordelijke alle details omschrijft en goedkeurt van de middelen die worden ingezet om het beoogde doel te bereiken, zou hij daarom, zoals reeds aangegeven in paragraaf III.1.b, in ieder geval nog wel moeten worden geïnformeerd over de belangrijkste onderdelen van de verwerkingsorganisatie (bijvoorbeeld: betrokkenen, beveiligingsmaatregelen, waarborgen voor verwerking in derde landen enz.), zodat hij nog steeds de regie kan voeren over de namens hem verwerkte gegevens.

Ook moet in aanmerking worden genomen dat de richtlijn weliswaar de aansprakelijkheid bij de voor de verwerking verantwoordelijke legt, maar dat in nationale wetgeving voor gegevensbescherming kan worden bepaald dat ook de verwerker in bepaalde gevallen aansprakelijk wordt geacht.

Onderstaande criteria kunnen een nuttige rol vervullen bij het vaststellen van de hoedanigheid van de diverse betrokkenen:

- De uitvoerigheid van de opdracht die de voor de verwerking verantwoordelijke verstrekt. Hieruit blijkt in hoeverre de gegevensverwerker nog vrijheid van handelen heeft.
- Het toezicht dat de voor de verwerking verantwoordelijke uitoefent op de uitvoering van de dienst. Permanent en zorgvuldig toezicht door de voor de verwerking verantwoordelijke om een volledige naleving van de opdrachten en de

contractbepalingen te waarborgen is een aanwijzing dat de voor de verwerking verantwoordelijke nog steeds en als enige verantwoordelijk is voor de verwerkingen.

- Zichtbaarheid/het beeld dat de voor de verwerking verantwoordelijke bij de betrokkene doet ontstaan, en verwachtingen van de betrokkenen op grond van deze zichtbaarheid.

Voorbeeld 20: Callcenters

Een voor de verwerking verantwoordelijke besteedt werkzaamheden uit aan een callcenter, met de opdracht dat het callcenter zich als de voor de verwerking verantwoordelijke moet presenteren wanneer de klanten van die verantwoordelijke worden gebeld. In dit geval leiden de verwachtingen van de klanten en de manier waarop de voor de verwerking verantwoordelijke zichzelf via de dienstverlener aan hen presenteert tot de conclusie dat de dienstverlener optreedt als gegevensverwerker voor (ten behoeve van) de voor de verwerking verantwoordelijke.

- Deskundigheid van de partijen: in bepaalde gevallen spelen de traditionele rol en de professionele deskundigheid van de dienstverlener een overheersende rol, waardoor hij als voor de verwerking verantwoordelijke kan worden aangemerkt.

Voorbeeld 21: Advocaten

Een advocaat vertegenwoordigt zijn/haar cliënt voor de rechter en verwerkt daarvoor persoonsgegevens die verband houden met de zaak van de cliënt. De rechtsgrond voor het gebruiken van de noodzakelijke informatie is de opdracht van de cliënt. Deze opdracht richt zich echter niet op het verwerken van gegevens maar op de vertegenwoordiging voor de rechter, waarvoor dergelijke beroepen traditioneel hun eigen rechtsgrond hebben. Deze beroepen moeten daarom worden beschouwd als onafhankelijke “voor de verwerking verantwoordelijken” wanneer zij in het kader van de juridische vertegenwoordiging van hun cliënt gegevens verwerken.

In een ander verband kan een nadere beoordeling van de middelen die worden ingezet om de doelen te bereiken ook bepalend zijn.

Voorbeeld 22: Website met gevonden en verloren voorwerpen

Van een website met gevonden en verloren voorwerpen werd gezegd dat deze site slechts een verwerker was, omdat degenen die gevonden en verloren voorwerpen op de site publiceren de inhoud vaststellen en dus – op microniveau – het doel (bijvoorbeeld het terugvinden van een verloren broche, papegaai enz.). Dit argument werd door een gegevensbeschermingsautoriteit verworpen. De website was opgezet met het zakelijke doel om geld te verdienen met het aanbieden van de mogelijkheid om verloren voorwerpen op de site te zetten en het feit dat de site niet vaststelde welke specifieke voorwerpen daarop zouden worden gepubliceerd (en dus niet de categorieën voorwerpen vaststelde) was niet van wezenlijk belang omdat in de definitie van “voor de verwerking van gegevens verantwoordelijke” niet uitdrukkelijk sprake is van het vaststellen van inhoud. De website stelt vast onder welke voorwaarden gevonden of verloren voorwerpen op de site kunnen worden gepubliceerd enz. en is verantwoordelijk voor de juistheid van de inhoud.

Hoewel er sprake zou kunnen zijn van een tendens om in algemene zin uitbesteding aan te merken als de taak van een verwerker, zijn de situaties en beoordelingen tegenwoordig vaak veel gecompliceerder.

Voorbeeld 23: Accountants

De hoedanigheid van accountants kan per situatie verschillen. Wanneer een accountant voor consumenten en het midden- en kleinbedrijf diensten verricht op basis van heel algemene opdrachten (“vul mijn belastingaangifte in”), dan is hij – net als een advocaat, die onder vergelijkbare omstandigheden en om vergelijkbare redenen handelt – voor de verwerking van gegevens verantwoordelijk. Wanneer een accountant echter bij een bedrijf in dienst is en zich moet houden aan nauwkeurig omschreven opdrachten van de bedrijfsaccountant, bijvoorbeeld om een specifiek onderzoek in te stellen, dan is hij in het algemeen gewoon een werknemer, en daarnaast een verwerker, vanwege de duidelijkheid van de opdrachten en de daaruit voortvloeiende beperkte handelingsvrijheid. Hierbij geldt echter wel een belangrijk voorbehoud, namelijk dat de accountant, indien hij meent onregelmatigheden te hebben aangetroffen die hij moet rapporteren, op grond van de voor hem geldende beroepsverplichtingen onafhankelijk als een voor de verwerking verantwoordelijke handelt.

Soms kan de gecompliceerde aard van verwerkingen leiden tot meer nadruk op de handelingsvrijheid van degenen die belast zijn met de verwerking van persoonsgegevens, bijvoorbeeld wanneer bij de verwerking sprake is van een specifiek privacyrisico. Wanneer voor de verwerking nieuwe middelen worden ingevoerd, kan er de voorkeur aan worden gegeven om de betrokkene aan te merken als voor de verwerking van gegevens verantwoordelijk, en niet als gegevensverwerker. Het resultaat kan zijn dat meer duidelijkheid ontstaat – en kan worden vastgesteld wie voor de verwerking verantwoordelijk is – zoals uitdrukkelijk in de wet wordt vereist.

Voorbeeld 24: Verwerking voor historische, wetenschappelijke en statistische doeleinden

Voor de verwerking van persoonsgegevens voor historische, wetenschappelijke en statistische doeleinden kan in de nationale wetgeving het begrip “intermediaire organisatie” worden ingevoerd voor het orgaan dat belast is met het omzetten van niet-gecodeerde gegevens in gecodeerde gegevens, waarbij betrokkenen worden geanonimiseerd voor degene die verantwoordelijk is voor de verwerking van de gegevens voor historische, wetenschappelijke en statistische doeleinden.

Wanneer meerdere voor de aanvankelijke verwerkingen verantwoordelijken gegevens aan een of meer derden doorgeven voor nadere verwerking voor historische, wetenschappelijke en statistische doeleinden, worden de gegevens eerst gecodeerd door een intermediaire organisatie. In dit geval kan de intermediaire organisatie volgens specifieke nationale regelgeving als voor de verwerking verantwoordelijk worden beschouwd en gelden voor deze organisatie alle hieruit voortvloeiende verplichtingen (relevantie van de gegevens, informatieverstrekking aan de betrokkene, aanmelding enz.). Dit is nodig omdat er een bijzonder risico voor de gegevensbescherming ontstaat wanneer gegevens uit verschillende bronnen bijeen worden gebracht. De intermediaire organisatie heeft daarom zijn eigen verantwoordelijkheid. Daarom wordt deze organisatie niet eenvoudigweg aangemerkt als een verwerker, maar als een voor de verwerking verantwoordelijke volgens het nationale recht.

Zo is ook de autonome beslissingsbevoegdheid van de diverse bij de verwerking betrokken partijen relevant. Uit het voorbeeld van klinisch geneesmiddelenonderzoek blijkt dat de verhouding tussen sponsors en externe entiteiten waaraan het onderzoek wordt opgedragen afhankelijk is van de handelingsvrijheid waarover de externe entiteiten voor de verwerking van gegevens beschikken. Dit betekent dat er meer dan een partij voor de verwerking verantwoordelijk kan zijn, maar ook dat er meer dan een verwerker of met de verwerking belaste persoon kan zijn.

Voorbeeld 25: Klinisch geneesmiddelenonderzoek

Farmaceutisch bedrijf XYZ sponsort geneesmiddelenonderzoek en selecteert de gegadigde onderzoekscentra door middel van een beoordeling van hun respectieve geschiktheid en belangen. Het stelt het onderzoeksprotocol op, verstrekt de centra de nodige richtsnoeren voor de verwerking van gegevens en controleert de naleving door de centra van zowel het protocol als de respectieve interne procedures.

Hoewel de sponsor niet rechtstreeks gegevens verzamelt, verkrijgt hij wel de patiëntengegevens die door de onderzoekscentra zijn verzameld en verwerkt hij deze op verschillende manieren (hij beoordeelt de informatie uit de medische documenten, ontvangt gegevens over bijwerkingen, voert deze gegevens in de relevante database in en verricht statistische analyses om tot onderzoeksresultaten te komen). Het onderzoekscentrum verricht het onderzoek zelfstandig, maar wel volgens de richtsnoeren van de sponsor. Het verstrekt bijsluiters aan de patiënten en verkrijgt hun toestemming, ook voor de verwerking van hun persoonsgegevens. Het geeft medewerkers van de sponsor toegang tot de originele medische documenten van de patiënten om het onderzoek te kunnen bewaken en beheert en beveiligt deze documenten. Daarom blijken individuele partijen verantwoordelijkheden te dragen.

Hierbij stellen zowel onderzoekscentra als sponsors belangrijke aspecten vast van de wijze waarop persoonsgegevens met betrekking tot klinisch onderzoek worden verwerkt. Daarom kunnen zij als gezamenlijk voor de verwerking verantwoordelijk worden beschouwd. De relatie tussen de sponsor en de onderzoekscentra kan anders worden geïnterpreteerd wanneer de sponsor de doelen en de wezenlijke aspecten van de middelen vaststelt en de onderzoeker en zeer beperkte vrijheid van handelen rest.

III.3. Definitie van derde

Het begrip “derde” kwam niet voor in Verdrag 108 maar werd in het gewijzigde voorstel van de Commissie ingevoerd naar aanleiding van een amendement van het Europees Parlement. Volgens de toelichting werd het amendement opnieuw geformuleerd om duidelijk te maken dat onder derden niet de betrokkene, noch de voor de verwerking verantwoordelijke, noch de personen vallen die onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of namens hem gegevens mogen verwerken, zoals het geval is met de verwerker. Dit betekent dat “*personen die werkzaam zijn voor een andere organisatie, ook wanneer deze deel uitmaakt van hetzelfde concern of dezelfde houdstermaatschappij, in algemene zin derden zijn*”, terwijl anderzijds “*kantoren van een bank die klantgegevens verwerken onder rechtstreeks gezag van hun hoofdkantoor geen derden zijn*”.

De richtlijn gebruikte “derde” op een wijze die niet afwijkt van de wijze waarop dit begrip doorgaans wordt gebruikt in het burgerlijk recht, waar een derde doorgaans een betrokkene is die geen deel van een entiteit of een overeenkomst uitmaakt. In het kader van de gegevensbescherming moet dit begrip worden geïnterpreteerd als elke betrokkene die geen specifieke legitimiteit of bevoegdheid heeft – bijvoorbeeld voortvloeiend uit zijn rol als voor de verwerking verantwoordelijke, verwerker, of een van hun werknemers – bij de verwerking van persoonsgegevens.

De richtlijn gebruikt dit begrip in een groot aantal bepalingen, meestal om verboden, beperkingen en verplichtingen vast te stellen voor de gevallen waarin persoonsgegevens kunnen worden verwerkt door andere partijen die oorspronkelijk niet geacht werden bepaalde persoonsgegevens te verwerken.

Hieruit kan worden geconcludeerd dat een derde die persoonsgegevens – al dan niet rechtmatig – ontvangt in beginsel een nieuwe voor de verwerking verantwoordelijke is, mits wordt voldaan aan de andere voorwaarden om deze partij als voor de verwerking verantwoordelijke te kunnen aanmerken en de wetgeving inzake gegevensbescherming wordt nageleefd.

Voorbeeld 26: Onbevoegde toegang door een werknemer

Bij de uitvoering van zijn werkzaamheden neemt een werknemer van een onderneming kennis van persoonsgegevens waartoe hij geen toegang heeft. In dit geval moet de werknemer ten opzichte van zijn werkgever als “derde” worden beschouwd, met alle daaruit voortvloeiende gevolgen en aansprakelijkheden met betrekking tot de rechtmatigheid van de verstrekking en de verwerking van gegevens.

IV. Conclusies

Het begrip “voor de verwerking verantwoordelijke” en zijn raakvlakken met het begrip “verwerker” spelen een cruciale rol in de tenuitvoerlegging van Richtlijn 95/46/EG, omdat aan de hand van deze begrippen wordt uitgemaakt wie verantwoordelijk is voor de naleving van de regelgeving met betrekking tot gegevensbescherming, op welke wijze betrokkenen hun rechten kunnen uitoefenen, welk nationaal recht van toepassing is en hoe effectief gegevensbeschermingsautoriteiten hun werk kunnen doen.

Organisatiedifferentiatie in zowel de publieke als de private sector, de ontwikkeling van ICT en de mondialisering van de gegevensverwerking maken de wijze waarop de persoonsgegevens worden verwerkt steeds gecompliceerder en vragen om verduidelijking van deze begrippen, zodat een effectieve toepassing en de praktische naleving kunnen worden gewaarborgd.

Het begrip “voor de verwerking verantwoordelijke” is autonoom, in die zin dat het met name dient te worden geïnterpreteerd volgens de communautaire wetgeving voor gegevensbescherming. Daarnaast is het functioneel, in die zin dat het bedoeld is om de verantwoordelijkheden te leggen op de plaats waar ook de feitelijke invloed ligt, en dus eerder op een feitelijke dan op een formele analyse gebaseerd.

De definitie in de richtlijn is opgebouwd uit drie hoofdonderdelen: het personele aspect (“*de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam*”), de mogelijkheid van gezamenlijke verantwoordelijkheid (“*die, respectievelijk dat, alleen of tezamen met anderen*”), en de wezenlijke aspecten waarmee de voor de verwerking verantwoordelijke van andere partijen kan worden onderscheiden (“*het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*”).

Een onderzoek van deze onderdelen leidt tot de volgende hoofduitkomsten:

- De bevoegdheid om “de doelen en de middelen *vast te stellen...*” kan voortvloeien uit verschillende juridische en/of feitelijke omstandigheden: een expliciete wettelijke bevoegdheid, wanneer de voor de verwerking verantwoordelijke bij wet wordt aangesteld of de opdracht of plicht tot het verzamelen en verwerken van bepaalde gegevens bij wet is geregeld, gemeenrechtelijke bepalingen of bestaande traditionele rollen waarbij normaliter sprake is van een bepaalde verantwoordelijkheid binnen bepaalde organisaties (bijvoorbeeld de werkgever met betrekking tot gegevens van zijn werknemer), feitelijke omstandigheden en andere feiten (waaronder contractuele betrekkingen, daadwerkelijke zeggenschap van een partij, zichtbaarheid jegens betrokkenen enz.).

Wanneer geen van deze bovengenoemde categorieën van toepassing is, moet de aanstelling van een voor de verwerking verantwoordelijke als nietig worden beschouwd. Een partij die geen juridische of feitelijke invloed heeft op de vaststelling van de wijze waarop persoonsgegevens worden verwerkt, kan namelijk niet als voor de verwerking verantwoordelijk worden beschouwd.

Wie het “doel” van de verwerking vaststelt, wordt (de facto) aangemerkt als voor de verwerking verantwoordelijk. Het vaststellen van de “middelen” voor de verwerking kan echter door de voor de verwerking verantwoordelijke worden gedelegeerd voor wat betreft technische of organisatorische aspecten. Punten van wezenlijk belang, die een centrale rol vervullen voor de rechtmatigheid van de verwerking – zoals de vraag welke gegevens moeten worden verwerkt, hoe lang zij moeten worden bewaard, wie toegang tot die gegevens heeft enz. – dienen echter door de voor de verwerking verantwoordelijke te worden vastgesteld.

- Het *personele* aspect van de definitie heeft betrekking op het brede scala van betrokkenen die de rol van voor de verwerking verantwoordelijke kunnen vervullen. Vanuit het strategische oogpunt van het beleggen van verantwoordelijkheden dient er echter de voorkeur aan gegeven te worden de onderneming of instantie zelf als voor de verwerking verantwoordelijk te beschouwen, en niet een specifieke persoon binnen de onderneming of de instantie. De onderneming of instantie is uiteindelijk verantwoordelijk voor de verwerking van gegevens en de verplichtingen die voortvloeien uit de wetgeving voor gegevensbescherming, tenzij duidelijk blijkt dat een natuurlijke persoon verantwoordelijk is, bijvoorbeeld wanneer een natuurlijke persoon die bij een onderneming of overheidsinstantie werkzaam is gegevens voor zijn of haar eigen doelen buiten de onderneming gebruikt.
- De mogelijkheid van *gezamenlijke verantwoordelijkheid* houdt rekening met het steeds toenemende aantal situaties waarin verschillende partijen als voor de verwerking verantwoordelijke optreden. Deze gezamenlijke verantwoordelijkheid dient op dezelfde wijze te worden beoordeeld als de “individuele”

verantwoordelijkheid. Daarbij dient een inhoudelijke en functionele benadering te worden gevolgd, en met name te worden gezien of de wezenlijke aspecten van de middelen door meer dan een partij worden vastgesteld.

Wanneer van gezamenlijke verantwoordelijkheid sprake is, hebben partijen bij het vaststellen van doelen van, en middelen voor de verwerking niet altijd een even grote rol en inbreng. In dit advies zijn vele voorbeelden opgenomen van verschillende vormen van gezamenlijke verantwoordelijkheid. Wanneer niet elke partij evenveel zeggenschap heeft, is ook niet elke partij in een zelfde mate verantwoordelijk en aansprakelijk, en zeker niet in alle gevallen kan worden aangenomen dat er sprake is van een “gezamenlijke en hoofdelijke” aansprakelijkheid. Bovendien is het goed mogelijk dat in complexe systemen met meerdere partijen de toegang tot persoonsgegevens en de uitoefening van andere rechten van betrokkenen op verschillende niveaus door verschillende partijen kan worden gewaarborgd.

In dit advies wordt ook gekeken naar het begrip “verwerker”, waarvan het bestaan afhangt van een besluit van de voor de verwerking verantwoordelijke, die kan besluiten om gegevens binnen zijn eigen organisatie te verwerken of de verwerking daarvan geheel of gedeeltelijk aan een externe organisatie te delegeren. De twee centrale voorwaarden om een partij als verwerker te kunnen aanmerken zijn dus enerzijds dat het een aparte rechtspersoon is, die los van de voor de verwerking verantwoordelijke staat, en anderzijds dat deze partij persoonsgegevens namens die voor de verwerking verantwoordelijke verwerkt. Deze verwerking kan zich beperken tot een zeer specifieke taak of context of ruimte laten voor een zekere mate van handelingsvrijheid ten aanzien van de wijze waarop de belangen van de voor de verwerking verantwoordelijke kunnen worden gediend, waarbij de verwerker de meest geschikte technische en organisatorische middelen kan kiezen.

Daarnaast is de rol van verwerker niet gekoppeld aan de aard van een partij die persoonsgegevens verwerkt maar wel afhankelijk van zijn concrete activiteiten in een specifiek kader en met betrekking tot specifieke gehelen van gegevens of bewerkingen. Criteria die een nuttige rol kunnen vervullen bij het vaststellen van de hoedanigheid van de diverse bij de verwerking betrokken partijen zijn de mate waarin de voor de verwerking verantwoordelijke tevoren opdrachten heeft gegeven, de bewaking door de voor de verwerking verantwoordelijke van de kwaliteit van de dienst, de zichtbaarheid voor betrokkenen, de deskundigheid van de partijen en de autonome beslissingsbevoegdheid waarover de diverse partijen nog beschikken.

De restcategorie van “derde” wordt omschreven als zijnde elke partij die geen specifieke legitimiteit of bevoegdheid heeft – bijvoorbeeld voortvloeiend uit zijn rol als voor de verwerking verantwoordelijke, verwerker, of hun werknemer – bij de verwerking van persoonsgegevens.

* * *

De Groep erkent dat het moeilijk is om de definities van de richtlijn toe te passen in een complexe omgeving, waarin vele scenario's mogelijk zijn met voor de verwerking verantwoordelijken en verwerkers, alleen of gezamenlijk, met verschillende mates van autonomie en verantwoordelijkheid.

In zijn analyse heeft de groep benadrukt dat verantwoordelijkheden zodanig moeten worden belegd dat de naleving van de regelgeving met betrekking tot gegevensbescherming in de praktijk voldoende is gewaarborgd. De groep heeft echter geen aanleiding gevonden om te veronderstellen dat het huidige onderscheid tussen voor de verwerking verantwoordelijken en verwerkers vanuit dat oogpunt niet langer relevant en werkbaar zou zijn.

Daarom hoopt de groep dat met de toelichting in dit advies en de vele concrete voorbeelden uit de dagelijkse praktijk van gegevensbeschermingsautoriteiten een bijdrage kan worden geleverd aan een effectieve informatievoorziening over de wijze waarop deze kerndefinities van de richtlijn moeten worden geïnterpreteerd.

Brussel, 16 februari 2010

*Namens de Groep,
Jacob Kohnstamm
Voorzitter*