Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1997–1998

25 892 Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)

Nr. 3

MEMORIE VAN TOELICHTING[1]

INHOUDSOPGAVE

Algemeen deel

[1] De meegezonden adviezen zijn ter inzage gelegd bij de afdeling Parlementaire Documentatie.

KST27835
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 1998

ALGEMEEN DEEL

1. De informatiemaatschappij en de interne markt

Elk tijdperk in de geschiedenis kent zijn thema's en deze thema's kunnen soms voor een krachtige stroomversnelling zorgen. Ook ons tijdperk kent dergelijke thema's: algemeen wordt aangenomen dat de totstandkoming van de informatiemaatschappij zo'n thema is. Hiermee voltrekt zich een nieuwe «industriële revolutie» die op langere termijn mogelijk niet onderdoet voor de vorige. Sinds enige tijd maakt de omvang van de informatie en het gemak waarmee deze verkregen en verspreid kan worden een welhaast exponentiële groei door. Met behulp van geautomatiseerde zoeksystemen kan nu of in de naaste toekomst op nagenoeg elke werkplek en in elke huiskamer in de westerse wereld een vrijwel onbegrensde hoeveelheid informatie snel worden geraadpleegd. Daarnaast opent de mogelijkheid op een dergelijke wijze en in die mate kennis en informatie te verspreiden ongekende bronnen voor intensivering en verbetering van produktieprocessen.
De in deze ontwikkelingen besloten liggende mogelijkheden voor economische groei trekken de aandacht van velen. Zo nam reeds in 1991 de vice-president van de Verenigde Staten het initiatief voor de bevordering van wat hij aanduidde als de elektronische snelweg[1]. Op 26 mei 1994 bood de Europese commissaris Bangemann zijn rapport «Europe and the global information society» aan aan de Europese Raad van Corfu. In dit rapport wordt ter wille van de economische ontwikkeling en parallel aan de Amerikaanse ontwikkelingen, bevordering van de elektronische snelweg bepleit.
Ondanks de hoopvol stemmende mogelijkheden van de informatiemaatschappij mag niet vergeten worden dat aan deze mogelijkheden ook gevaren kleven. Gevaren die de menselijke waardigheid kunnen aantasten. Bijvoorbeeld één van de schaduwzijden van de informatiemaatschappij is de inbreuk op de persoonlijke levenssfeer die het gevolg kan zijn van een ongebreidelde vergaring, bewerking en verspreiding van persoonsgegevens. De vruchten van nieuwe technische mogelijkheden moeten worden verenigd met een nieuwe verantwoordelijkheid van de mens om zodanig met informatie om te gaan, dat een humane informatiemaatschappij als nieuw cultuurgoed wordt verwerkelijkt. Dit noopt tot de ontwikkeling van nieuwe normen en waarden die voor een deel ook in het recht moeten worden vastgelegd.
De economische voordelen van de elektronische snelweg waren begin 1995 voorwerp van overleg in de groep van de zeven grootste gendustrialiseerde landen, de G7. Tijdens dit overleg kwamen ook de gevaren van de elektronische snelweg ter sprake. Ten aanzien van deze gevaren was een conclusie van dit overleg dat een internationale aanpak gewenst zou zijn. De reden hiervoor is dat informatie op de elektronische snelweg een immaterieel karakter heeft en dat het als gevolg hiervan moeilijk is om aanknopingspunten te vinden bij een bepaald territoir en dus te bepalen onder welke jurisdictie de informatie valt. Met het oog op de totstandbrenging van de informatiemaatschappij in de interne markt heeft de Europese Commissie in 1990 een regeling voorgesteld voor het omgaan met persoonsgegevens. Deze regeling, in de vorm van een richtlijn tot harmonisatie van de desbetrefffende wetgeving in de lidstaten, was noodzakelijk om het vertrouwen van de consument te behouden wanneer hij zich op deze snelweg zou begeven. In verband met de elektronische snelweg kan op het niveau van de Unie gewezen worden op artikel 129 B tot en met 129 D van het verdrag tot oprichting van de Europese Gemeenschap (verder te noemen het EG-verdrag).

[1] De elektronische snelweg is een metafoor voor het internationale computernetwerk. Hieronder valt «Internet», maar ook andere (toekomstige) wijzen van elektronisch gegevensverkeer.

2. Voorgeschiedenis van de totstandkoming van de richtlijn

De gevaren voor het individu die de informatiemaatschappij met zich mee zou kunnen brengen, hebben reeds enige tijd de belangstelling van het Europees Parlement. Op 8 april 1976 droeg het Europees Parlement in een resolutie de Commissie op feiten en inlichtingen te verzamelen ter bescherming van de rechten van het individu in verband met mogelijke risico's die voortkomen uit de ontwikkeling van de informatietechnologie[1]. Enkele jaren later, op 8 mei 1979, nam het Europees Parlement een tweede resolutie aan[2]. In het verlengde hiervan werd de Commissie uitdrukkelijk gevraagd een richtlijn te ontwerpen, rekening houdend met het parlement. Ten slotte nam het Europees Parlement op 9 maart 1982 een resolutie aan[3], waarin de Commissie uitdrukkelijk werd gevraagd een richtlijn te ontwerpen, rekening houdend met de wensen van het parlement.
In 1981 kwam het Verdrag inzake gegevensbescherming van de Raad van Europa[4] tot stand. Blijkens artikel 4, tweede lid, moet een staat voorafgaand aan de bekrachtiging zijn wetgeving daarmee in overeenstemming hebben gebracht. Artikel 12 bevat een bepaling over vrij gegevensverkeer. Een groot aantal landen binnen de Europese Unie heeft sindsdien het verdrag bekrachtigd. Het vrije gegevensverkeer binnen de Unie bleek daarmee echter geenszins verzekerd. Verder moesten met de te verwachten ontwikkeling van de informatietechnologie verdergaande belemmeringen in het vrije gegevensverkeer worden gevreesd. Bovendien leden met name in Italië en Griekenland diverse pogingen om tot wetgeving te komen schipbreuk. De totstandkoming van de interne markt en de economische voordelen die daarvan worden verwacht, konden langs deze weg niet worden verzekerd.
De Commissie kwam, gevolg gevend aan de aandrang van het parlement, daarom op 27 juli 1990 met een eigen voorstel. Het werd ingediend bij het Europees Parlement en bij de Raad van Ministers van de Europese Unie. Het had als doel het vrije verkeer van persoonsgegevens binnen de Unie te garanderen. Het middel hiertoe was een vergaande, zij het geen volledige, harmonisatie van de bestaande wetten op dit terrein van de Lid-Staten. Gelet op artikel 100A, derde lid, van het EG-verdrag is de Commissie uitgegaan van een hoog niveau van bescherming. Inzet van de harmonisatie was te trachten geen afbreuk te doen aan het niveau van bescherming van persoonsgegevens in de Lid-Staten.[5]
Het overleg in de Raad heeft er toe geleid dat dit hoge niveau van bescherming niet op alle punten is doorgezet; de onderlinge verschillen tussen de Lid-Staten bleken daarvoor toch te groot. Alle landen hebben op onderdelen op hun eigen niveau van bescherming moeten inleveren. Zo is voor Nederland de vergaande risico-aansprakelijkheid van artikel 9 van de Wet persoonsregistraties (WPR) in de nieuwe wetgeving enigszins afgezwakt.
Naar aanleiding van het advies van het Europees Parlement diende de Commissie op 15 oktober 1992 een gewijzigd voorstel van de richtlijn bij de Raad in[6]. Belangenorganisaties hadden de mogelijkheid op het gewijzigde voorstel te reageren zowel bij de Europese Commissie als bij de delegaties van de lid-staten. Veel organisaties hebben van deze mogelijkheid gebruik gemaakt.
In Nederland zijn de reacties geïnventariseerd. Deze hebben telkens een rol gespeeld bij de voorbereiding van het Nederlands standpunt in de raadswerkgroep waar over het ontwerp van de richtlijn werd onderhandeld. Daarnaast hebben vertegenwoordigers van het Ministerie van Justitie meerdere keren overleg gehad met de Werkgroep persoonsregistraties van de Raad van de Centrale Ondernemingsorganisaties (RCO). Voorafgaand aan elke bijeenkomst van de desbetreffende raadswerkgroep in Brussel vond interdepartementaal overleg plaats. Dit

[1] PbEG C 100 van 3 mei 1976, blz. 27.
[2] PbEG C 140 van 5 juni 1979, blz. 34.
[3] PbEG C 87/39 van 9 maart 1982.
[4] Trb. 1988, 7.
[5] Zie ook overweging 10 bij de richtlijn.
[6] COM (92) 422 def. syn 287, gepubliceerd in PbEG C 311-/30 van 27 november 1992.

gebeurde onder leiding van een vertegenwoordiger van het Ministerie van Buitenlandse Zaken.
De vaste Commissie voor Justitie van de Tweede Kamer heeft op 27 augustus 1993 een aantal vragen over de richtlijn gesteld, die de Minister van Justitie heeft beantwoord[1]. Precies twee maanden later vond hierover mondeling overleg plaats[2]. Op 29 september 1994 hebben de vaste Kamercommissie voor Justitie en de algemene Commissie voor Europese Zaken een nader overleg gehad met de Minister van Justitie[3]. Dit gebeurde naar aanleiding van een brief van 27 juni 1994 van de Minister van Justitie, mede aangeboden namens de Staatssecretaris van Buitenlandse Zaken, over de nadere ontwikkelingen bij de totstandkoming van de richtlijn[4]. Op 9 november vond er een overleg plaats met ambtenaren van de Europese Commissie[5] en tot slot vond op 7 december 1994 een laatste overleg van beide commissies plaats met de Minister van Justitie en de Staatssecretaris van Buitenlandse Zaken. Op basis van dit overleg heeft de Nederlandse regering zich op 8 december 1994 in de Raad van Ministers van de Europese Unie uitgesproken ten gunste van een gemeenschappelijk standpunt overeenkomstig het ontwerp van de richtlijn. Mede naar aanleiding van het overleg met de commissies uit de Tweede Kamer heeft de Nederlandse delegatie tot uitgangspunt genomen dat aan de bescherming van de persoonlijke levenssfeer zoals deze is geregeld in de WPR in beginsel geen afbreuk kan worden gedaan. Ook andere landen namen ten opzichte van hun eigen wetgeving een vergelijkbaar standpunt in.
De Raad stelde op 20 februari 1995 definitief het gemeenschappelijk standpunt vast[6]. Over dit gemeenschappelijk standpunt bracht het Europees Parlement op 14 juni 1995 in tweede lezing een advies uit. De Europese Commissie nam van dit advies zeven amendementen over. De Raad van Ministers nam op 24 juli 1995 de geamendeerde tekst van de richtlijn over. De Staatssecretaris van Buitenlandse Zaken heeft de Voorzitter van de Algemene Commissie voor Europese Zaken hiervan op 25 juli 1995 per brief op de hoogte gesteld. De richtlijn kwam tot stand op 24 oktober 1995 door de gezamenlijke ondertekening door de voorzitters van het Europees Parlement en de Raad. Hij werd gepubliceerd op 23 november 1995 (PbEG L 281, blz. 31). De implementatietermijn loopt af op 24 oktober 1998. Daarmee is binnen de Europese Gemeenschap, voor zover het het communautaire recht betreft, een gemeenschappelijk rechtsgebied wat betreft de bescherming van persoonsgegevens tot stand gebracht. Ingevolge de jurisprudentie van het Europese Hof van Justitie heeft dit onder meer tot gevolg dat op dit terrein de Gemeenschap in internationale gremia, bij voorbeeld de Raad van Europa, een gecoördineerd standpunt dient uit te dragen. Dit wordt telkens bij gekwalificeerde meerderheid binnen de Gemeenschap vastgetsteld. Deze procedure is reeds gevolgd bij bij voorbeeld het ontwerp van de Aanbeveling van de Raad van Europa over de verwerking van persoonsgegevens voor statistische doeleinden. Daarnaast zal de jurisprudentie van het Europese Hof van Justitie richting geven aan de verdere rechtsontwikkeling binnen de Gemeenschap. De rechtsontwikkeling binnen de Gemeenschap zal gevolgen hebben voor de nationale rechtsontwikkeling.

Het onderhavige voorstel voor een nieuwe Wet bescherming persoonsgegevens (verder te noemen WBP) strekt tot de implementatie van de richtlijn. Zoals opgemerkt leidt de richtlijn niet tot een volledige harmonisatie van de privacywetgeving, maar biedt zij een zekere bandbreedte: er is een zeker minimum en een maximum dat niet mag worden overschreden. Binnen dit kader zijn de Lid-Staten vrij hun wetgeving in te richten. Anderzijds dient gewezen te worden op artikel 5 van de richtlijn. Deze bepaling geeft de opdracht aan de Lid-Staten binnen de grenzen van Hoofdstuk II van de richtlijn nader de voorwaarden te bepalen waaronder de verwerkingen van persoonsgegevens rechtmatig zijn. De vraag rijst op

[1] Kamerstukken II 1992/93, 22 800 VI, nr 43.
[2] Kamerstukken II 1993/94, 23 400 VI, nr 9.
[3] zie voor het verslag Kamerstukken II 1994/95, 23 900 VI, nr 11.
[4] zie Kamerstukken II 1994/95, 23 900 VI, nr 11, blz. 12 e.v.
[5] zie Kamerstukken II 1994/95 VI, nr 13.
[6] PbEG van 13 april 1995, C 93.

welke wijze de wetgever invulling dient te geven aan deze bepaling. Verschillende benaderingen zijn mogelijk.
Een eerste uitwerking van artikel 5 van de richtlijn zou kunnen zijn om steeds elke norm van hoofdstuk II van de richtlijn in het onderhavige wetsvoorstel zelf te concretiseren. Het voordeel van deze benadering is dat op een heldere wijze in een en dezelfde wet uitvoering wordt gegeven aan de verplichting van artikel 5. Voorts zou een preciezere normering in de WBP de rechtszekerheid kunnen bevorderen. Daar staan evenwel belangrijke nadelen tegenover. Precisering van normen die in zeer uiteenlopende casusposities moeten worden toegepast, kan tot gevolg hebben dat de wet een keurslijf wordt dat onvoldoende op de praktijk is toegesneden. Dat gevaar is zeker aanwezig op het onderhavige terrein. Te vergaande detaillering in de WBP houdt bovendien het risico in dat de bandbreedte van de richtlijn wordt overschreden.
Vanwege de nadelen die aan deze eerste benadering zijn verbonden, is gekozen voor een genuanceerdere benadering waarin de precisering slechts deels in het wetsvoorstel heeft plaatsgevonden. Als voorbeeld kan worden gewezen op artikel 9, tweede lid, waarin factoren worden geschetst die een rol spelen bij de vraag of een verwerking van persoonsgegevens verenigbaar is met het doel waarvoor deze gegevens zijn verkregen. In dit voorschrift wordt artikel 6, eerste lid, onderdeel b, van de richtlijn geconcretiseerd. Ook de voorschriften met betrekking tot de verwerking van bijzondere gegevens zijn op diverse punten te beschouwen als een concretisering van de uitzonderingen op het verbod van artikel 8, eerste lid, van de richtlijn.
Daarnaast zal de concretisering van de richtlijn in belangrijke mate op een andere wijze dienen plaats te vinden. In sectorale wetgeving worden reeds thans nadere voorwaarden gesteld ten aanzien van het verwerken van persoonsgegevens. Zo geeft de Wet geneeskundige behandelingsovereenkomst aanvullende voorschriften op het terrein van de verwerking van persoonsgegevens ten behoeve van de medische behandeling van personen. Ook de Archiefwet 1995 kan als zodanig worden beschouwd. Op deze wijze kan worden aangesloten bij de behoefte in de specifieke sectorale wet een nadere invulling te geven aan het kader dat de WBP biedt en waarin expliciet rekening wordt gehouden met de hierdoor bestreken vormen van gegevensverwerking. In bepaalde gevallen is het voorts mogelijk de concretisering via zelfregulering na te streven. Organisaties kunnen er voor kiezen zelf in een gedragscode een nadere invulling te geven aan het normenkader van de WBP. Ook blijft het mogelijk in reglementen vast te leggen hoe binnen de organisatie met de verwerking van persoonsgegevens wordt omgegaan. Tot slot zal een deel van de concretisering ook plaats moeten hebben in de jurisprudentie.
Binnen de ruimte die de richtlijn liet, is uitgegaan van het beschermingsniveau van de WPR, voor zover de evaluaties geen aanwijzingen hebben opgeleverd voor een afwijkend standpunt (zie verder onder 15). De thans geldende WPR komt daarmee geheel te vervallen.

3. De bescherming van persoonsgegevens als object van wetgeving

In het tijdperk dat voorafging aan de informatiemaatschappij beschermden verschillende onderdelen van het recht het individu tegen aantasting van eer en goede naam en tegen inbreuken op de persoonlijke levenssfeer. Jurisprudentie inzake onrechtmatige daad bij ontoelaatbare publikaties over iemands persoon; strafbepalingen inzake belediging, smaad en laster; regelingen omtrent archivering van overheidsdocumenten en de geheimhoudingsplicht van hulpverleners, vormden op uiteenlopende wijze een bescherming tegen onoirbaar geachte vormen van omgaan met persoonsgegevens. Het object van de regelgeving was

hier echter steeds verschillend; persoonsgegevens vormden niet zelfstandig het voorwerp van regelgeving.
Met de komst van nieuwe technieken kunnen grote hoeveelheden persoonsgegevens gemakkelijk worden opgeslagen en ontsloten. Gegevens zijn een bron van informatie; informatie is de basis van kennis en kennis is macht. Deze macht kan ten goede, maar ook ten kwade worden aangewend. Met dit besef ontstaat de behoefte dergelijke samenhangende verzamelingen van persoonsgegevens als afzonderlijke juridische eenheid tot voorwerp van regelgeving te verheffen.
Bij de herziening van de Grondwet in 1983 werd in artikel 10, eerste lid, de bescherming van de persoonlijke levenssfeer uitdrukkelijk als klassiek grondrecht geformuleerd. Daarnaast werd in het tweede en derde lid aan de formele wetgever de opdracht gegeven om regels te stellen omtrent de bescherming van persoonsgegevens. Artikel 10 sloot aan bij zich gelijktijdig ontwikkelende jurisprudentie van het Europese Hof voor de rechten van de mens over de omvang van het recht op respect voor het privé-leven van het individu, neergelegd in artikel 8 van het EVRM, in relatie tot de opslag en het gebruik van persoonsgegevens.
De Wet persoonsregistraties, die op 1 juli 1989 in werking trad, geeft uitvoering aan artikel 10 van de Grondwet en geeft regels voor samenhangende verzamelingen van persoonsgegevens. Deze wet regelt eveneens omstandigheden waarin voorheen geen inbreuk op enig recht werd aangenomen. Met deze wet convergeerde de ontwikkeling van voorheen onderscheiden rechtsgebieden en werd aangeknoopt bij een maatschappelijke ontwikkeling waarbij op enkele plaatsen in computers grote verzamelingen persoonsgegevens werden aangelegd en van daaruit aan gebruikers werden verstrekt.
De ontwikkeling van de techniek verloopt evenwel onafhankelijk van de ontwikkeling van het recht en het vormt een uitdaging aan de rechtspraktijk nieuwe juridische begrippen te ontwikkelen, die tot op zekere hoogte technologie-neutraal zijn en daardoor minder snel verouderen ten gevolge van technische ontwikkelingen. Het begrip «persoonsregistratie» is een voorbeeld van een technologie-afhankelijk begrip en het onderhavige wetsvoorstel neemt dan ook het meer neutrale begrip «gegevensverwerking» als aangrijpingspunt. Met dit nieuwe begrip wordt aangesloten bij de realiteit van netwerkvorming waarin de computers van weleer vaak slechts een ondergeschikt knooppunt vormen.

4. Grondrechtelijke aspecten

4.1 De Grondwet en de mensenrechtenverdragen

Artikel 10, eerste lid, van de Grondwet erkent het recht op eerbiediging van de persoonlijke levenssfeer en schrijft voor dat inbreuken daarop bij of krachtens wet in formele zin moeten zijn geregeld. Het tweede en derde lid verlangen van de wetgever nadere maatregelen over het omgaan met persoonsgegevens. De WPR en het onderhavige wetsvoorstel als opvolger van deze wet, vloeien voort uit de opdracht in de Grondwet tot het geven van deze regels. Niet elke verwerking van persoonsgegevens vormt een inbreuk op de persoonlijke levenssfeer. Wanneer dit wel en wanneer niet het geval is, kan in zijn algemeenheid niet worden aangegeven; het is afhankelijk van de aard van de gegevens en de wijze waarop deze worden gebruikt. Wel kan worden aangenomen dat de verwerking van gevoelige gegevens, gelet op hun aard, onafhankelijk van de samenhang waar in zij worden gebruikt, veelal een dergelijke inbreuk wordt gemaakt. Het wetsvoorstel geeft ter uitvoering van artikel 10, derde lid, van de Grondwet, de betrokkene aanspraken met betrekking tot de verwerking van hem betreffende gegevens, ongeacht de vraag of er sprake is van een inbreuk op de persoonlijke levenssfeer.
In het volkenrecht is het recht op bescherming van de persoonlijke

levenssfeer gewaarborgd in artikel 8 van het EVRM en in artikel 17 van het IVBPR. De in deze verdragen gebruikte term «privé leven», heeft dezelfde betekenis als de term «persoonlijke levenssfeer» in de Grondwet. Artikel 8 van het EVRM eist dat als inbreuken plaatsvinden, deze voorzien moeten zijn in de wet en noodzakelijk moeten zijn op grond van een aantal nader aangegeven gronden. Uit de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) blijkt dat een beperking op verschillende wijze «bij de wet» kan zijn voorzien: een wet in materiële zin, een beleidsregel of zelfs een in de jurisprudentie gevormde regel. Deze wet of regel moet echter wel voor de burger toegankelijk zijn en voorts zo precies zijn dat de burger in staat is zijn concrete gedrag daarnaar te richten. Naast artikel 8 EVRM geven de WPR en de WBP ook uitvoering aan het eerdergenoemde, op artikel 8 EVRM steunende Verdrag inzake gegevensbescherming.

Daarnaast heeft het wetsvoorstel tevens betrekking op de bescherming van andere in de Grondwet en verdragen neergelegde rechten, zoals het non-discriminatiebeginsel. Wij komen daarop hieronder in paragraaf 4.5 nog terug. Een ongebreidelde verwerking van persoonsgegevens kan ook een negatieve uitwerking hebben de vrijheid van meningsuiting en politieke participatie.
Ten slotte houdt het recht van de betrokkene op informatie van de verantwoordelijke verband het recht op toegang tot de rechter. Dit recht is neergelegd in artikel 13 EVRM en artikel 17 van de Grondwet. Dit recht omvat zowel het recht om op initiatief van de verantwoordelijke te worden geïnformeerd over de verwerking van gegevens (de artikelen 33 en 34) als het recht op kennisneming, uitgeoefend op initiatief van de betrokkene jegens de verantwoordelijke (artikel 35). De verwerking van persoonsgegevens onttrekt zich naar haar aard aan kenbaarheid door de betrokkene, terwijl wel zijn rechten in het geding zijn. Compenserende wettelijke maatregelen, daaronder begrepen de bevoegdheden van de Registratiekamer, zijn daarom nodig om de uitoefening van rechten desondanks mogelijk te maken.

4.2 Subsidiariteits- en proportionaliteitsbeginsel

Bij de toepassing van de in grondrechtenbepalingen opgenomen beperkingsclausules spelen het proportionaliteits- en subsidiariteitsbeginsel een belangrijke rol. Het evenredigheids- of proportionaliteitsbeginsel geldt rechtstreeks op grond van artikel 8 van het EVRM. Het Europese Hof van Justitie van de Europese Unie te Luxemburg aanvaardt in zijn jurisprudentie de grondslagen van het recht in de Lid-Staten van de Unie. Het EVRM en de daarop gebaseerde jurisprudentie van het Hof te Straatsburg worden tot deze grondslagen gerekend. In deze jurisprudentie neemt het proportionaliteitsbeginsel een zeer centrale positie in. De inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel. Deze toets speelt een rol wanneer het gaat om de toepassing van de uitoefening van een bevoegdheid tot het verkrijgen van persoonsgegevens, waarbij een inbreuk op een grondrecht aan de orde is. Zij vergt een belangenafweging aan de hand van de omstandigheden van het concrete geval. Er moet telkens sprake zijn van «a fair balance that has to be struck between the demands of the general interest and the interest of the individual».
Het subsidiariteitsbeginsel maakt in deze jurisprudentie geen expliciet onderdeel uit van het noodzakelijkheidsvereiste, maar wordt door het Hof wel beschouwd als een factor die een rol speelt in het kader van de evenredigheidstoetsing. Het doel waarvoor de persoonsgegevens worden verwerkt dient in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze te

kunnen worden verwerkelijkt. Op degene die persoonsgegevens verwerkt rust de plicht om binnen redelijke grenzen een inbreuk op de persoonlijke levenssfeer van anderen te vermijden dan wel zo beperkt mogelijk te houden. Deze plicht omvat een tweetal aspecten. Allereerst dient men af te zien van de verwerking van persoonsgegevens indien hetzelfde doel ook langs andere weg en met minder ingrijpende middelen kan worden gerealiseerd, bij voorbeeld door de vergaring van anonieme gegevens. Wordt desondanks tot gegevensverwerking overgegaan, dan is van belang dat degene die gegevens wil verwerken in redelijkheid alle eventuele bestaande mogelijkheden benut om de inbreuk op de persoonlijke levenssfeer van betrokkenen te beperken.
Deze mede op de grondrechten gebaseerde beginselen nemen ook in het onderhavige wetsvoorstel een centrale positie in. Op veel plaatsen in het wetsvoorstel wordt de verwerking van gegevens gebonden aan het noodzakelijkheidscriterium. De norm behelst in die gevallen de noodzakelijkheidstoets in relatie tot een welbepaald, concreet aangeduid of nader aan te duiden doel.

4.3 Informationele zelfbeschikking en transparantie

In een uitspraak van 15 december 1983 heeft het Duitse Constitutionele Hof uit het algemene persoonlijkheidsrecht en de menselijke waardigheid het beginsel afgeleid dat binnen de relatie overheid en burger, ieder zelf mag bepalen in hoeverre informatie over hem wordt gebruikt en verder bekendgemaakt; zij het dat het individu zich in het algemeen belang bepaalde beperkingen op dit grondrecht moet laten welgevallen. Dit beginsel wordt in de Duitse jurisprudentie aangeduid als het beginsel van de informationele zelfbeschikking.
De vraag rijst in hoeverre de zeggenschap van de betrokkene over de hem betreffende gegevens binnen de grenzen van de Nederlandse wetgeving, moet worden gezien als een uitwerking van het beginsel van informationele zelfbeschikking. In hoeverre heeft deze zeggenschap in Nederlandse wetgeving materiële betekenis, in de zin dat de betrokkene zelf in beginsel kan uitmaken of een ander gegevens over hem vastlegt en gebruikt? In de vorm zoals erkend in de Duitse jurisprudentie, zelfs al zijn daarop uitzonderingen mogelijk, is dit beginsel in Nederland geen onderdeel van het geldend recht. Ook de harmonisatie van het recht inzake gegevensbescherming tussen de landen van de UNie dwingt niet tot een receptie van dit beginsel in de Nederlandse rechtsorde. Hier wordt aangesloten bij de mening van onze ambtsvoorgangers, dat het Nederlands recht zich hierin, ook wat betreft zijn uitgangspunten, onderscheidt van het Duitse[1]. In het Nederlandse systeem geldt buiten de werkingssfeer van artikel 10, eerste lid, van de Grondwet als algemeen uitgangspunt dat noch de handelingsvrijheid van de degene die persoonsgegevens verwerkt, noch het recht op bescherming van de persoonlijke levenssfeer van de betrokkene in abstracto zwaarder weegt. Als in een concreet geval beide belangen dreigen te botsen, dienen zij tegen elkaar te worden afgewogen, waarbij rekening moet worden gehouden met de bijzondere (grondwettelijke) waarde van het recht op bescherming van de persoonlijke levenssfeer. Het wetsvoorstel beoogt slechts voor deze afweging het nodige instrumentarium aan te reiken. Het concretiseert in dat verband de criteria aan de hand waarvan moet worden afgewogen, of maakt in een enkel geval, bijvoorbeeld bij gevoelige gegevens, zelf de verlangde afweging.
Het uitgangspunt in de WPR is daarbij dat iedereen in de gelegenheid moet zijn om na te kunnen gaan waar gegevens over hem zijn vastgelegd en worden verwerkt. De betrokkene die de wijze waarop zijn gegevens worden verwerkt onrechtmatig vindt, kan dit zelf langs privaatrechtelijke weg aanvechten. Hij moet dan wel van het bestaan van de verwerking van hem betreffende gegevens op de hoogte zijn. Duidelijkheid over de

[1] zie de memorie van antwoord aan de Tweede Kamer inzake de Wet persoonsregistraties (Kamerstukken II 1986/87, 19 095, nr. 6, blz. 15.

verwerking van gegevens, de zogenaamde transparantie, kan langs publiekrechtelijke weg worden afgedwongen. De strafbepalingen in artikel 50 WPR zijn hierop gericht. Uitzonderingen op het beginsel van transparantie zijn uiteraard mogelijk, maar de uitzonderingen moeten strikt worden geïnterpreteerd. Dit uitgangspunt vormt ook een belangrijke basis voor het onderhavige wetsvoorstel. Bij de diverse onderdelen van deze memorie komen wij daar nog op terug.

4.4 Het algemeen persoonlijkheidsrecht

De afwijzing van het informationele zelfbeschikkingsrecht sluit verdergaande beïnvloeding vanuit het Duitse recht in de toekomst echter niet uit. Van een zodanige beïnvloeding lijkt sprake te zijn geweest in een recent arrest van de Hoge Raad, waarin het recht om te weten van welke ouders men afstamt in principiële zin werd erkend[1]. In dit arrest nam de Hoge Raad een «aan grondrechten als het recht op respect voor het privé-leven, het recht op vrijheid van gedachte, geweten en godsdienst en het recht op vrijheid van meningsuiting ten grondslag liggend algemeen persoonlijkheidsrecht» tot uitgangspunt. In de Duitse Grondwet – waar de conclusie van de AG bij dit arrest naar verwees – is dit recht in algemene zin omschreven als het recht van een ieder op ontplooiing van zijn persoonlijkheid. Het gaat om een recht dat onlosmakelijk met de persoonlijkheid van het individu is verbonden.
Tegen de achtergrond van het aldus te karakteriseren rechtsgoed wordt aangenomen dat persoonlijkheidsrechten in beginsel niet overdraagbaar zijn en daarom niet voor contractuele afstand vatbaar zijn. Vanuit deze algemene notie gelden de voorschriften van de WBP als dwingend recht. Daarmee wordt geen verandering beoogd ten opzichte van de huidige situatie want de WPR bevat blijkens de parlementaire behandeling eveneens voorschriften van dwingend recht[2]. Voorts sluit de kwalificatie van de WBP als dwingend recht goed aan bij de doorwerking van het grondrecht op eerbiediging van de persoonlijke levenssfeer in particuliere rechtsverhoudingen. Deze doorwerking, ook wel aangeduid als horizontale werking, is in beginsel door de Hoge Raad erkend[3]. De kwalificatie van de WBP als dwingend recht heeft tot gevolg dat een rechtshandeling waarbij afstand wordt gedaan van de door de WBP toegekende rechten in beginsel wegens strijd met de openbare orde nietig is op grond van artikel 3:40 van het Burgerlijk Wetboek (BW).
Een en ander betekent dat contractuele afwijkingen van de wettelijke voorschriften niet toelaatbaar zijn, tenzij dat in de wet uitdrukkelijk wordt bepaald. In dit verband kan worden gewezen op artikel 8, onder a, van de WBP waarin bepaald wordt dat gegevensverwerking geoorloofd is als de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend. Aan de gegeven toestemming worden wel zware eisen gesteld. Dit ligt in het verlengde van het BW. Op grond van het BW een dergelijke toestemming, indien deze rechtstreeks voortkomt uit een afhankelijkheidssituatie, nietig zijn wegens misbruik van omstandigheden[4]. Het BW biedt op dit punt voldoende ruimte voor doorwerking van uit de richtlijn voortvloeiende privacyrechten.
Voorts wordt in artikel 8, onder b, van het wetsvoorstel bepaald dat verwerking van gegevens is toegestaan voor zover dat noodzakelijk is voor de uitvoering van een overeenkomst waarbij betrokkene partij is. Hierbij gaat het om de situatie waarin de overeenkomst zelf niet gericht is op de verwerking van persoonsgegevens, maar waarbij de verwerking van persoonsgegevens een noodzakelijke bijkomstigheid is. Anders dan in artikel 8, onder a, is gegevensverwerking hier dus accessoir.

4.5 Verhouding tot andere grondrechten

De verwerking van persoonsgegevens kan ook andere grondrechten dan

[1] HR 15 april 1994, NJ 1994, 608.
[2] Kamerstukken I 1987/88, 19 095, nr. 2b, blz. 12.
[3] HR 9 januari 1987, NJ 1987, 928.
[4] art. 3:44 BW.

het recht op privacy raken. Het gaat hierbij met name om het gelijkheidsbeginsel, zoals verwoord in artikel 1 van de Grondwet. Dit beginsel is nader uitgewerkt in de Algemene wet gelijke behandeling (AWGB). Deze wet verbiedt het maken van onderscheid tussen personen op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat bij verschillende vormen van economisch en maatschappelijk verkeer, tenzij de wet het maken van onderscheid toestaat dan wel het om indirect onderscheid gaat dat objectief gerechtvaardigd is. De meeste van de genoemde gronden worden ook vermeld in een aantal bepalingen in dit wetsvoorstel over de verwerking van bijzondere gegevens. Deze bepalingen – zie de artikelen 16, 17, 18 en 19 – bieden extra waarborgen bij het verwerken van persoonsgegevens betreffende onder meer iemands godsdienst of levensovertuiging, ras, politieke gezindheid en seksuele leven. Aldus werkt het gelijkheidsbeginsel oom door in dit wetsvoorstel.
Een verwerking met de intentie om een ongerechtvaardigd onderscheid te maken, is onrechtmatig in de zin van artikel 6 van de WBP. Verwerking van persoonsgegevens omvat ook het verzamelen van persoonsgegevens. Het verzamelen valt weer uiteen in twee deelactiviteiten: het vragen en het verkrijgen van gegevens. Er is al sprake van verzamelen als persoonsgegevens mondeling of schriftelijk worden gevraagd. Daarbij is niet relevant of de betrokkene wel of niet een antwoord geeft en of de betrokkene tot antwoorden verplicht is of niet. Deze bepaling leidt ertoe dat aan personen geen vragen mogen worden gesteld die slechts tot doel kunnen hebben een onderscheid te maken dat verboden is in de AWGB. In die zin verbiedt het voorstel voor een WBP gedragingen, die in de voorfase liggen van de gedragingen op het terrein van de AWGB. De AWGB verbiedt slechts het daadwerkelijk maken van onderscheid, terwijl de WBP gegevensverwerkingen verbiedt waarvan het resultaat gebruikt zou kunnen worden voor het maken van onderscheid. Deze vorm van gevaarzettend gedrag wordt op deze manier binnen het bereik van het recht gebracht.
De Registratiekamer stelt in haar advies dat een ongebreidelde verwerking van persoonsgegevens ook een negatieve uitwerking kan hebben op de vrije uitoefening van andere grondrechten, zoals de vrijheid van meningsuiting, politieke participatie en dergelijke. Daarbij zal dan met name gedacht moeten worden aan gevallen waarin een persoon of instantie over iemand zoveel gegevens met een zodanige lading heeft verzameld dat die persoon of instantie door het schermen met deze gegevens het gedrag van de betrokkene, waaronder ook het uitoefenen van grondrechten, kan beïnvloeden. De waarborgen die dit wetsvoorstel biedt, zullen er mede toe kunnen dienen dat dergelijke praktijken worden voorkomen.

5. Algemene normen en sectorale invulling

Het is mogelijk twee benaderingen te onderscheiden in de wettelijke bescherming van persoonsgegevens. De eerste is een benadering die uitgaat van verschillende sectoren of van bepaalde problemen in de samenleving. In Nederland vormden de problemen rond de volkstelling in 1971 de aanleiding tot regelgeving op dit gebied en in andere landen van de Unie waren andere problemen de aanleiding, zoals de kredietregistratie. In bepaalde sectoren was er al een lange traditie van een zorgvuldige omgang met persoonsgegevens, bijvoorbeeld met de medische gegevens van patiënten binnen de gezondheidszorg. Het is mogelijk om voor specifieke problemen te volstaan met sectorale wetgeving. In de Verenigde Staten heeft deze aanpak nog steeds de voorkeur. Er is echter ook een andere benadering mogelijk.
Deze is die van een overkoepelende regelgeving, waarbij de noodzakelij-

kerwijs algemene en vage normen vervolgens voor de verschillende sectoren moeten worden uitgewerkt. Dit heeft het voordeel dat er geen witte plekken in de bescherming van persoonsgegevens zijn. Het nadeel is een noodzakelijkerwijs hoog abstractieniveau van normstelling, dat in een aantal sectoren concretisering behoeft. Zolang deze er niet is, dient in het concrete geval de algemene norm nader te worden genterpreteerd. In Europa is deze weg gevolgd. Zo is het reeds genoemde Verdrag inzake gegevensbescherming tot stand gekomen. Dit verdrag bevat algemene normen gericht op een zorgvuldige omgang met persoonsgegevens. De algemene normen van het verdrag van de Raad van Europa zouden grotendeels zonder gevolg blijven als zij niet worden uitgewerkt in sectorale aanbevelingen. Om deze reden zijn er binnen de Raad van Europa aanbevelingen tot stand gekomen over de sociale zekerheid, de politieregisters, de direct marketing, telecommunicatie, de omgang met medische gegevens enz.[1]

In overeenstemming met het Verdrag gaat ook de WPR uit van een aantal overkoepelende normen. Deze algemene normen moeten geconcretiseerd worden en de WPR reikt hiervoor instrumenten aan, zoals de gedragscode, het meldingsformulier, het reglement en het Besluit genormeerde vrijstelling. De concretisering heeft daarnaast op een aantal terreinen plaatsgevonden op het niveau van de wet in formele zin. Voorbeelden hiervan zijn de Archiefwet, de Organisatiewet Sociale Verzekering, de Algemene Bijstandswet, de Wet gemeentelijke basis-administratie, de Wet geneeskundige behandelingsovereenkomst en de Wet politieregisters. Deze bijzondere wetten staan formeel-juridisch naast de WPR; ze bevinden zich echter wel binnen de grenzen die de normen in het Verdrag stellen.

De EG-richtlijn bescherming persoonsgegevens beweegt zich geheel binnen de randvoorwaarden van het Verdrag en geeft eveneens algemene normen voor het verwerken van gegevens. Artikel 5 van de richtlijn verplicht tot concretisering van de algemene normen van de richtlijn waar dit mogelijk en dienstig is. De richtlijn voorziet zelf in de mogelijkheid van een Europese gedragscode. Daarnaast is de bedoeling ook sectorale richtlijnen te ontwikkelen. Een eerste aanzet hiertoe is gegeven met het ontwerp van een richtlijn tot bescherming van persoonsgegevens op het terrein van de telecommunicatie[2].

Op alle niveaus, dat van de Raad van Europa, van de Europese Unie of van de Nederlandse wetgeving, geldt dat voor zover de algemene normen niet zijn geconcretiseerd in bijzondere regelgeving, de toepasselijkheid van de algemene normen in het concrete geval moet worden beoordeeld. Om normen per sector in formele wetgeving te concretiseren, kunnen twee modellen worden onderscheiden. Het ene is dat waarbij bepaalde regels in een bijzondere wet worden opgenomen, en waarbij de WBP als algemene wet van toepassing is op de gebieden die niet geregeld zijn. In dit model zijn in de betreffende sector in beginsel zowel de WBP als de bijzondere wet van toepassing. De andere is het model waarbij voor een sector een uitputtend (privacy-)regime is geschapen en waarbij in de wet wordt vermeld dat de toepasselijkheid van de algemene regels geheel wordt uitgesloten. In beide modellen moeten de regels, voor zover zij onder het communautaire recht vallen, in overeenstemming zijn met de richtlijn.

Voorbeelden van het eerste model zijn afdeling 5, titel 7, boek 7 BW over de geneeskundige behandelingsovereenkomst, de artikelen 42 en volgende van de Wet op de jeugdhulpverlening, de Kadasterwet, de Handelsregisterwet, alsmede de informatieparagrafen in de Organisatiewet Sociale Verzekering en de Algemene Bijstandswet. Voorbeelden van het tweede model zijn de Wet politieregisters, de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag, de Wet op de inlichtingen- en veiligheidsdiensten en de Wet gemeentelijke basisadministratie persoonsgegevens.

[1] Een aantal hiervan is opgenomen in de editie Schuurman & Jordens van de Wet persoonsregistraties, nr 199, tweede druk, blz. 340 e.v.

[2] Gemeenschappelijk standpunt van de Raad van 12 september 1996, nr 57/96, PbEG 24 oktober 1996, C 315/30.

Bijzondere vragen over het eerste model kunnen aan de orde komen bij de toepassing van wetten die verplichten tot verstrekking van persoonsgegevens na een afweging gericht op eerbiediging van de persoonlijke levenssfeer. Dit komt voor in artikel 10, tweede lid, van de Wet openbaarheid van bestuur en in artikel 15, eerste lid, onder a, van de Archiefwet. De bepalingen in het onderhavige wetsvoorstel zijn in ieder geval in zoverre van toepassing dat een verstrekking plaatsvindt op grond van artikel 8, onder c, daar deze noodzakelijk is wegens een verplichting krachtens een bijzondere wet. De bijzondere wet schrijft een afweging voor, voordat de verplichting tot verstrekking ontstaat. De regels van de WBP komen daarbij niet als direkt juridisch bindend normen in beeld. Wel zullen in de praktijk de normen van het wetsvoorstel indirekt hun reflexwerking hebben. Andere regels van de WBP, bij voorbeeld het toezicht door de Registratiekamer, zijn daarentegen ook op het terrein van dergelijke bijzondere wetten, rechtstreeks van kracht. Op de specifieke verhouding van het wetsvoorstel tot de WOB en de Archiefwet wordt in paragraaf 16 van het algemeen deel van deze memorie nog afzonderlijk ingegaan.
Voor het overige zullen veel bijzondere wetten op onderdelen concretiseringen bevatten, gericht op de sector die zij regelen. Het gaat daarbij formeel om leges speciales die derogeren aan de bepalingen van dit wetsvoorstel, maar materieel om een sectorale invulling die moet worden beoordeeld tegen de achtergrond van deze algemene normen, mede gelet op het feit ook deze bijzondere wetten aan de richtlijn zullen moeten voldoen voor zover zij geheel of ten dele communautair recht bestrijken. Zo is bijvoorbeeld in de artikelen 50g tot en met 50n van de Organisatiewet Sociale Verzekering en in de artikelen 84a, 84d tot en met 84l van de Algemene Bijstandswet een nauwkeurig regime van gegevensverwerking uitgewerkt. De onderdelen 161 en 162 van de Aanwijzingen voor de regelgeving schrijven voor dat bij nieuwe wetten telkens moet worden nagegaan hoe de informatievoorziening zal verlopen. Gaat het om persoonsgegevens dan zal telkens moeten worden bezien of de regels van de onderhavige wetsvoorstel toereikend zijn, dan wel of een nader uitgewerkt regime in de betreffende bijzondere wet moet worden gecreëerd. De rechtspraak van het Europese Hof van Justitie te Luxemburg over de verschillende begrippen is mede richtinggevend, ook wanneer daaraan nader inhoud is gegeven in sectorale wetgeving.
In artikel 2 WPR is ervan uitgegaan dat bij wetten van het tweede model de niet-toepasbaarheid van WPR steeds in deze laatste wet zelf is vastgelegd. Het onderhavige wetsvoorstel kiest voor een continuering van dit systeem. Deze keuze brengt met zich dat ook bij eventuele toekomstige wetgeving bevattende een uitputtend regime voor de bescherming van persoonsgegevens in een bepaalde sector, het niet van toepassing zijn van de WBP in deze laatste wet zelf wordt vermeld. Deze keuze voorkomt vragen over de verhouding tussen verschillende wettelijke systemen.

6. Geen aparte regeling voor de communautaire gegevensverwerking

De richtlijn verplicht de Lid-Staten van de Europese Unie om hun wetgeving in overeenstemming te brengen met de bepalingen van de richtlijn voor zover het gaat om het communautaire recht. Het betreft de gebieden van de z.g. eerste peiler, de onderwerpen die zijn geregeld in het EG-verdrag. De samenwerking tussen de landen van de Unie in de tweede en derde peiler, dat wil zeggen op de gebieden van het gemeenschappelijk buitenlands en veiligheidsbeleid, alsmede betreffende de samenwerking op het gebied van justitie en binnenlandse zaken, wordt niet bestreken door de richtlijn. Ingevolge artikel K.9 van het Unie-verdrag kan de Raad bij eenparigheid van stemmen beslissen dat het gemeenschapsrecht op een bepaald onderwerp van de samenwerking op het gebied van

Justitie en Binnenlandse Zaken van toepassing is. In artikel 3, tweede lid, onder eerste streepje, van de richtlijn is bepaald dat, ook in dat geval echter verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat – waaronder de economie van de Staat, wanneer deze verwerkingen in verband staan met vraagstukken van staatsveiligheid – en de activiteiten van de Staat op strafrechtelijk gebied, niet onder het bereik van de richtlijn vallen. Dit betekent onder meer dat de richtlijn geen betrekking heeft en ook niet zal hebben op de verwerkingen die zijn geregeld in de Wet politieregisters of de Wet op de inlichtingen- en veiligheidsdiensten.
Deze beperking hangt samen met de grondslag van de richtlijn, te weten de harmonisatie met het oog op de totstandkoming van de interne markt. De Lid-Staten blijven vrij de regelgeving voor het overige naar eigen inzicht in te richten, zij het binnen de grenzen van het Verdrag inzake gegevensbescherming voor zover zij dit hebben bekrachtigd.
De reikwijdte van het communautaire recht is inherent dynamisch. De organen van de Gemeenschap hebben de opdracht om het communautaire recht uit te breiden en aan te passen ter verwezenlijking van onder meer de interne markt. Deze activiteit leidt tot een voortdurende verandering van de scheidslijn tussen het nationale en het communautaire recht.
Het wetsvoorstel behelst de keuze af te zien van het onderscheid of een vorm van gegevensverwerking al dan niet onder het communautaire recht valt. Dit vermijdt onnodige vragen over de precieze reikwijdte van het zich voortdurend uitbreidende communautaire recht, alsmede vragen naar de rechtvaardiging waarom een bepaald rechtsgebied dat onder het communautaire recht valt, anders wordt geregeld dan een rechtsgebied waarbij dat (nog) niet het geval is. Dit laat onverlet dat de wet op onderdelen die niet onder het communautaire recht vallen, afwijkt van de algemene regels van de richtlijn wanneer daar inhoudelijk een bijzondere aanleiding toe bestaat. Dit laat ook onverlet voor bepaalde onderwerpen, ook al vallen die onder het communautaire recht, te kiezen voor een regeling in een aparte wet, bij voorbeeld de aanpassing van de Wet op de ondernemingsraden. Deze keuze is gemaakt wanneer het zinvol lijkt in een sectorale wet aparte bepalingen over gegevensverwerking op te nemen, waarbij dan uiteraard wel de grenzen van de richtlijn in acht moeten worden genomen.

7. Algemene karakterisering van het wetsvoorstel

Het wetsvoorstel bestaat uit onderdelen met elk een eigen karakter; de wet kan niet in zijn geheel worden ondergebracht onder één van de bestaande rechtsgebieden. Zij bevat delen die interacteren met het civiele recht, meer in het bijzonder met het leerstuk van de onrechtmatige daad; zij verleent subjectieve rechten aan degenen van wie persoonsgegevens worden verwerkt; zij is een organieke wet gericht op de vormgeving van een grondrecht en bevat voorts bestuursrechtelijke componenten in de sfeer van de uitvoering van de wet, het toezicht op de naleving en de sanctionering.
De eerste artikelen van het wetsvoorstel bevatten definities of bepalen de reikwijdte van de wet, zoals in veel wetten gebruikelijk is. De hierop volgende artikelen van hoofdstuk 2 bevatten inhoudelijke normen voor de verwerking van persoonsgegevens, waarvan de uitkomst vatbaar is voor volledige toetsing door de rechter. Deze bepalingen geven niet steeds eenduidige gedragsvoorschriften, maar schrijven afwegingen voor op grond van bepaalde criteria met inachtneming van bepaalde belangen. In deze laatste zin vormt het een nadere normering van wat voor de publieke sector uit hoofde van algemene beginselen van behoorlijk bestuur geldt, terwijl het in de private sector gaat om een precisering van wat private partijen uit hoofde van maatschappelijke zorgvuldigheid jegens elkaar zijn

verschuldigd. De verantwoordelijke blijft in rechte volledig aansprakelijk voor het resultaat van de afweging. Het kan dus voorkomen dat desgevraagd de rechter tot het oordeel komt dat de afweging tot een ander resultaat had behoren te leiden. Het gaat hier hoofdzakelijk om open normen die afhankelijk van omstandigheden en zich ontwikkelende opvattingen in rechtspraktijk en jurisprudentie zich verder moeten ontwikkelen.
Naar aanleiding van het advies van de Registratiekamer is de aanduiding van hoofdstuk 2 en de daarin vervatte paragrafen meer in overeenstemming gebracht met de tekst van de richtlijn, daarmee tot uitdrukking brengend dat het gaat om rechtstreeks juridisch bindende normen.
Het veel gehoorde verwijt dat de privacywetgeving onduidelijk is, gaat vaak terug op de impliciete veronderstelling dat deze wetgeving gedragsvoorschriften zou bevatten waaraan verantwoordelijken zich zonder meer zouden kunnen refereren als ware het strafbepalingen. Deze veronderstelling is evenwel onjuist. Verantwoordelijken in de publieke sector behouden de op hen rustende plicht tot behoorlijk bestuur. In de private sector hebben verantwoordelijken de plicht tot inachtneming van de maatschappelijke zorgvuldigheid jegens medeburgers. Deze algemene verplichtingen brengen een grote onzekerheid met zich mee. Zonder de nadere invulling via deze wetsvoorstel, zou deze onzekerheid bij de omgang met persoonsgegevens echter nog groter zijn.
Uiteindelijk gaat het bij het beoordelen of een bepaalde verwerking van persoonsgegevens toelaatbaar is of niet, niet alleen om deskundigheid op het gebied van privacyrecht maar ook om de eigen verantwoordelijkheid van de verantwoordelijke als onderdeel van het openbaar bestuur of als partij in het maatschappelijk verkeer dat wordt beheerst door het burgerlijk recht. Het onderhavig wetsvoorstel brengt evenwel de belangen die bij de verwerking van gegevens in het geding zijn en de criteria waaraan in concreto moet worden getoetst, uitdrukkelijk in beeld.
De artikelen van hoofdstuk 4 en 5 zijn enerzijds van meer formele aard, doch geven anderzijds invulling aan de eis van een behoorlijke verwerking tegenover de betrokkene door de openheid die jegens hem moet worden betracht. Zij beogen verder de openbaarheid van de gegevensverwerking tegenover de toezichthoudende instanties en een breder publiek. Ook ter uitvoering van deze bepalingen is soms een nadere afweging nodig. Zo kan van spontane informatieverstrekking aan de betrokkene worden afgezien wanneer dit van de verantwoordelijke een onevenredige inspanning zou vergen. De interpretatie van het begrip «onevenredig» vergt een afweging van belangen waarvan de uitkomst niet op voorhand vaststaat. Hetzelfde geldt voor de toepasselijkheid van de uitzonderingsgronden van artikel 43.
De artikelen 35 tot en met 42 geven mede uitvoering aan artikel 10, derde lid, van de Grondwet en verlenen concrete aanspraken aan de betrokkene. Het gaat om subjectieve rechten van de betrokkene die hij desgewenst voor de rechter geldend kan maken. Ziet de betrokkene af van gebruikmaking van deze rechten, dan vloeien daaruit ook geen verplichtingen voor de verantwoordelijke voort.
De regeling van de Registratiekamer in hoofdstuk 9, paragraaf 1, bevat bepalingen van bestuursrechtelijke aard. Zij bevestigen het bestaan van dit zelfstandig bestuursorgaan en leggen de taken en bevoegdheden daarvan opnieuw vast. De Kamer heeft een divers takenpakket dat in verschillende opzichten vergelijkbaar is met dat van de Nationale ombudsman, van de Commissie gelijke behandeling, van een inspectiedienst met toezichthoudende bevoegdheden en van een adviesorgaan van de regering.
Voor het overige bevat het wetsvoorstel bijzondere bepalingen over de aansprakelijkheid van de verantwoordelijke, die wat bewijslastverdeling betreft afwijkt van die van het gewone burgerlijk recht. Voorts bevat hoofdstuk 11 bepalingen over het internationale gegevensverkeer.

8. De verhouding tussen WBP en WPR

8.1 Algemeen

Het wetsvoorstel voor de WBP legt op een aantal punten andere accenten dan de WPR (WPR). Deels noodzaakt de richtlijn hiertoe, deels geven de uitgevoerde evaluaties van de WPR hiertoe aanleiding. Het gaat daarbij zowel om aanscherpingen, als om verruimingen. Samengevat zijn de belangrijkste wijzigingen:

– Het object van regelgeving is niet langer de «persoonsregistratie», maar de «verwerking van persoonsgegevens» in al haar stadia.
– Het begrip «houder» (van een persoonsregistratie) wordt vervangen door «verantwoordelijke» (voor de gegevensverwerking). Bepalend voor wie verantwoordelijke is, is primair de vraag wie juridisch bevoegd is om doel en middelen van de gegevensverwerking vast te stellen. Door aan te sluiten bij de bestaande bevoegdhedenstructuur in publiek- en privaatrecht wordt beoogd de blijkens de evaluaties bestaande verwarring omtrent het houderschapsbegrip weg te nemen. De formele bevoegdheden zijn duidelijker en dienen daarom het aanknopingspunt te zijn in plaats van de feitelijke machtsverhoudingen met betrekking tot de te verwerken persoonsgegevens. Deze laatste zijn voor de betrokkene minder transparant. Voor zover echter in een concreet geval niet duidelijk zou zijn wie bevoegd is en meerdere personen of instanties betrokken zijn bij de gegevensverwerking en in verband met de aard van die betrokkenheid in aanmerking komen om als verantwoordelijke te worden aangeduid, dient aan de hand van algemeen in het maatschappelijk verkeer aanvaarde maatstaven te worden bezien aan wie een bepaalde gegevensverwerking moet worden toegerekend.
– Het wetsvoorstel is in beperkte mate van toepassing op pers, radio en televisie. Krachtens de WPR gold voor deze sector een algehele uitzondering. Ook zal de WBP van toepassing zijn, voor zover de desbetreffende wetten geen bijzondere bepalingen bevatten, op openbare registers (bijv. het kadaster en het handelsregister) en persoonsgegevens die vallen onder het regime van de Archiefwet.
– De materiële eisen waaraan elke vorm van gegevensverwerking moet voldoen, krijgen een andere systematiek. Deels gaat het om aanscherpingen, deels gaat het om versoepelingen. Net als in de WPR gaat het om een abstract normenkader dat door middel van sectorale wetgeving of zelfregulering (m.n. gedragscodes) zijn verdere invulling zal moeten krijgen.
– Het regime inzake gevoelige gegevens is enigszins aangescherpt. Achtergrond is de algemene eis van de richtlijn inhoudende dat verwerking van gevoelige gegevens alleen is toegestaan in een aantal concreet omschreven gevallen en voorhet overige voor zover noodzakelijk ten behoeve van «een zwaarwegend algemeen belang».
– De informatieverplichtingen van de houder tegenover de betrokkene – d.w.z. degene over wie de gegevens worden verwerkt – worden uitgebreid, zij het dat belangrijke uitzonderingen mogelijk blijven. Het bestanddeel «redelijkerwijs kan weten» van artikel 28 WPR valt weg. De verantwoordelijke dient de betrokkene «op de hoogte te stellen», behoudens in een limitatief omschreven aantal uitzonderingsgevallen.
– In aanvulling op de reeds bestaande rechten wordt aan degene van wie de gegevens worden verwerkt, het recht van verzet toegekend, wanneer een gerechtvaardigd individueel belang kan worden aangetoond. In geval van verwerkingen in de sector van direct marketing is dit recht absoluut in die zin dat een gerechtvaardigd individueel belang in geval van verzet van rechtswege wordt aangenomen.
– In het wetsvoorstel is sprake van een gedifferentieerd systeem van

rechtsbescherming. Tegen een beslissing van een bestuursorgaan op verzoeken strekkende tot het honoreren van door de wet toegekende rechten, staat op grond van de Algemene wet bestuursrecht (Awb) bezwaar en beroep open.
- De bestaande risico-aansprakelijkheid voor onrechtmatige gegevensverwerking wordt afgezwakt. De verantwoordelijke is niet aansprakelijk indien hij kan aantonen dat hem aangaande de betreffende onrechtmatigheid geen verwijt treft.
- Het bestaande onderscheid tussen de publieke en private sector komt ingevolge het wetsvoorstel te vervallen. De reglementsplicht voor de publieke sector wordt daarmee afgeschaft. De meldingsplicht wordt verzacht: handmatige verwerkingen behoeven in beginsel niet te worden gemeld, de melding omvat minder gegevens en het aantal vrijstellingen zal ten opzichte van de WPR worden uitgebreid (nader te regelen bij algemene maatregel van bestuur).
- Voor zover de houder niet wordt vrijgesteld van zijn verplichting om verwerkingen te melden bij de Registratiekamer, wordt een alternatief voor deze meldingsplicht gecreëerd: per organisatie of per branche kan een toezichthouder worden aangesteld die in dat geval in aanvulling op de Registratiekamer bepaalde toezichthoudende bevoegdheden kan uitoefenen.
- De bevoegdheden van de Registratiekamer worden uitgebreid. Het betreft onder de meer de bevoegdheid om voorafgaand onderzoek te doen naar verwerkingen met bijzondere risico's, de bevoegdheid om bestuursdwang toe te passen en de bevoegdheid om bestuurlijke boeten op te leggen. Daar staat tegenover dat de rechtsbescherming tegen handelingen van de Registratiekamer wordt uitgebreid. Tegen beslissingen van de kamer zal op grond van de Awb bezwaar en beroep openstaan.

Op een aantal van deze verschillen wordt hieronder ingegaan.

8.2 Een andere systematiek

Een aantal verschillen tussen WBP en WPR hangt samen met het feit dat de richtlijn (en dus ook de nieuwe wet) een andere systematiek kent dan de WPR. De WPR neemt als object van regelgeving de persoonsregistratie: een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens. Persoonsgegevens die (nog) geen deel uitmaken van een samenhangend groter geheel, vallen dus niet onder de normering. Pas bij de nadere omschrijving in welke gevallen sprake is van een groter, meer omvattend geheel, komt het onderscheid aan de orde tussen geautomatiseerde opslag van gegevens en handmatige opslag van gegevens. Bij opslag langs geautomatiseerde weg wordt van rechtswege aangenomen dat een doeltreffende raadpleging mogelijk is. Bij handmatige verwerking wordt het wetsvoorstel pas van toepassing wanneer er maatregelen zijn getroffen om de vastgelegde gegevens voor raadpleging toegankelijk te maken. In beide gevallen is evenwel voor de toepasselijkheid van het wetsvoorstel noodzakelijk dat de persoonsgegevens deel uitmaken van een groter geheel: de persoonsregistratie.
Voor persoonsgegevens op deelterreinen bevatten bijzondere wetten in een aantal gevallen een aanvullende regeling, ongeacht de vraag of deze persoonsgegevens deel uitmaken van een persoonsregistratie. Bijvoorbeeld voor persoonsgegevens in dossiers introduceerde de Wet geneeskundige behandelingsovereenkomst in artikel 7:454 BW een aanvullende regeling. De artikelen 42 tot en met 45 van de Wet op de jeugdhulpverlening bevatten vergelijkbare bepalingen. Ook de Wet openbaarheid van bestuur bevat een aanvullende regeling voor persoonsgegevens uit overheidsdocumenten.
De WPR stelt voorts regels omtrent de aanleg en het gebruik van

persoonsregistraties. De invulling van nadere regels gebeurt aan de hand van de beginselen van doelbinding en verenigbaar gebruik. Deze beginselen zijn neergelegd in het Verdrag inzake gegevensbescherming. Wat betreft het beginsel van doelbinding verbindt de WPR het doel van een persoonsregistratie met het belang van de verantwoordelijke. De wet laat slechts toe dat het belang van de verantwoordelijke, indien dit redelijkerwijs aanleiding daartoe geeft, de grondslag kan zijn voor de aanleg van een persoonsregistratie.
Wat betreft het beginsel van verenigbaar gebruik kunnen binnen de organisatie van de verantwoordelijke de gegevens ook worden gebruikt voor andere doeleinden, althans voor zover deze verenigbaar zijn met het oorspronkelijk doel. Worden de gegevens daarentegen buiten de organisatie van de verantwoordelijke gebruikt, dan gelden strakkere normen: verstrekking aan derden is in beginsel slechts toegestaan voor zover dit voortvloeit uit het doel van de registratie. Voor de overheid geldt op grond van de WPR een deels ander regime. Zo geldt dat binnen zekere randvoorwaarden op verzoek ook gegevens mogen worden verstrekt aan andere overheidsorganen, voor zover zij deze gegevens nodig hebben voor de uitvoering van hun taak.
Met name ten aanzien van de bovengenoemde punten is in de WBP een andere inhoud gegeven. In het wetsvoorstel is het object van regelgeving de verwerking van persoonsgegevens. De verwerking van persoonsgegevens is gedefinieerd als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés. Het begrip persoonsregistratie komt niet meer voor in de WBP. De regelgeving met betrekking tot dit begrip speelt slechts indirect nog een rol voor zover het gaat om louter handmatige verwerkingen. Het wetsvoorstel gebruikt daarvoor het begrip «bestand». De zelfstandige betekenis van dit begrip zal met de ontwikkeling van informatietechnologie naar verwachting afnemen. Daar de binding met de persoonsregistratie in beginsel is losgelaten, is het ook mogelijk persoonsgegevens in de fase van het verzamelen onder de werking van het wetsvoorstel te brengen.
Het beginsel van verenigbaar gebruik krijgt een ruimere strekking dan onder de WPR. Het onderscheid tussen verwerking binnen en buiten de organisatie van de verantwoordelijke komt in dat verband grotendeels te vervallen. Voor verstrekking aan derden is niet meer noodzakelijk dat dit voortvloeit uit het doel van de registratie. Het is dan ook niet meer relevant aan welke derde gegevens worden verstrekt, maar wie de gegevens, binnen of buiten de organisatie van de verantwoordelijke, verwerkt. In de WBP komt het begrip «ontvanger» voor. Met dit begrip wordt degene aan wie de gegevens worden verstrekt bedoeld. Het begrip speelt een rol in de informatieplicht van de verantwoordelijke ten opzichte van de betrokkene en in de informatie die de verantwoordelijke bij de aanmelding bij de toezichthouder moet verstrekken. Daarmee verliezen vragen omtrent het intern of extern gebruik bij grote concerns grotendeels hun relevantie. Dit sluit aan bij de maatschappelijke ontwikkeling van een toenemende schaalvergroting in het bedrijfsleven, gepaard gaande met produktdiversificatie.

8.3. Transparantie

Om de betrokkene effectief in staat te stellen zijn rechten te verwerkelijken, moet hij van de verwerking van hem betreffende gegevens op de hoogte zijn. De bedreiging van de persoonlijke levenssfeer in de informatiemaatschappij bestaat echter juist uit de vele mogelijkheden om persoonsgegevens buiten medeweten van de betrokkene te verwerken. Het wetsvoorstel bevat daarom inzake de informatieverstrekking aan de betrokkene een aangescherpt regime gericht op de transparantie van gegevensverwerking. De verplichtingen van de verantwoordelijke om de

betrokkene op de hoogte te stellen van de verwerking zijn aangescherpt. De aanscherping heeft zowel op het geval dat gegevens bij hem worden vergaard, als op het geval van secundair gebruik van gegevens betrekking. De verantwoordelijke mocht onder de werking van artikel 28 WPR er nog vanuit gaan dat informatie aan de betrokkene achterwege mocht blijven wanneer de betrokkene redelijkerwijs kan weten van de opname in een persoonsregistratie. Onder de werking van het wetsvoorstel dient hij de betrokkene op de hoogte te stellen, tenzij deze al daadwerkelijk over de desbetreffende informatie beschikt. Op de betrokkene rust geen onderzoeksplicht. Zie verder de toelichting op de artikelen 33 en 34.
Ter bevordering van de transparantie wordt voorts in de WBP voorgeschreven dat wanneer betrokkenen niet worden genformeerd, bijvoorbeeld omdat dat een onevenredige inspanning zou vergen, de herkomst van de gegevens moet worden bijgehouden. Te denken valt aan gevallen waarin gegevens buiten de betrokkene om zijn verkregen met het oog op direct marketing of voor het verrichten van sociaal-wetenschappelijk onderzoek. Vanuit de gedachte van transparantie bestaat het voornemen geen vrijstellingen op de aanmeldingsprocedure op te nemen voor gegevensverwerkingen die geheel of ten dele het gevolg zijn van onopgemerkte waarneming van de betrokkene. Een verdere aanscherping van de transparantie ligt voorts besloten in de eis van artikel 30, derde lid. In dit artikel wordt vermeld dat ook omtrent gegevensverwerkingen die van aanmelding zijn vrijgesteld de verantwoordelijke desgevraagd aan een ieder informatie moet verstrekken, vergelijkbaar met de informatie die in het kader van de aanmelding aan de Registratiekamer moet worden verstrekt.
Tegenover de aanscherping van de informatieverplichting van de verantwoordelijke jegens de betrokkene staan vereenvoudigingen met betrekking tot de melding van verwerkingen aan de Registratiekamer. Op grond van de WPR bestaat een reglementsplicht voor – kort gezegd – de publieke en semi-publieke sector en een meldingsverplichting voor de private sector, behoudens de gevallen die zijn vrijgesteld ingevolge het Besluit genormeerde vrijstelling. Uit de evaluaties blijkt dat dit systeem niet goed heeft gefunctioneerd. Aannemelijk is dat de genoemde verplichtingen in aanzienlijke mate zijn genegeerd, dan wel slechts gediend hebben als papieren formaliteit. Het bestand van aanmeldingen en reglementen bij de Registratiekamer schiet kwalitatief gezien ernstig tekort. Ook is er veel kritiek op het Besluit genormeerde vrijstelling: zij heeft naar uit de evaluaties blijkt tot veel onduidelijkheid en onzekerheid in de uitvoeringspraktijk geleid.
Artikel 18 van de richtlijn laat de lidstaten niet de ruimte om volledig af te zien van een systeem van meldingsverplichtingen. Een dergelijk vergaande stap gaat ook te ver. Bij verwerkingen die afwijken van het normale patroon of uit privacyoogpunt een gevoelig karakter dragen, is er reden de meldingsverplichting te handhaven om de Registratiekamer en andere toezichthouders in staat te stellen op adequate wijze hun taak uit te voeren. Niettemin zijn er gezien ook de evaluaties enige vereenvoudigingen aangebracht.
Een eerste belangrijke verandering is dat de reglementsplicht voor de publieke en semi-publieke sector wordt geschrapt. Over de gehele linie geldt in beginsel een meldingsverplichting. Dit is te beschouwen als een vereenvoudiging. Het als problematisch ervaren onderscheid tussen publieke en private sector – neergelegd in het op artikel 17 WPR gebaseerde Afbakeningsbesluit – vervalt.
Een tweede verandering is dat handmatige verwerkingen in beginsel niet hoeven te worden gemeld. Aan deze beperking ligt de gedachte ten grondslag dat handmatige vormen van gegevensverwerking in de regel minder bedreigend zijn voor de persoonlijke levenssfeer. Voorts is van belang dat in de melding minder gegevens hoeven te worden opgenomen

dan onder de WPR het geval is. Ook in dat opzicht is sprake van een zekere vereenvoudiging.
In het verlengde van de WPR geeft de richtlijn in artikel 20, tweede lid, aan de lidstaten de mogelijkheid om gegevensverwerkingen van de meldingsplicht vrij te stellen. Vrijstelling is krachtens deze bepaling alleen mogelijk voor zover een «inbreuk op de rechten en vrijheden van de betrokkenen onwaarschijnlijk is». Dit criterium is minder stringent dan het wellicht op het eerste gezicht lijkt. Tijdens de totstandkoming van de richtlijn is de bedoeling uitgesproken dat een groot deel van de vele vormen van gegevensverwerking zal worden vrijgesteld. Daarbij moet vooral worden gedacht aan verwerkingen die standaard zijn en waarvan algemeen bekend is dat zij plaatsvinden. Het ligt in de rede dat de verwerkingen die thans onder de WPR zijn vrijgesteld, straks opnieuw van de meldingsplicht zullen worden uitgezonderd. In dat opzicht zal de bestaande situatie derhalve worden gecontinueerd. Bij de totstandkoming van de algemene maatregel van bestuur die het Besluit genormeerde vrijstelling gaat vervangen, zal voorts nader worden bezien in hoeverre het aantal vrijstellingen nog verder kan worden uitgebreid.
Ten slotte is van belang dat de richtlijn de mogelijkheid biedt om per organisatie of per branche een functionaris voor de gegevensbescherming aan te stellen. Van deze mogelijkheid wordt in het wetsvoorstel gebruik gemaakt. De taak van deze functionaris is om op onafhankelijke wijze toezicht uit te oefenen op de toepassing van de op grond van de richtlijn geldende wettelijke voorschriften binnen de betreffende organisatie of branche. De aanstelling van een functionaris voor de gegevensbescherming betekent dat de melding in beginsel bij hem kan plaatsvinden en niet bij de Registratiekamer. Voor de verantwoordelijke bestaat in dat geval de mogelijkheid tussen beide opties te kiezen.

9. Het systeem van materiële normen

9.1. Algemene beginselen van gegevensverwerking

De regels die betrekking hebben op de toelaatbaarheid en de kwaliteit van de gegevensverwerking zijn te vinden in de artikelen van hoofdstuk II van het wetsvoorstel. Er is een algemeen basisprincipe voor de gegevensverwerking neergelegd in artikel 6, eerste lid, onder a, van de richtlijn dat bepaalt dat gegevens eerlijk en rechtmatig moeten worden verwerkt. Dit geldt voor alle fasen van het proces van gegevensverwerking. Het begrip «eerlijk» – een vertaling van het Engelse «fair» – komt in het Nederlandse recht nauwelijks voor. Teneinde beter aansluiting te vinden bij het overige recht is dit beginsel in het wetsvoorstel anders verwoord: in artikel 6 is bepaald dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Met het begrip «zorgvuldigheid» wordt enerzijds aangesloten bij de zorgvuldigheidnorm uit artikel 6:162 BW, anderzijds bij het zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur. Dit interpretatie van dit begrip in het kader van de verwerking van persoonsgegevens vindt uiteraard weer zijn nadere inkleuring door de normen van het wetsvoorstel.
Dit basisbegrip wordt verder uitgewerkt in diverse andere bepalingen. Indien het proces van gegevensverwerking chronologisch wordt benaderd stuit de verantwoordelijke bij het verzamelen van gegevens eerst op artikel 7. Hierin wordt bepaald dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen. Dit houdt in dat geen gegevens mogen worden verzamelen zonder een precies doel. Dit is immers medebepalend is voor een eventuele beoordeling van de rechtmatigheid van de gegevensverwerking. De omschrijving van het doel zal hetzij blijken uit de melding van de verwerking die de verantwoordelijke op grond van de wet uit

hoofde van de wet verplicht is te verrichten – zie artikel 28, eerste lid, onder b, van het wetsvoorstel – hetzij uit de algemene maatregel van bestuur waarin precies zal worden geregeld welke verwerkingen van de meldingsverplichting worden vrijgesteld.
Het derde element van artikel 7 – gegevens worden verkregen voor «gerechtvaardigde doeleinden» – vindt zijn nadere uitwerking in artikel 8 van het wetsvoorstel. In deze bepaling worden limitatief de rechtvaardigingsgrondslagen opgesomd voor de verwerking van persoonsgegevens. Ze zijn alternatief: elke gegevensverwerking of categorie van gegevensverwerkingen dient herleidbaar te zijn tot ten minste één van de in artikel 8 opgesomde gronden. Voor gevoelige gegevens geldt daarenboven het stringentere regime van paragraaf 2 van het onderhavige hoofdstuk. De rechtmatigheid van de verwerking van gevoelige gegevens dient dus te worden beoordeeld aan de hand van artikel 8 in samenhang met de artikelen 16 tot en met 23.
Indien eenmaal vaststaat dat de gegevensverwerking toelaatbaar is, zijn er vervolgens eisen met betrekking tot de wijze waarop de gegevens mogen worden gebruikt. Gegevens mogen niet worden verwerkt op een wijze die «onverenigbaar» is met de doeleinden waarvoor zij zijn verkregen. Gegevens mogen ook voor andere doeleinden worden gebruikt dan waarvoor zij zijn verkregen, doch die andere doeleinden mogen met het oorspronkelijke doel «niet onverenigbaar» zijn.
De richtlijn geeft over de precieze reikwijdte van dit begrip geen uitsluitsel. Wel maakt zij duidelijk dat inieder geval de verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden niet als onverenigbaar wordt beschouwd, mits «passende garanties» worden geboden. Uit dit op een bepaalde sector toegesneden voorschrift zijn tot op zekere hoogte algemene criteria te destilleren die voor het bepalen van de verenigbaarheid van belang zijn. Zo gaat het bij verwerking van gegevens voor wetenschappelijke doeleinden niet om gebruik waarvan de betrokkene nog enige gevolgen zal ondervinden. Dit ligt anders indien gegevens worden gebruikt voor de vaststelling van het recht op uitkering of voor de beslissing of de betrokkenen voor een levensverzekering in aanmerking komt. De ingrijpendheid van de gevolgen van de betrokkene is derhalve een factor die van belang is voor de verenigbaarheidstoets.
Voorts laat de bepaling inzake wetenschappelijk onderzoek zien dat verwerking van gegevens voor een bepaald doel eerder verenigbaar is indien met het oog op het belang van de betrokkene passende garanties worden geboden. Duidelijk is dat gebruik van gegevens voor een ander doel eerder niet onverenigbaar is, indien de betrokkene over dat gebruik wordt geïnformeerd of – een stap verder – hem om toestemming voor zodanig gebruik wordt gevraagd. Verder ligt het voor de hand om aan te nemen dat de aard van de gegevens een rol kan spelen, alsmede de wijze waarop de gegevens zijn verkregen.
Om de verantwoordelijke een handvat te bieden bij de toepassing van de norm van verenigbaar gebruik is in artikel 9 van het wetsvoorstel uitdrukkelijk een aantal van de hiervoor genoemde factoren genoemd waar de verantwoordelijke bij zijn afweging in elk geval rekening dient te houden. Het betreft hier geen limitatieve opsomming: ook andere factoren dan die in de wet genoemd kunnen een rol spelen.
Vervolgens zijn er enkele aanvullende voorwaarden. Deze hebben in de eerste plaats betrekking hebben op de inhoudelijke kwaliteit van de gegevens. Deze moeten blijkens artikel 11 toereikend, ter zake dienend, niet bovenmatig en nauwkeurig zijn. Voorts dienen de gegevens te worden beveiligd. Verwezen wordt naar de artikelen 12, 13 en 14.
Tot slot bepaalt artikel 10 dat persoonsgegevens niet langer mogen worden bewaard dan nodig is voor de verwezenlijking van de doeleinden waarvoor de gegevens zijn verzameld of vervolgens zijn verwerkt. Een soepeler norm geldt krachtens hetzelfde artikel voor persoonsgegevens

die worden bewaard voor historische, statistische of wetenschappelijke doeleinden.
Resumerend kunnen – de chronologie van het proces van gegevensverwerking zoveel mogelijk volgend – vanuit het gezichtspunt van de verantwoordelijke achtereenvolgens de volgende stappen worden onderscheiden:

1. Algemeen: gegevensverwerking in overeenstemming met de wet en behoorlijk en zorgvuldig (artikel 6).
2. Verzameling voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7).
3. Grondslag rechtmatigheid gegevensverwerking (artikel 8: is uitwerking van «gerechtvaardigde doeleinden» als bedoeld in artikel 7).
4. Verdere verwerking niet onverenigbaar met doeleinden van verkrijging (artikel 9).
5. Kwaliteit gegevens: toereikend, relevant, niet bovenmatig, nauwkeurig (artikel 11).
6. Beveiliging (artikelen 12, 13 en 14)
7. Bewaring: niet langer dan noodzakelijk voor verwerkingsdoeleinden (artikel 10).

Bij de toepassing van artikel 8 (zie punt 3) geldt steeds in aanvulling op artikel 8 voor gevoelige gegevens op grond van paragraaf 2 van hoofdstuk 2 een verscherpt regime.

9.2. Verwerking van gevoelige gegevens

Artikel 8 van de richtlijn bevat bijzondere voorschriften omtrent de verwerking van gevoelige gegevens. Zij vormen een aanscherping van het zojuist geschetste algemene regime. De voorwaarden gelden krachtens de richtlijn uitdrukkelijk cumulatief. De verwerking van gevoelige gegevens dient niet alleen in overeenstemming te zijn met artikel 8 van de richtlijn, maar dient daarnaast ook steeds aan de eisen van artikel 6 en 7 te voldoen. Deze gelaagde systematiek van de richtlijn vindt zijn vertaling in het wetsvoorstel. Met betrekking tot gevoelige gegevens blijven naast de bijzondere voorschriften van artikel 16 e.v. de algemene beginselen van gegevensverwerking onverkort van toepassing. Indien het verbod om gevoelige gegevens te verwerken als bedoeld in artikel 16 wordt opgeheven door een van de daarop volgende bepalingen (artt. 17–23), zal de gegevensverwerking vervolgens moeten worden getoetst aan de algemene beginselen zoals vastgelegd in de artikelen 6 tot en met 15.
Achtergrond van het verscherpte regime is – zo blijkt ook uit overweging 33 van de richtlijn – dat bepaalde gegevens vanwege hun aard een inbreuk op de fundamentele vrijheden kunnen maken, meer in het bijzonder op de persoonlijke levenssfeer. Om welke gegevens het gaat blijkt uit artikel 8, eerste lid, van de richtlijn: gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijkt, alsmede gegevens die de gezondheid of het seksuele leven betreffen. Uit artikel 8, vijfde lid, blijkt voorts impliciet dat strafrechtelijke en aanverwante gegevens tot deze categorie moeten worden gerekend.
Artikel 8 van de richtlijn is in het wetsvoorstel geïmplementeerd in de artikelen 16 tot en met 23. Artikel 16 vormt de basisbepaling. Zij is conform de richtlijn geconstrueerd als een verbod om de in dat artikel aangeduide gegevens te verwerken, tenzij aan bepaalde voorwaarden is voldaan. In artikel 23, eerste lid, onder e, wordt voorts in algemene zin aangegeven om welke voorwaarden het gaat. Verwerking is slechts toegestaan indien dat noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen ter bescherming van de persoonlijke levenssfeer worden geboden en dat bij wet is bepaald of de Registratiekamer daarmee bij beschikking heeft ingestemd.
De artikelen 17 tot en met 22 bevatten vervolgens volgens het geschetste

stramien per categorie gevoelige gegevens de regeling van diverse situaties waarin een ontheffing geldt van het verbod als bedoeld in artikel 16. De artikelen betreffen concrete situaties en sectoren in de samenleving alsmede de verschillende soorten gevoelige gegevens. Specifiek wordt aangegeven wanneer en onder welke voorwaarden een ontheffing van het verbod geldt. In deze concrete gevallen heeft de wetgever reeds een afweging gemaakt van het belang van de verwerking van gegevens enerzijds en het belang van de bescherming van de persoonlijke levenssfeer van de betrokkene anderzijds. Zoals gezegd laat dit onverlet dat steeds ook voldaan zal moeten worden aan de algemene beginselen van gegevensverwerking zoals geregeld in het wetsvoorstel.
Een soortgelijk karakter hebben eveneens de voorschriften, bedoeld in artikel 23. Laatstgenoemde voorschriften doelen daarentegen niet op specifieke situaties maar hebben een ruimer bereik en hebben betrekking op alle sectoren van de samenleving en zien op alle soorten gevoelige gegevens tegelijkertijd. Doordat ze van meer algemene aard zijn, ontkomen ze er niet aan alsnog een nadere belangenafweging voor te schrijven, zij het dat de afwegingscriteria in elk onderdeel verschillen. Artikel 23 bevat een aantal afwegingscriteria voor de gevallen die niet in de artikelen 17 tot en met 22 zijn behandeld. In die zin moet artikel 23 worden beschouwd als een algemene restbepaling. Omdat het onmogelijk is een specifieke regeling te geven voor alle mogelijke gevallen waarin een uitzondering op het verwerkingsverbod gerechtvaardigd is, zijn dergelijke aanvullende bepalingen noodzakelijk.
De vraag is hoe de verhouding is tussen de specifieke artikelen 17 tot en met 22 enerzijds en de algemene bepaling van artikel 23 anderzijds. Met name kan de vraag rijzen in hoeverre een ontheffing van het verwerkingsverbod dat niet kan worden gebaseerd op een van de specifieke bepalingen, alsnog zijn grondslag kan vinden in artikel 23. Deze vraag kan niet voor alle gevallen gelijkluidend worden beantwoord. Met name dient inzake de strekking van de artikelen 17 tot en met 22 acht te worden geslagen op bepalingen die ten opzichte van artikel 23 uitputtend zijn bedoeld, dan wel een verbiedend karakter dragen. Dit laatste is afhankelijk van de terminologie die in de bepaling wordt gehanteerd.
De eerste categorie wordt gevormd door de bepalingen met een uitputtend of verbiedend karakter. Dit wordt met name tot uitdrukking gebracht door de woorden «worden geen persoonsgegevens aan derden verstrekt», «is slechts niet van toepassing» of woorden met een dergelijke strekking. Het komt bijvoorbeeld voor in de artikelen 17, derde lid, 18, eerste en tweede lid, 19, tweede lid en 20, tweede lid. Het verbod, opgenomen in artikel 17, derde lid, impliceert bij voorbeeld het volgende. Indien een persoon geen toestemming geeft voor het verwerken van hem betreffende gegevens omtrent godsdienst met het oog op zijn geestelijke verzorging, zal het verstrekken van deze gegevens aan derden niet op artikel 23 kunnen worden gebaseerd. Het verbiedend karakter van artikel 17, derde lid, juncto eerste lid, onder c, staat er aan in de weg dat buiten dit voorschrift om gegevens worden verstrekt. Voor een hernieuwde afweging op grond van artikel 23 is dan, gegeven dit verbod, geen plaats meer. Artikel 21 is daarentegen niet uitputtend bedoeld. Dit artikel staat er niet aan in de weg dat een ontheffing van het verbod om gezondheidsgegevens te verwerken kan worden gebaseerd op artikel 23, bijvoorbeeld indien sprake is van uitdrukkelijke toestemming van de betrokkene.
Aldus kan de verhouding tussen de diverse bepalingen als volgt worden samengevat. Het karakter van de specifieke voorschriften, bedoeld in de artikelen 17 tot en met 22 brengt met zich dat indien een ontheffing om gevoelige gegevens te verwerken kan worden gebaseerd op één van deze artikelen, ter zake niet meer getoetst hoeft te worden aan artikel 23. Indien een ontheffing daarentegen niet kan worden gebaseerd op de artikelen 17 tot en met 22, dient wel te worden bezien of deze wellicht wel op artikel 23 kan worden gebaseerd. Daarbij dient bij de toepassing van de artikelen 17

tot en met 22 per afzonderlijke bepaling te worden bezien of zij een uitputtend of verbiedend karakter dragen. Het een en ander is tot uitdrukking gebracht met het woord «onverminderd» in de aanhef van artikel 23, eerste lid. Dit brengt immers met zich dat zowel de uitputtende en verbiedende bepalingen alsook de overige bepalingen van de artikelen 17 tot en met 22 onverkort van toepassing zijn.
Artikel 23 bevat een aantal gronden die het verwerken van gevoelige gegevens aanvullend veroorloven, voor zover de voorafgaande bepalingen geen verbod bevatten. Het artikel zelf bevat geen bepaling die als een verbod is geformuleerd. Dit houdt in dat, mocht bij voorbeeld de betrokkene gelet op artikel 23, eerste lid, onder a, voor een verwerking geen uitdrukkelijke toestemming geven, het karakter van dit voorschrift er niet aan in de weg staat dat een ontheffing van het algemene verwerkingsverbod van artikel 16 desondanks kan worden gegrond op bij voorbeeld artikel 23, eerste lid, onder e. Indien de verwerking in een bepaalde situatie noodzakelijk is met het oog op een zwaarwegend algemeen belang, dan kan de Registratiekamer niettemin een ontheffing verlenen van het verwerkingsverbod, ook al is niet voldaan onder de voorwaarde onder a. Dezelfde situatie doet zich voor als de betrokkene op grond van artikel 23, eerste lid, onder a, zijn toestemming intrekt. Ook dan kan artikel 23, eerste lid, onder e, een toereikende basis zijn.

9.3. Openbare registers

De materiële normen zijn ook van toepassing op openbare registers. Er zijn registers waarvan de openbaarheid is voorgeschreven bij wet, zoals de het handelsregister, het voogdijregister, het huwelijksgoederenregister, het openbaar register voor registergoederen, de kadastrale registratie e.d. Daarnaast zijn er registers die feitelijk openbaar zijn, zoals telefoonboeken, almanakken e.d. Bij de eerste heeft de wetgever bepaald dat de verantwoordelijke zonder toets van de motieven van de verzoeker, gegevens dient te verstrekken. Bij de tweede categorie vloeit de openbaarheid voort uit de aard van de publikatie en hebben betrokkenen in de regel gelegenheid bezwaar te maken tegen openbaarmaking van hun gegevens. Of de vorm van gegevensverwerking die bestaat uit de verstrekking aan een verzoeker, is gerechtvaardigd, kan dan niet meer in het individuele geval aan de wet worden getoetst. De bepalingen van de wet houden evenwel hun werking met betrekking tot andere onderdelen van de gegevensverwerking. Niet alleen normeren zij de inhoud van de registers, doch ook de wijze van verstrekking. Op dit laatste gaan wij nader in.
Wanneer een openbaar register tot doel heeft informatie te geven, is bij verstrekking van persoonsgegevens het achterliggende doel van het register medebepalend voor de wijze van verstrekking. Artikel 13 legt op de verantwoordelijke de plicht om bij voorbeeld bij ontsluiting van een openbaar register via Internet of CD-ROM, de gegevens adequaat te beveiligen tegen enige vorm van onrechtmatige verwerking. Dit omvat mede een vorm van verstrekking die inherent zou zijn aan een dergelijk onverenigbaar gebruik. Zie ook de artikelsgewijze toelichting op dat artikel.
Zo is het telefoonboek in digitale vorm, bij voorbeeld op CD-ROM, voor het publiek beschikbaar. Daarop kan op personen worden gezocht. Er zijn evenwel beveiligingen aangebracht tegen het zoeken op telefoonnummer. Zo kunnen verder uit de kadastrale registratie gegevens worden verstrekt omtrent de eigenaar van een bepaald erf. Het zou evenwel onverenigbaar zijn met het doel van deze registratie wanneer een eventuele, digitaal ter beschikking staande versie van de registratie, tot gevolg zou hebben dat ieder zonder bijzondere inspanning daarop zoekfuncties zou kunnen loslaten die bij voorbeeld een lijst zouden opleveren van alle personen die een pand in eigendom hebben boven een bepaalde waarde. Een laatste voorbeeld is het handelsregister. Het zou niet verenigbaar zijn met het

doel van dit register wanneer de gegevens beschikbaar zouden worden gesteld in zodanige vorm dat bij voorbeeld ten aanzien van bepaalde personen zou kunnen worden nagegaan bij hoeveel rechtspersonen zij zijn betrokken. Een voorbeeld is artikel 30, derde lid, van de Handelsregisterwet, waarin de verstrekking van overzichten van []gegevens gerangschikt naar individuele natuurlijke personen aan beperkingen is onderworpen. Voor de opsporing van strafbare feiten geldt een bijzondere bevoegdheid voor de (hulp)officier van justitie. Wanneer voor andere openbare registers vergelijkbare bevoegdheden nodig zijn, dan behoeven de desbetreffende opsporingsorganen daartoe een afzonderlijke wettelijke basis.

10. Rechtsbescherming

De WPR kent thans aan de geregistreerde het recht toe om zich via een verzoekschrift te wenden tot de burgerlijke rechter indien de houder weigert om aan bepaalde verzoeken van de geregistreerde gevolg te geven. De richtlijn dwingt niet om van de civiele rechtsgang af te zien. In artikel 22 wordt slechts bepaald dat de lidstaten ervoor moeten zorgen dat een ieder zich tot de rechter kan wenden wanneer de aan hem toegekende rechten op dit terrein worden geschonden. Het Nederlandse recht voldoet reeds aan deze eis. Niettemin geven de evaluaties aanleiding om nader te bezien op welke wijze de privacywetgeving beter zou kunnen aansluiten bij het rechtsstelsel als geheel. Die aansluiting is thans onvoldoende. De WPR heeft een relatief geïsoleerd bestaan geleid. Privacygeschillen zijn in de jurisprudentie veelal los van de WPR beoordeeld aan de hand van in publieken privaatrecht geldende algemene beginselen.
Derhalve bestaat de behoefte om de privacywetgeving beter te laten aansluiten bij de algemene ontwikkelingen binnen het publieken privaatrecht. Dat ligt ook voor de hand. De verwerking van persoonsgegevens speelt zowel in publieke als private organisaties een belangrijke rol. Zij vormt vaak de basis van beslissingen die binnen de betreffende organisatie worden genomen. De rechtmatigheid van de gegevensverwerking dient bij voorkeur ook in die context te worden beoordeeld. In de praktijk blijkt dat ook vaak op deze wijze te worden ervaren. Gebleken is dat binnen de openbare sector verzoeken krachtens de WPR aanvankelijk volgens de bezwaarschriftenprocedure worden afgedaan. De afhandeling van soms sterk verwante verzoeken krachtens de Wet openbaarheid van bestuur vindt immers ook op deze wijze plaats. Bij nadere bestudering van de zaak, blijkt dan dat de specifieke procedurebepalingen van de WPR afwijken, zodat dan alsnog de procedure van het Wetboek van Burgerlijke Rechtsvordering moet worden gevolgd. Onnodig tijdverlies is daarvan het gevolg.
Tegen deze achtergrond is in het wetsvoorstel, anders dan in de WPR, gekozen voor een gedifferentieerd systeem van rechterlijke toetsing. Zowel de bestuursrechter als de burgerlijke rechter hebben een taak. Concreet betekent dit dat beslissingen van bestuursorganen in hun hoedanigheid van verantwoordelijke naar aanleiding van een op de wet gebaseerd verzoek van de betrokkene – bijvoorbeeld een weigering van een verzoek om inzage of correctie – in bestuursrechtelijke zin als besluit zullen gelden. Op grond van de Awb staat daartegen bezwaar en beroep open. Met deze benadering wordt ook een betere aansluiting bewerkstelligd bij de Wet openbaarheid van bestuur, in het kader waarvan immers tegen vergelijkbare besluiten eveneens bezwaar en beroep openstaat.
Overigens verdient hier vermelding dat aanduiding van bedoelde beslissingen als een besluit in de zin van de Awb buiten de rechterlijke toetsing ook nog andere gevolgen heeft. Daarbij gaat het onder meer over de wijze waarop beslissingen moeten worden voorbereid. Zo volgt bijvoorbeeld uit de Awb dat voorafgaand aan de beslissing omtrent een

verzoek om inzage in beginsel zowel de betrokkene zelf als eventuele derden-belanghebbenden moeten worden gehoord. De verplichting moet afhankelijk van de omstandigheden worden afgeleid uit artikel 4:8 of artikel 3:2 Awb.
Voor de private sector is er wat de rechtsbescherming betreft geen verandering, met dien verstande dat de thans geldende verzoekschrift-procedure bij de civiele rechter niet alleen openstaat voor de betrokkene maar voor alle belanghebbenden. Verwezen zij naar artikel 46 van het wetsvoorstel. Overigens kunnen ook hier vergelijkbare eisen aan de procedure worden gesteld die aan de rechterlijke toetsing voorafgaat. De maatschappelijke zorgvuldigheid kan met zich brengen dat de verantwoordelijke alvorens een beslissing te nemen omtrent bijvoorbeeld een verzoek om inzage de betrokkene en eventuele derden-belanghebbenden hoort. Het verlenen van inzage zonder dat derden die daarvan nadeel kunnen ondervinden in de gelegenheid zijn gesteld daarover hun opvatting kenbaar te maken, kan onder omstandigheden een onrechtmatige daad opleveren.

11. Toezicht

11.1 De Registratiekamer

In alle landen van de Europese Unie met wetgeving op het gebied van gegevensbescherming is voorzien in een apart toezichthoudend orgaan. In aansluiting op deze ontwikkeling wordt in artikel 28 van de richtlijn voorgeschreven dat elke lidstaat een of meer toezichthoudende autoriteiten dient in te stellen, belast met het toezicht op de toepassing van de binnen zijn grondgebied ter uitvoering van de richtlijn vastgestelde bepalingen. In Nederland heeft een dergelijk toezichthoudend orgaan reeds vorm gekregen in de Registratiekamer onder het regime van de WPR. In de nieuwe situatie zal de Registratiekamer deze taak behouden. Voor het Nederlandse recht vormt zij de «toezichthoudende autoriteit» in de zin van artikel 28 van de richtlijn. Hoewel het voorwerp van regelgeving niet meer de persoonsregistratie, maar de verwerking van persoonsgegevens zal zijn, willen wij toch de naam «Registratiekamer» handhaven, omdat deze inmiddels tot op zekere hoogte is ingeburgerd.
De instelling van een toezichthoudende autoriteit krachtens de richtlijn kent als achtergrond dat het toezicht op de naleving van de wettelijke voorschriften niet uitsluitend afhankelijk kan worden gesteld van het initiatief van de burger. De toenemende informatietechnologische mogelijkheden tot manipulatie van persoonsgegevens maken de positie van de burger steeds kwetsbaarder. Het is voor de individuele burger zeer moeilijk greep te houden op de wijze waarop er met zijn persoonsgegevens wordt omgegaan. Dat hangt samen met het feit dat de verwerking van persoonsgegevens zich in belangrijke mate aan zijn waarneming onttrekt. Deze achtergrond rechtvaardigt de instelling van een overheidsorgaan met eigen bevoegdheden om de naleving van de wettelijke voorschriften en de rechtsontwikkeling op dit punt te bevorderen.
Ten opzichte van de WPR is de positie van de Registratiekamer in een aantal opzichten gewijzigd. Allereerst heeft de Kamer als rechtshandhavende instantie de beschikking gekregen over een aantal bevoegdheden waarmee ze daadwerkelijk in een proces van gegevensverwerking kan ingrijpen. Gewezen kan worden op met name de bevoegdheden, geregeld in hoofdstuk 10 van het wetsvoorstel (bestuursdwang, bestuurlijke boete). Daarmee wordt de toezichthoudende funktie van de Kamer uitgebreid in die zin dat waar de Kamer onrechtmatig gedrag constateert, deze constatering kan leiden tot een rechtens afdwingbare beslissing van de Kamer. Aan de andere kant wordt ook de rechtspositie van de verantwoordelijke versterkt omdat deze, anders dan onder de WPR, de

beslissing van de Registratiekamer in rechte kan aanvechten. Aldus wordt de regeling, in overeenstemming met de aanbevelingen van de juridische evaluatie, beter ingebed in het algemene recht.
In het kader van haar uitvoerende taken kan de Kamer onder bepaalde omstandigheden goedkeuren dat gevoelige gegevens in aanvulling op het wettelijk regime worden verwerkt (artikel 23, eerste lid, onder e). Verder bevat artikel 77, tweede lid, de bevoegdheid middels de afgifte van een vergunning de doorgifte van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt, mogelijk te maken. Voorts heeft zij bij bepaalde gegevensverwerkingen met bijzondere risico's de bevoegdheid voorafgaand onderzoek te doen, beoordeelt zij gedragscodes en houdt zij een openbaar register van binnengekomen meldingen. Ook voor de uitoefening van deze uitvoerende taken geldt dat de rechtsbescherming tegen handelingen van de Kamer is versterkt.
De Registratiekamer moet worden beschouwd als een zelfstandig bestuursorgaan. De notitie «Herstel van het primaat van de politiek bij de aansturing van zelfstandige bestuursorganen», waarin het kabinetsstandpunt over het rapport van de Algemene Rekenkamer «Zelfstandige bestuursorganen en ministeriële verantwoordelijkheid» is opgenomen (kamerstukken II, 1994/1995, 24 130, nr. 5, blz. 9), alsmede de Aanwijzingen inzake zelfstandige bestuursorganen (regeling van 5 september 1996, nr. 96M006572) komen dan in beeld. Dit doet onder meer de vraag rijzen naar de politieke controle op de wijze waarop de Registratiekamer haar bevoegdheden uitoefent.
De bevoegdheden van de Kamer zijn rechtstreeks verbonden aan het publieke belang dat zij behartigt: de behartiging van bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens. De bevoegdheden van de Kamer richten zich in eerste aanleg, uitgaande van de verticale werking van het grondrecht op bescherming van de persoonlijke levenssfeer, tot de gegevensverwerkingen binnen de overheidssector. Deze positie vraagt om een onafhankelijk funktioneren van de Kamer ten opzichte van die overheid. In artikel 28, eerste lid, van de richtlijn komt dit ook tot uitdrukking. Hierin wordt voorgeschreven dat de toezichthoudende autoriteit – voor Nederland zijnde de Registratiekamer – de opdragen taken in volledige onafhankelijkheid moet kunnen vervullen.
Deze overwegingen pleiten ervoor de Kamer in het wetsvoorstel – net als onder de huidige WPR – de vorm te geven van een zelfstandig bestuursorgaan, zijnde een bestuursorgaan op het niveau van de centrale overheid, dat hiërarchisch niet ondergeschikt is aan een minister.[1]
Hiermee blijft de onafhankelijke positie van de Kamer gewaarborgd. De Kamer moet bijvoorbeeld in haar toezichthoudende en handhavende taak volledig vrij zijn in de prioriteitstelling, in het bepalen welke gegevensverwerkingen haars inziens nader onderzocht moeten worden en in welke gevallen daadwerkelijk moet worden ingegrepen wegens vermeende onrechtmatigheid.
Dat laat onverlet dat de Minister van Justitie over bepaalde bevoegdheden dient te beschikken om de ministeriële verantwoordelijkheid voor de Registratiekamer als zelfstandig bestuursorgaan te kunnen effectueren. De Minister is echter slechts verantwoordelijk is voor zover zijn bevoegdheden gaan. Bij de reikwijdte van deze bevoegdheden is rekening gehouden met de bijzondere aard van de Registratiekamer. Deze laatste moet immers de vrijheid hebben zo nodig maatregelen te treffen ten gegevensverwerkingen die vallen onder de verantwoordelijkheid van de Minister van Justitie.
De bevoegdheden van de Minister kunnen worden beschouwd als een «minimum-pakket» aan noodzakelijke ministeriële bevoegdheden. In aansluiting op de genoemde notitie zijn de volgende bevoegdheden opgenomen:

[1] Aanwijzing 124a inzake zelfstandige bestuurorganen. Zie mede aanwijzing 124c.

– een algemeen inlichtingenrecht van de Minister (artikel 59, eerste lid);
– goedkeuring van het bestuursreglement (artikel 56, derde lid);
– een bevoegdheid om beleidsregels te stellen met betrekking tot de door de Kamer op te leggen bestuurlijke boete (artikel 74);
– regeling van de rechtspositie van de leden van de Kamer bij algemene maatregel van bestuur (artikel 55, eerste lid);
– benoeming van de leden van de Kamer (artikelen 53 en 54).

De Aanwijzingen inzake zelfstandige bestuursorganen zijn daarbij als uitgangspunt gehanteerd.
Op de documenten die bij de Registratiekamer berusten is blijkens artikel 1, onder b, van het Aanwijzingsbesluit bestuursorganen WOB en WNo, de Wet openbaarheid van bestuur (WOB) van toepassing. Dit betekent dat de Registratiekamer een verzoek om informatie moet honoreren, tenzij de uitzonderingsgronden van artikel 10 van die wet van toepassing zijn.
De Wet Nationale ombudsman (WNo) is daarentegen niet van toepassing op de Registratiekamer op grond van artikel 1a, eerste lid, onder b, van de WNo. In de plaats daarvan zijn in artikel 54, tweede lid, de met de WNo verwante bepalingen uit de Wet op de rechterlijke organisatie van overeenkomstige toepassing verklaard. Dit is gelet op artikel 39, tweede lid, WPR conform de huidige situatie. Voor de Commissie gelijke behandeling – die een met de Registratiekamer vergelijkbare positie inneemt – gelden dezelfde bepalingen. Aangezien langs deze weg is voorzien in een toereikende klachtenvoorziening en de ervaringen tot dusverre geen aanleiding geven tot heroverweging, is de WPR op dit punt gehandhaafd. In het kader van de voorgenomen algehele herziening van het klacht- en tuchtrecht voor de rechterlijke organisatie kan opnieuw de vraag aan de orde komen of aanpassing noodzakelijk is en de Registratiekamer alsnog onder het bereik van de WNo moet worden gebracht.
Verder heeft de Registratiekamer de bevoegdheid een door haar geconstateerde onrechtmatige verwerking bij de overheid in bepaalde gevallen onder de aandacht te brengen van de rechter. Uit artikel 1:2, tweede lid, in verband met artikel 8:1, eerste lid, Awb volgt dat de Registratiekamer als belanghebbende beroep kan instellen tegen gegevensverwerkingen voor zover zij als een besluit kunnen worden aangemerkt. Aldus wordt althans voor een deel uitvoering gegeven aan artikel 28, derde lid, derde streepje, van de richtlijn.
Als ieder bestuursorgaan dient ook de Registratiekamer te handelen volgens de algemene beginselen van behoorlijk bestuur, waaronder het zorgvuldigheidsbeginsel. Dit houdt onder meer in dat in voorkomend geval de Kamer het beginsel van hoor en wederhoor toepast. Dit betekent dat alvorens zij een rapport over een verantwoordelijke of een groep van verantwoordelijken vaststelt, zij deze in de gelegenheid stelt over het ontwerp een standpunt te bepalen en dat de Kamer kenbaar te maken. Deze procedure wordt in de praktijk ook toegepast door de Algemene Rekenkamer. Ditzelfde geldt ook bij de aankondiging van een onderzoek middels een persbericht. Onder omstandigheden is dit een doeltreffend en nuttig instrument. In gevallen dat een dergelijke aankondiging echter schade kan toebrengen aan de goede naam van de desbetreffende branche, behoort het tot het zorgvuldigheidsbeginsel het voornemen daartoe eerst bekend te maken bij de te onderzoeken verantwoordelijken. Waar hun belangen in het geding zijn, moeten zij in de gelegenheid zijn eventueel via een kort geding dreigende schade van hun belangen door de voorgenomen publicatie te kunnen afwenden.

11.2. De functionaris voor de gegevensbescherming

Zoals hiervoor al aangegeven wordt in het wetsvoorstel een wettelijke basis gecreëerd voor de functionaris voor de gegevensbescherming. De constructie is afkomstig uit het Duitse recht. Het Duitse recht kende vanouds binnen de private sector een toezichthouder binnen het eigen

bedrijf. In de richtlijn heeft dit de vertaling gevonden in de mogelijkheid voor de lid-staten om als alternatief voor de melding bij de van overheidswege ingestelde toezichthouder, te kunnen melden bij een door de verantwoordelijke of een organisatie van verantwoordelijken aangestelde toezichthouder. Voor de Nederlandse wetgeving is het nieuw: een dergelijk instituut kent de WPR niet. Niettemin sluit regeling van dit instituut in bepaalde sectoren in belangrijke mate aan bij een reeds bestaande praktijk. In een aantal organisaties functioneren reeds privacyofficers en commissie van toezicht. In de praktijk zijn positieve ervaringen opgedaan met dergelijke functionarissen of commissies. Binnen een bedrijf, organisatie, branche of overheidssector wordt een dergelijke functionaris de vraagbaak voor de medewerkers. Ten opzichte van de Registratiekamer vervult zo'n functionaris de rol van intermediair. Tot nu toe ging het om functionarissen zonder bevoegdheden. De waarde van het nieuwe instituut is met name gelegen in de mogelijkheden om de uitoefening van taken en bevoegdheden van de Registratiekamer, onder behoud van haar positie, door deze functionaris te laten verrichten op een voor de desbetreffende organisatie, branche of sector geëigende wijze. Het gaat om een facultatieve regeling: aanstelling van een privacyfunctionaris is niet verplicht. Instelling van de privacyfunctionaris heeft – zoals hiervoor al vermeld – in beginsel tot gevolg dat niet bij de Registratiekamer gemeld behoeft te worden. Volgens artikel 18, tweede lid, van de richtlijn dient de functionaris op onafhankelijke wijze toezicht uit te oefenen op de naleving van de bij of krachtens de wet gestelde voorschriften binnen de organisatie of branche waar hij is aangesteld. Om zijn toezicht daadwerkelijk te kunnen uitoefenen, is het noodzakelijk dat de functionaris toegang heeft tot alle systemen waar mogelijk gegevens worden verwerkt. Daartoe is in het wetsvoorstel opgenomen dat hij beschikt over vergelijkbare bevoegdheden als de Registratiekamer met betrekking tot de verwerkingen waarvoor hij is aangesteld.
Treft de functionaris onregelmatigheden aan, dan ligt in zijn taakopdracht en in zijn aanstelling besloten dat hij daarover verslag uitbrengt aan de verantwoordelijke of de organisatie waardoor hij is aangesteld. Zijn rol tegenover de verantwoordelijke is louter adviserend. Het is aan de verantwoordelijke om te beslissen of hij een advies van de privacyfunctionaris opvolgt. De functionaris heeft geen verplichting onregelmatigheden te melden bij de Registratiekamer. Daar staat tegenover dat de Registratiekamer te allen tijde zijn bevoegdheden kan uitoefenen, ook al is er een functionaris aangesteld binnen de organisatie of branche.

12. Handhaving

De handhaving van wettelijke voorschriften wordt in EU-verband beschouwd als een terrein dat in beginsel is voorbehouden aan de lidstaten. De richtlijn stelt op dit terrein dan ook geen gedetailleerde eisen. In artikel 24 wordt bepaald dat de lidstaten «passende maatregelen» nemen om de toepassing van de uit de richtlijn voortvloeiende voorschriften te garanderen, waarbij met name gedacht wordt aan de vaststelling van sancties. Op een enkel punt is de richtlijn concreter. In relatie tot de bevoegdheden van de toezichthoudende autoriteit – lees: de Registratiekamer – spreekt de richtlijn onder meer over «effectieve bevoegdheden om in te grijpen» met verwijzing naar enkele voorbeelden. Evenals onder de huidige wet zal het in de WBP bij de handhaving van wettelijke voorschriften in belangrijke mate aankomen op het initiatief van degene van wie gegevens worden verwerkt. In de richtlijn worden daartoe aan de betrokkene enkele rechten toegekend. Die rechten verschillen – behoudens het recht op verzet – niet wezenlijk van de aanspraken die thans ingevolge de WPR worden toegekend. Op dit punt is dus in sterke mate sprake van continuïteit.
Wel is er een belangrijk verschil in de wijze waarop de bedoelde rechten in

rechte zullen kunnen worden afgedwongen. De rol van de burgerlijke rechter zal minder belangrijk worden. Hiervoor is immers reeds vermeld dat in de publieke sector niet langer de weg naar de burgerlijke rechter, maar naar de bestuursrechter zal openstaan. Tegen bijvoorbeeld een weigering tot inzage door een bestuursorgaan zal onder de nieuwe wet de Awb-procedure moeten worden gevolgd.
Een belangrijke verandering is voorts dat de Registratiekamer de beschikking zal krijgen over enkele bestuursrechtelijke handhavingsinstrumenten. In de eerste plaats zal de Registratiekamer de bevoegdheid krijgen om bestuursdwang en daarmee verwante bestuurlijke maatregelen toe te passen. De basis daarvoor is te vinden in artikel 28, derde lid, van de richtlijn. In deze bepaling wordt onder meer gesproken over «de bevoegdheid om afscherming, uitwissing of vernietiging van gegevens te gelasten». Materieel gezien komt deze bevoegdheid overeen met hetgeen in de Awb met «bestuursdwang» wordt aangeduid.
Op de bestuursdwangbevoegdheid van de Registratiekamer zal de Awb van toepassing zijn. In de derde tranche van deze wet – die op 1 juli 1997 in werking zal treden[1] – zijn omtrent bestuursdwang algemene regels opgenomen. Hierin wordt onder meer bepaald dat aan de overtreder – behoudens spoedeisende gevallen – eerst nog een termijn moet worden gegund waarbinnen hij de tenuitvoerlegging van de bestuursdwangbeschikking kan voorkomen door zelf maatregelen te nemen. De kosten die aan de toepassing van bestuursdwang zijn verbonden, zullen voor rekening komen van de overtreder. In de regel zal dit de verantwoordelijke zijn. Voorts zal de Awb regelen dat een bestuursorgaan dat bevoegd is bestuursdwang toe te passen, in plaats daarvan een last onder dwangsom kan opleggen.
Naast de bestuursdwangbevoegdheid kent het wetsvoorstel de Registratiekamer de bevoegdheid toe om een bestuurlijke boete op te leggen indien de verantwoordelijke ten onrechte niet of op onvolledige wijze heeft voldaan aan zijn meldingsverplichting. Thans geldt een dergelijke overtreding uitsluitend als een strafbaar feit. Strafrechtelijke handhaving van een dergelijke administratieve verplichting lijkt evenwel in de regel minder geschikt. Voor zover bekend is ook nog nooit strafrechtelijke vervolging ingesteld. Met het oog op een effectievere handhaving wordt voorgesteld om de bestuurlijke boete in te voeren. De maximum-hoogte van de boete verschilt niet wezenlijk van de boete die thans langs strafrechtelijke weg kan worden opgelegd.
Conform het kabinetsbeleid[2] inzake bestuurlijke boeten is in het wetsvoorstel een aantal nadere voorzieningen en waarborgen opgenomen. Deze houden onder meer verband met de eisen die voortvloeien uit artikel 6 EVRM. Alvorens de boete wordt opgelegd, zal de verantwoordelijke eerst moeten worden gehoord. De bevoegdheid vervalt indien de verantwoordelijke aantoont dat hem geen verwijt treft. De verantwoordelijke heeft echter ook het recht om te zwijgen. Vanaf het moment dat redelijkerwijs duidelijk is dat aan de verantwoordelijke een boete zal worden opgelegd, is hij niet verplicht ter zake daarvan enige verklaring af te leggen.
Een belangrijk sluitstuk van de bestuursrechtelijke handhaving zal worden gevormd door de mogelijkheid van rechterlijke toetsing. Tegen bestuursdwang-, dwangsom- en boetebeschikkingen staat conform de Awb bezwaar en beroep open.
De thans reeds bescheiden rol van het strafrecht in de WPR zal verder afnemen. Op grond van artikel 50 WPR zijn – kort gezegd – alleen het in werking hebben van een niet-aangemelde persoonsregistratie en de overtreding van de regels voor het internationale gegevensverkeer strafbaar gesteld. Wat het eerste betreft zal het accent veel sterker komen te liggen op de bestuursrechtelijke handhaving. In geval van overtreding van de meldingsverplichting zal waarschijnlijk in het overgrote deel van de gevallen alleen een bestuurlijke boete in aanmerking komen. In

[1] Wet van 20 juni 1996, Stb. 1996, 333.
[2] Kamerstukken II 1993–1994, 23 400 VI, nr. 48. Door het huidige kabinet overgenomen.

uitzonderingsgevallen kan het strafrecht evenwel niet worden gemist. Dat hangt nauw samen het feit dat sommige overtreders zich fysiek in het buitenland bevinden.
De formulering als strafbaar feit heeft gevolgen in de sfeer van het internationale strafrecht en de omvang van de nationale jurisdictie. Van belang is de vraag of een gedraging onder nationaal recht valt. Met het gebruik van moderne informatietechnologische middelen met betrekking tot persoonsgegevens is de situatie geenszins denkbeeldig dat de gevolgen van een feit zich in Nederland manifesteren en daarmee het feit in Nederland wordt gepleegd, maar dat de dader in het buitenland is. Een dergelijk feit valt dan onder de Nederlandse jurisdictie. Zo kan het voorkomen dat iemand vanuit het buitenland via telecommunicatie onopgemerkt persoonsgegevens in Nederland vergaart of persoonsgegevens doelbewust in Nederland verspreidt of ter beschikking stelt, zonder de verwerking aan te melden. Dit kan een in Nederland gepleegd strafbaar feit zijn, ook al bevindt de dader zich op het moment van het plegen in het buitenland. Raadpleegt daarentegen iemand vanuit Nederland via telecommunicatie gegevens die in het buitenland zijn opgeslagen, dan pleegt degene die de gegevens ter beschikking stelt geen strafbaar feit op Nederlands territoir. Zijn handeling is namelijk niet in het bijzonder op Nederland gericht.
Als het feit wordt gepleegd door iemand die zich niet in Nederland bevindt, dan zijn er mogelijkheden de strafvervolging over te dragen aan het land van verblijf of om te vragen om uitlevering. Gaat het om relatief lichte vergrijpen, dan zullen deze instrumenten slechts beperkt bruikbaar zijn. Een strafrechtelijke vervolging zal wegens problemen met de vaststelling van de identiteit van de dader en overige problemen met betrekking tot de bewijsvergaring, niet altijd mogelijk zal zijn. Ook zal in een aantal gevallen de tenuitvoerlegging van een eventuele veroordeling in Nederland voor de veroordeelde slechts tot gevolg hebben dat hij, hangende de termijn van de verjaring van het recht van tenuitvoerlegging van de straf, een bezoek aan Nederland zal vermijden. De duurzame arbeid aan de verbetering van de internationale samenwerking op strafrechtelijk gebied zal een deel van de problemen op dit terrein kunnen wegnemen.
Met betrekking tot bepaalde gedragingen die uitwerking hebben op Nederlands territoir, is het in het belang van de Nederlandse rechtsorde dat deze gedragingen strafrechtelijk kunnen worden gehandhaafd. Overweging 21 van de richtlijn maakt duidelijk dat de richtlijn geen afbreuk doet aan de toepasselijkheid van het Nederlands strafrecht. De handhaving van het strafrecht is een aangelegenheid van openbare orde en ingevolge het EG-Verdrag is dat voorbehouden aan het nationale recht. Daar waar de richtlijn voorschrijft of toestaat bepaalde gedragingen te verbieden, onttrekt vervolgens de eventuele toepassing van het strafrecht op de niet-naleving van deze gedragingen zich aan het communautaire recht. Een strafrechtelijke sanctionering laat onverlet dat overtredingen ook langs bestuursrechtelijke weg kunnen worden afgedaan.
Naast de meldingsplicht blijven ook een beperkt aantal overtredingen strafbaar die samenhangen met het internationale gegevensverkeer. Het betreft in de eerste plaats het verbod gericht tot een verantwoordelijke die buiten de Unie is gevestigd, om in Nederland gegevens te verwerken zonder een vertegenwoordiger aan te wijzen. Daarnaast is strafbaar de doorgifte van gegevens naar landen buiten de Unie waarvan op Europees niveau is bepaald dat geen passend beschermingsniveau aanwezig is.

13. Kosten

13.1. Kosten algemeen

Tijdens de voorbereiding van de richtlijn zijn verschillende onderzoeken gedaan naar de te verwachten financiële gevolgen. Daarbij is op opeenvolgende tijdstippen uitgegaan van volgende versies van het ontwerp van de richtlijn, telkens weerspiegelende de stand van de onderhandelingen. In deze onderhandelingen speelden ook weer de resultaten van eerdere kostenonderzoeken een rol.
Het eerste onderzoek is dat van L.G.M. Veeken en J.A. Knigge van het Economisch Instituut voor het Midden- en Kleinbedrijf (EIM) van april 1994, verricht in opdracht van het Ministerie van Economische Zaken als bedrijfseffectenrapportage. Het ging uit van de tekst van het ontwerp van de richtlijn van 15 oktober 1992. Op basis van een opgave van vertegenwoordigers van de desbetreffende bedrijfstak kwam het EIM tot de conclusie dat vooral de banken, de verzekeraars en de direct-marketingbedrijven veel extra kosten zouden moeten maken bij invoering van de tekst in de toenmalige versie.
Een belangrijke kostenpost in deze studie vond zijn oorsprong in de opvatting van de banken dat, gegeven de onzekerheid over de wettelijke criteria, zij al hun klanten afzonderlijk toestemming voor de verwerking van de hen betreffende persoonsgegevens zouden moeten vragen. Daarnaast werden hoge kosten verwacht bij de aanpassing van computerprogrammatuur. De andere branches kwamen op lagere kosten uit. Verder bestond zorg over een aantal PM-posten, waarvan de mogelijke kosten op dat moment nog niet konden worden gekwantificeerd. De studie heeft aanleiding gegeven enerzijds tot toevoegingen van interpretatieve overwegingen voorafgaand aan de richtlijn, anderzijds tot aanpassingen van de tekst van de richtlijn zelf.
Een tweede onderzoek is uitgevoerd in november 1994 in opdracht van de Europese Commissie door mevrouw J.E.J. Prins van de Universiteit te Tilburg en J. Theeuwes van de Universiteit te Leiden, als onderdeel van een voor het overige in het Verenigd Koninkrijk uitgevoerde studie. Dit onderzoek is gebaseerd op de tekst van de richtlijn in de versie van juli 1994. De studie laat een discrepantie zien tussen de perceptie van de houders in de informatie-intensieve sectoren en de inschatting van de onderzoekers. Verder is met name op het punt van de direct marketing, mede naar aanleiding van deze studie, in de laatste fase van de totstandkoming van de richtlijn een aanmerkelijke vereenvoudiging aangebracht op het punt van de informatieverstrekking aan de betrokkenen.
Een derde onderzoek is in Nederland uitgevoerd door mevrouw C. G. M. van Oosteren en J. S. van Vliet door het Instituut voor Onderzoek van Overheidsuitgaven (IOO) in november 1994, onder begeleiding van een commissie onder leiding van prof. H. W. K. Kaspersen. De aanleiding hiertoe was het mondeling overleg tussen de Minister van Justitie en de vaste commissie voor Justitie van de Tweede Kamer op 27 oktober 1993. Het onderzoek omvatte zowel de zorgsector, uitvoeringsorganen van de sociale verzekeringen als de lagere overheden.
Het bracht aan het licht dat voor de overheid vooral initiële kosten zijn te verwachten wanneer met het oog op de invoering van de nieuwe wet programmatuur moet worden aangepast, in het bijzonder wat betreft de mogelijkheid gegevens desgevraagd af te schermen tegen gebruik voor direct marketing. Wanneer evenwel in het kader van periodieke aanpassingen van de programmatuur aan nieuwe ontwikkelingen in de techniek of de wetgeving, geleidelijk aan, hangende de implementatietermijn, ook de eisen van de richtlijn worden verwerkt, dan kunnen de kosten worden teruggebracht tot een bedrag dat verwaarloosbaar is ten opzichte van de beheerskosten van de desbetreffende informatiesystemen in het

algemeen. Verder werden extra kosten gevreesd als gevolg van de verruimde bevoegdheden van de Registratiekamer.
Dit onderzoek schat de initiële kosten op 25 tot 50 miljoen, uitgaande van aanpassing van beleid en programmatuur. Minstens de helft daarvan is gelokaliseerd bij de gemeenten. De jaarlijks weerkerende kosten worden geschat op 1 miljoen. Daarnaast zijn er extra kosten voor de Registratiekamer. Hetzelfde onderzoek bracht ook baten in kaart, te weten een verbeterde fraudebestrijding als gevolg van de nieuwe mogelijkheden tot een onbelemmerde internationale uitwisseling van persoonsgegevens binnen de Unie. Deze baten zijn moeilijk te becijferen.
Na vaststelling van de richtlijn is er voor gekozen geen hernieuwd onderzoek te doen naar de te verwachten financiële consequenties van de implementatie van de richtlijn. Daarvoor was geen reden aangezien de reeds verrichte onderzoeken, waarbij met name kan worden gewezen op het onderzoek uitgevoerd in opdracht van de Europese Commissie en het onderzoek van het Instituut voor Onderzoek van Overheidsuitgaven, waren gebaseerd op teksten van de richtlijn die niet veel afwijken van de tekst van de richtlijn zoals die uiteindelijk is vastgesteld. De wijzigingen die in de definitieve tekst waren opgenomen zouden naar verwachting zodanig geringe financiële consequenties hebben dat een hernieuwd onderzoek niet noodzakelijk werd geacht.
In aanvulling op de verrichte onderzoeken merken wij over de kosten nog het volgende op. Wat betreft de toepassing van de materiële normen, voor zover het niet gaat om de verwerking van de gevoelige gegevens, hebben wij reeds duidelijk gemaakt dat deze sterk samenhangen met de toepassing van meer algemene beginselen. In het civiele recht betreft het het leerstuk van de onrechtmatige daad. Wat betreft het bestuursrecht gaat het om de toepassing van beginselen van behoorlijk bestuur. Er zijn enige aandachtspunten bij de concretisering van deze beginselen in het geval van verwerking van persoonsgegevens: de doelbinding, het verenigbaar gebruik en het belang van de betrokkene. Ten opzichte van de WPR zijn deze niet nieuw. Een verruiming van deze beginselen vindt in zoverre plaats dat verstrekking aan derden niet meer beperkt is tot verstrekkingen die voortvloeien uit het doel van de registratie: ook andere, verenigbare doelen kunnen gediend worden, daaronder begrepen doelen van derden. Onder de WPR was de notie van het verenigbaar gebruik beperkt tot het eigen gebruik door de houder. Een kostenvermeerdering als gevolg van de omschrijving van materiële normen in het wetsvoorstel, valt daarom niet te verwachten.
De transparantie is in het onderhavig wetsvoorstel aangescherpt. De verplichting de betrokkene informatie ter beschikking te stellen over de verwerking van zijn gegevens zal slechts beperkte kosten met zich brengen in het geval de gegevens bij de betrokkene worden vergaard. Er hoeven immers geen kosten te worden gemaakt om de betrokkene te bereiken. Zeker waar de gegevens in de naaste toekomst steeds vaker via de elektronische snelweg worden vergaard, kan de informatie van de betrokkene zonder veel problemen langs dezelfde weg plaatsvinden. In het geval de gegevens buiten de betrokkene om worden vergaard, dient de betrokkene te worden geïnformeerd. In dat geval geldt evenwel een uitzonderingsgrond indien de verstrekking van informatie aan de betrokkene over de verwerking van gegevens over hem, onmogelijk blijkt of een onevenredige inspanning kost. Deze clausule voorkomt de noodzaak onder omstandigheden disproportionele kosten te maken.
Een ander aspect van de transparantie is de melding bij de toezichthouder. Wat betreft de private sector is het aantal gegevens dat bij de melding moet worden verstrekt, zoals neergelegd in de algemene maatregel van bestuur van 22 december 1989 (Stb. 587) geringer dan de gegevens die ingevolge het onderhavige wetsvoorstel moet worden gemeld. Zo hoeft geen opgave meer te worden gedaan van de aard van de gegevens die worden verwerkt, de wijze van verkrijging, de verwij-

dering, de soort van gegevens die wordt verstrekt, de personen die rechtstreeks toegang hebben en de gegevens waarvan zij mogen kennis nemen, eventuele verbanden met andere registraties, de wijze van kennisneming en verbetering en de hoofdlijnen van het beheer. Een aanmerkelijke lastenverlichting mag worden verwacht van de beëindiging van de meldingsplicht voor handmatige bestanden, hoewel de materiële regels van het wetsvoorstel daarop van toepassing blijven en onder omstandigheden voorafgaande toetsing door de Registratiekamer is voorgeschreven.
Daarvoor komt in de plaats dat, anders dan voorheen, wel een opgave moet plaatsvinden van de (categorieën van) personen aan wie binnen de organisatie van de verantwoordelijke gegevens worden verstrekt. Dit sluit aan bij de ontwikkeling van multifunctionele informatiesystemen. Verder dienen voorgenomen overdrachten aan landen buiten de Europese Unie te worden gemeld, alsmede een algemene beschrijving van de veiligheidsmaatregelen. De balans opmakend kan worden verwacht dat de inhoud van de melding aanmerkelijk eenvoudiger zal zijn dan tot dusver.
Wat betreft de procedure is er verder de mogelijkheid om in plaats van aan de Registratiekamer te melden bij een eigen toezichthouder met een op het eigen bedrijf of de eigen branche toegesneden aanmeldingsprocedure. Beide aspecten, inhoud en procedure, kunnen leiden tot besparingen ten opzichte van nu.
Wat betreft de publieke sector vervalt de reglementsplicht krachtens hetwelk in een uitgeschreven regeling de werking van de registratie moet zijn beschreven. Dit betekent een substantiële lastenverlichting. In de overgangsfase naar de nieuwe wet staat daar voor private en publieke sector tegenover een eenmalige lastenverzwaring in die zin dat niet-vrijgestelde gegevensverwerkingen overeenkomstig het nieuwe regime moeten worden gemeld.
Er zijn allerlei mogelijke lastenverlichtingen enverzwaringen die tegen elkaar moeten worden afgewogen. De precieze omvang ervan is wegens vele onzekerheden niet nader vaststelbaar. Zo is onzeker hoe de interpretatie van de verschillende vage begrippen, mede in verband met de technische ontwikkelingen, in de loop der tijd zich zal ontwikkelen. Wel is aannemelijk dat ook zonder een wettelijke regeling als de onderhavige, krachtens algemene rechtsbeginselen, de jurisprudentie toch eisen ter bescherming van de burger zou stellen, daar waar zijn gerechtvaardigde belangen in de knel zouden dreigen te komen.
In het algemeen brengt de richtlijn de interne markt binnen de Unie ook het gebied van de uitwisseling van persoonsgegevens tot stand. Daar waar naar verwachting het economisch verkeer via de elektronische snelweg een hoge vlucht zal nemen, is het noodzakelijk de mogelijkheden weg te nemen dit verkeer te belemmeren om redenen van gegevensbescherming. De financiële bate in dit opzicht is onzeker, valt niet te becijferen, doch ook niet weg te cijferen. Hetzelfde geldt voor het consumentenvertrouwen mede gebaseerd op de wetenschap van een min of meer uniform niveau van becherming van persoonsgegevens binnen de Unie.
Het een en ander overziende menen wij dat – mede gezien het ruime bereik van het wetsvoorstel – het redelijk is de verantwoordelijke zowel de kosten die het wetsvoorstel met zich brengt, te laten dragen, als te profiteren van de baten die het oplevert.
Bij brief van 18 november 1996 aan de Minister van Justitie heeft de Vereniging van Nederlandse Gemeenten (VNG) de aandacht gevraagd voor de door haar verwachte lastenverzwaring die de invoering van het wetsvoorstel voor gemeenten mee zal brengen en de verwachting uitgesproken dat de gemeenten daarvoor financieel zullen worden gecompenseerd. Bij brief van 29 oktober 1997, kenmerk 646937/97/4, is door de Minister van Justitie, mede namens de Minister van Financiën en de Staatssecretarissen van Binnenlandse Zaken aan de VNG medegedeeld

dat de ministerraad van 13 juni 1997 heeft besloten om de financiële consequenties van de uitvoering van de WBP niet te compenseren aan instanties die persoonsgegevens verwerken. Het door de VNG aangehaalde artikel 2 van de Financiële-verhoudingswet, wel aangeduid als «boter bij de vis»-bepaling, heeft betrekking op kosten die gemeenten ingevolge medebewind moeten maken. De verplichtingen die voortvloeien uit de WBP gelden voor iedere verantwoordelijke voor verwerking van persoonsgegevens, ongeacht of het de particuliere of publieke sector betreft. Het zijn algemene verplichtingen, die zich niet specifiek richten op gemeenten. Dat leidt ertoe dat geen sprake is van medebewind als bedoeld in artikel 108 van de Gemeentewet. Compensatie van kosten is daarom niet vereist.

13.2. Kosten van de Registratiekamer

a. Reeds uitgevoerde uitbreiding

Ten tijde van instelling van de Registratiekamer in 1988 is budget vrijgemaakt van f 2,8 mln. voor de werkzaamheden van de Registratiekamer. Dit budget is destijds door vrijwel alle departementen gezamenlijk gefinancierd, vanuit de gedachte dat ieder departement klant is van de Registratiekamer. In de afgelopen jaren is de werklast van de Registratiekamer echter substantieel gestegen. Ter illustratie:
– het aantal onderzoeken vertoont een continue forse stijging;
– het aantal telefonische verzoeken is ruimschoots verdubbeld;
– het aantal getoetste modelreglementen is verzesvoudigd;
Het aantal aan de rechterlijke macht dan wel inzake wetgeving/beleid gegeven adviezen is in de loop van de tijd stabiel gebleven (ongeveer 25 per jaar), het aantal adviezen inzake wetgeving en beleid aan de rechtelijke macht is licht afgenomen. Met ingang van 1996 worden privacy-audits uitgevoerd. Dergelijke audits zijn noodzakelijk om normconform handelen op grond van de WPR en andere voor de privacybescherming relevante wetten te bevorderen. Het belang hiervan is nog eens onderstreept in de conclusies van de parlementaire enquete-commissie opsporingsmethoden. In de richtlijn is de mogelijkheid van het houden van audits voorzien en extra ondersteund door het geven van processuele bevoegdheid aan door de wet in het leven geroepen privacy beschermende organisaties.
Met de werklasttoename van de Registratiekamer sinds 1988, inclusief de nieuwe taak van de privacy-audits is een structurele budgetuitbreiding gemoeid van fl 2,1 mln. Bij de geleidelijke budgetuitbreiding in de afgelopen jaren is afgezien van interdepartementale versleuteling wegens de jaarlijks relatief geringe omvang van de kostenstijging. Omdat de jaarlijkse werklastverzwaring direct samenhangt met de vereisten van dit wetsvoorstel, is het vanzelfsprekend dat deze groeikosten mee worden genomen bij de financiele consequenties van het wetsvoorstel. Immers een groot deel van de vereisten in het kader van dit wetsvoorstel is al opgevangen door de geleidelijke uitbreiding van de kamer.

b. Extra uitbreiding conform vereisten WBP

Met de taakuitvoering volgens de vereisten van dit wetsvoorstel is een werklasttoename te verwachten. Ten opzichte van de huidige taakuitvoering en werkbelasting is daarom een verdere uitbreiding van de Registratiekamer vereist. Aan de Registratiekamer worden immers extra bevoegdheden toegekend. Hieronder is aangegeven wat de te verwachten kosten zijn van deze nieuwe bevoegdheden. Daarbij is voorzien in de mogelijkheid van een rechterlijke toetsing door de bestuursrechter van die bevoegdheden.
– onderzoeks- en handhavingsbevoegdheden: in dit wetsvoorstel is

vastgelegd niet alleen de bevoegdheid tot het doen van onderzoeken, maar ook tot het doen van voorafgaand onderzoek en de bevoegdheid tot het uitoefenen van bestuursdwang dan wel het (doen) opleggen van een administratieve boete. De structurele kosten hiervan zijn f 330 000.

– aanmelding van gegevensverwerkingen: het huidige WPR-bestand bevat ruim 50 000 aanmeldingen. Wegens de ruimere meldingsplicht is voor het inbrengen van nieuwe aanmeldingen in het systeem in het jaar van invoering (incidenteel) f 290 000 nodig. Voorts dient het geautomatiseerde systeem te worden aangepast in verband met artikel 30, eerste lid, van dit wetsvoorstel. De incidentele kosten voor de ontwikkeling van een geautomatiseerd systeem van aanmeldingen en inzage is voorlopig geschat op f 250 000. Hoewel de omvang van het aanmeldingenbestand naar verwachting zal afnemen, zal het onderhoud van het bestand (nieuwe aanmeldingen en mutaties) kwalitatief hogere eisen stellen aan de betrokken functionarissen. Het aanmeldingenbestand speelt immers een belangrijke rol in het handhavingstraject. Dit veronderstelt voldoende inhoudelijke deskundigheid en zelfstandige werkzaamheid. Benodigd is een structurele aanpassing en uitbreiding van de formatie (f 80 000).
– procesvoering en sancties: de uitvoering van de taken zoals genoemd in hoofdstuk 10 van dit wetsvoorstel komen te liggen bij een afzonderlijke eenheid Procesvoering en sancties. Deze taken moeten binnen strakke termijnen worden uitgevoerd en vragen een specifieke kennis op de desbetreffende gebieden. De Registratiekamer moet onder andere een gedetailleerd, goed onderbouwd proces-verbaal overleggen. Hiertoe hebben de betrokken medewerkers opsporingsbevoegdheid nodig. De hieruit voortvloeiende structurele kosten zijn f 335 000.
– voorlichting: Bij de invoering van de nieuwe wet zal een intensieve algemene voorlichtingscampagne moeten worden gehouden. alsmede campagnes per sector. De kosten worden voorshands geraamd op incidenteel f 350 000,=.

Samengevat: De extra kosten voor de Registratiekamer zijn

– f 2,1 miljoen wegens werklastverzwaring sinds 1988
– f 0,7 mln, aanvulling om te voldoen aan de EU Richtlijn
– f 2,8 mln structureel
– f 0,9 mln. incidenteel

14. Evaluaties

14.1. Algemeen

Het onderhavige wetsvoorstel bouwt voort op de Wet persoonsregistraties, daarbij tevens de internationale rechtsontwikkeling incorporerend. Daarbij is dankbaar gebruik gemaakt van de resultaten van twee evaluaties van de WPR: een juridische en een sociaal-wetenschappelijke. De juridische evaluatie is verricht door mevrouw G. Overkleeft-Verburg in haar dissertatie «De Wet persoonsregistraties, norm, toepassing en evaluatie» (Tjeenk Willink, Zwolle, augustus 1995). De studie werd begeleid door een commissie onder leiding van M. Scheltema. Als promotor trad op E. M. H. Hirsch Ballin. De sociaal-wetenschappelijke evaluatie, getiteld «In het licht van de Wet persoonsregistraties, zon, maan of ster ?» (Samson, Alphen a/d Rijn, december 1995), werd verricht in het kader van het interdepartementale onderzoeksprogramma «Informatietechnologie & recht» (ITeR) onder het voorzitterschap van het Ministerie van Economische Zaken, door een team van de Katholieke Universiteit Brabant onder leiding van mevrouw J. E. J. Prins. De studie werd begeleid door een commissie met onder meer vertegenwoordigers van overheid

en bedrijfsleven en onder leiding van H. Franken. Het werd afgerond in december 1995.
Beide evaluaties hebben duidelijk gemaakt dat de WPR slechts in beperkte mate de rechtsvorming in de omgang met persoonsgegevens heeft beïnvloed. Veel energie is gaan zitten in de uitvoering van de administratieve voorschriften, zoals het inzenden van meldingsformulieren en het opstellen van reglementen. Het doel achter deze voorschriften is daarmee enigszins uit zicht geraakt. Wel blijkt dat de bescherming van persoonsgegevens als buitengewoon wenselijk wordt ervaren.

14.2. De juridische evaluatie

De juridische evaluatie brengt aan het licht hoe de WPR nog de sporen van haar wording draagt die begon in een tijd van het prille begin van de informatietechnologie: grote computers bedienden vanuit een centraal punt perifere afnemers. De zorg was gericht op de onoverzienbare gevolgen bij koppeling van deze bestanden. De regeling van deze centrale bestanden vormde daarom het aanknopingspunt van de regeling. Ook uit de naam die aan de wet is gegeven, blijkt dat het gaat om persoonsregistraties: de normering van de gebundelde macht die besloten ligt in centrale gegevensopslag. Het aanknopingspunt vormde het doel van deze bundeling. Ondanks de ontwikkeling sindsdien van multifunctionele informatiesystemen, veelal via een netwerk met elkaar verbonden, was het mogelijk via een evoluerende interpretatie van bestaande begrippen, enige greep te houden op de omgang met persoonsgegevens. De spanningen nemen evenwel toe.
De evaluatie richt zich vervolgens in het bijzonder op de ontwikkeling van gedragscodes als vorm van collectieve zelfregulering. Deze worden uitvoerig besproken en geanalyseerd. Hoewel een aantal frictiepunten aanwijsbaar zijn, is het algemene oordeel daarover positief. De Nederlandse wet blijkt op dit punt terecht model te hebben gestaan voor de EG-richtlijn. Daarnaast komt het Besluit genormeerde vrijstelling, het Afbakeningsbesluit, het begrip «houder» en de reglements-, en aanmeldingsplicht aan de orde. Een aantal andere onderwerpen, waaronder de werking van de materiële bepalingen van de WPR, is niet aan de orde gekomen.
De evaluatie wijst in het algemeen op een gebrekkige inbedding van de WPR in het overige Nederlandse recht. Deze constatering wordt ondersteund door de schaarste aan jurisprudentie krachtens deze wet. De bescherming van de persoonlijke levenssfeer bij de omgang van persoonsgegevens is vaak vorm gegeven op basis van het gewone civiele recht, in de regel krachtens het leerstuk van de onrechtmatige daad, dan wel in de publieke sector krachtens beginselen van behoorlijk bestuur of de Wet openbaarheid van bestuur. In het onderhavige wetsvoorstel is getracht deze aansluiting beter te doen plaatsvinden. We wijzen op een aantal elementen.
Het wetsvoorstel bevat geen sluitend stelsel van concrete materiële normen over wat wel en wat niet zou mogen bij de verwerking van persoonsgegevens. Weliswaar geldt voor gevoelige gegevens dat zij ingevolge de richtlijn slechts kunnen worden verwerkt indien de wet of de Registratiekamer in individuele gevallen om redenen van zwaarwegend algemeen belang dit uitdrukkelijk toestaat. Andere persoonsgegevens kunnen daarentegen worden verwerkt – afgezien van enige met name genoemde doeleinden – na een zorgvuldige afweging van de belangen van de verantwoordelijke en van de betrokkene. Artikel 8, onder f, is in dit opzicht een open norm: de afweging van belangen is opgedragen aan de verantwoordelijke. Het artikel geeft daarmee geen op het concreet geval toegespitst antwoord op de vraag of verwerking van persoonsgegevens wel of niet is toegestaan, maar vormt een kristallisatiepunt voor jurisprudentie en nadere sectorale wetgeving. De verwerking voor een ander doel

of ten behoeve van een derde moet – wederom een open norm – verenigbaar zijn met het oorspronkelijke doel. In de zich snel ontwikkelende informatiemaatschappij zou het niet goed zijn de rechtsontwikkeling op voorhand te veel vast te leggen.
Slechts waar het gaat om de systematische verwerking (mede) ten behoeve van een andere verantwoordelijke is de afweging voorbehouden aan de wetgever. De afweging moet echter ook dan voldoen aan de normen van het Verdrag inzake gegevensbescherming, alsmede aan die van de richtlijn althans wat dit laatste betreft voor zover het gaat om recht dat valt onder de Europese Gemeenschap.
De bepaling inzake de afweging van belangen heeft in zoverre een kameleontisch karakter dat de toets in rechte achteraf of een aanvaardbare afweging heeft plaatsgevonden zich kleurt naar gelang het gaat om een gegevensverwerking in de publieke, dan wel in de private sector. In het eerste geval wordt getoetst of bij de afweging is voldaan aan de bestuursrechtelijke beginselen van behoorlijk bestuur; in het tweede geval of de zorgvuldigheid die volgens het ongeschreven recht in het maatschappelijk verkeer betaamt. In het eerste geval gaat het ook om de verticale werking van grondrechten, terwijl het in tweede geval gaat om de indirect daarvan afgeleide horizontale werking van deze rechten.
In die zin verwijst op dit wezenlijk onderdeel het onderhavige wetsvoorstel naar het andere recht, met dien verstande dat het voorschrijft dat het belang van de betrokkene uitdrukkelijk als zodanig gewicht in de schaal legt en het gebruik verenigbaar moet zijn met het oorspronkelijk doel van de gegevensverwerking. De voorschriften die de transparantie van de gegevensverwerking beogen, dienen het doel dat de betrokkene in rechte de gemaakte afweging aan de orde kan stellen. Anders dan bij de open normen van het materiële recht, zijn op dit punt de voorschriften strikt.
Anders dan in de WPR voorziet het wetsvoorstel in een gedifferentieerd stelsel van rechterlijke toetsing. Met de totstandkoming van de Awb ligt het in de rede, althans bepaalde beslissingen van de overheid volgens de procedures van die wet te laten verlopen. In de particuliere sector blijft de rechtspraak bij de civiele rechter. Het gevaar voor uiteenlopende jurisprudentie achten wij niet groot, daar de concretisering van de open normen toch dient plaats te vinden tegen de achtergrond van de algemene noties die enerzijds in het bestuursrecht, anderzijds in het civiele recht gelden.
Zoals gezegd is een aantal bijzondere onderwerpen uitvoeriger besproken.
Wat betreft de gedragscodes zijn de volgende details gewijzigd ten opzichte van de WPR. De inspraak van betrokkenen, zoals voorgeschreven in artikel 15, tweede lid, WPR, blijkt niet goed van de grond te zijn gekomen. De groepen van personen van wie de gegevens in een registratie werden opgenomen, bleken ontoereikend georganiseerd. Dit onderzoeksresultaat heeft ermede toe bijgedragen dat de verplichting van de Registratiekamer betrokkenen in de gelegenheid te stellen de code van commentaar te voorzien, is komen te vervallen. Uiteraard laat dit onverlet dat waar hiertoe aanleiding bestaat, organisaties van betrokkenen wel worden ingeschakeld.
Een tweede aspect is het tot dusver ontbreken van een beroep op de rechter. Een dergelijk beroep is in artikel 15, zevende lid, WPR uitgesloten. Teneinde een controverse te vermijden over de vraag of de (weigering van een) goedkeuring van een gedragscode moet worden aangemerkt als een besluit in de zin van artikel 1.3 Awb, is in het onderhavig wetsvoorstel een dergelijk beroep uitdrukkelijk opengesteld, zonder overigens wijziging te brengen in het karakter van een gedragscode van een staand advies aan de rechter.
De in de evaluatie besproken problemen met het Besluit genormeerde vrijstelling zullen grotendeels worden ondervangen doordat de vrijstel-

lingen in mindere mate kunnen worden genormeerd. Artikel 29, tweede lid, staat slechts een beperkt aantal criteria toe aan de hand waarvan gegevensverwerkingen worden beschreven als zijnde vrijgesteld van de meldingsplicht. Overigens ligt het in de bedoeling van deze vrijstellingsmogelijkheid op ruime schaal gebruik te maken. Deze doelstelling is ook in deze zin bij de voorbereiding van de richtlijn besproken.
Het Afbakeningsbesluit blijkt onwerkbaar. Onder de WPR was dit nodig om de werking van de materiële normen en de transparantie te differentiëren (melden via een formulier of een reglement). Daar publieke en private sector thans in dit opzicht op één lijn worden gesteld, is een afbakening niet meer nodig. Wel keert het onderscheid terug in de rechterlijke procedure in geval van een geschil. De andere invulling van materiële normen (samenhangend met de verticale of horizontale werking van grondrechten), krijgt door de verschillende jurisprudentie gestalte, zoals hierboven reeds is uiteengezet. De afbakening is dan evenwel niet één die eigen is aan het privacyrecht, doch is er één van de Awb. Aldus vindt wederom een betere inbedding in het overige recht plaats.
Het begrip «houder» is conform de aanbeveling vervangen door een ander woord: de «verantwoordelijke». In het begrip zelf ligt besloten dat steeds een rechtssubject aanspreekbaar is op de verwerking van persoonsgegevens. Eén van de algemene doelstellingen van het informaticarecht is immers de situatie te vermijden dat personen schade ondervinden van geautomatiseerde gegevensverwerking zonder dat een ander rechtssubject daarop aanspreekbaar is. Verder is in de toelichting duidelijk gemaakt dat in het openbaar bestuur daarmee wordt gedoeld op degene die in publiekrechtelijke zin bevoegd is, terwijl in de private sector de verantwoordelijke slechts op concernniveau kan worden aangenomen in het geval het daadwerkelijk gaat om gegevensverwerking voor het concern, zulks te onderscheiden van gegevensverwerking uitsluitend of in hoofdzaak ten behoeve van de dochters.
De gebleken problemen bij de aanmelding van persoonsregistraties bij de Registratiekamer, zijn mede aanleiding geweest in de richtlijn de mogelijkheid op te nemen om te melden bij een eigen toezichthouder. Daarmee wordt bovendien een verdere spreiding van de expertise inzake gegevensbescherming bevorderd, evenals de naleving van de meldingsplicht. De zelfregulering wordt hiermee gediend.

14.3. De sociaal-wetenschappelijke evaluatie

De sociaal-wetenschappelijke evaluatie mondt uit in een aantal aandachtspunten voor de wetgever. De bespreking daarvan begint op blz. 56 van het rapport. Aan de hand daarvan wordt rekenschap afgelegd in hoeverre en hoe met de resultaten van de evaluatie wordt rekening gehouden, voor zover de onderwerpen niet in het voorgaande reeds aan de orde kwamen.
Het eerste punt is de aanbeveling van een korte, bondige wet tegen de achtergrond van de wel gestelde vraag of een aparte privacywet überhaupt wel nodig is. Veel privacyrecht is immers al in andere wetten geregeld.
Achter dit punt gaat een groot aantal vooronderstellingen schuil. De eerste is dat de WPR dan wel het onderhavige wetsvoorstel zou bepalen welke persoonsgegevens onder bepaalde omstandigheden wel en welke niet zouden mogen worden opgeslagen. Het gaat daarbij dus om de materiële normen. We wezen er hierboven reeds op dat, afgezien van de gevoelige gegevens, er geen verbod is op de verwerking van persoonsgegevens. Met of zonder wet, zowel in de publieke als in de private sector hebben verantwoordelijken die gegevens verwerken zorgvuldigheid jegens de betrokkenen te betrachten. De open normen schrijven slechts voor dat daarbij het belang van de betrokkene uitdrukkelijk moet worden gewogen aan de hand van een aantal algemene gezichtspunten en een doelafwijking verenigbaar moet zijn met het oorspronkelijk doel. Op het

punt van de materiële regelgeving is het wetsvoorstel naar ons oordeel bondig. Sectorale wetgeving kan in aanvulling daarop bijzondere regels geven. Een sluitend systeem van regels over de verwerking van persoonsgegevens zal wel nooit mogelijk zijn en is in ieder geval gegeven de snelle technologische ontwikkelingen van dit moment niet wenselijk.
Gevoelige gegevens worden als zodanig aangemerkt omdat zij naar hun aard eerder een inbreuk kunnen maken op de persoonlijke levenssfeer. Bij de systematische verstrekking aan derden, al dan niet met behulp van een identificatienummer, spelen overeenkomstige overwegingen. Derhalve is ook daarvoor bepaald dat steeds een wettelijke grondslag aanwezig is. Artikel 10, eerste lid, van de Grondwet eist immers een uitdrukkelijke wettelijke machtiging bij inbreuken op de persoonlijke levenssfeer.
Het onderhavige wetsvoorstel haakt dus aan bij open normen in het civiele en administratieve recht. De verwerkelijking van het recht van de betrokkenen vereist echter bijzondere voorzieningen. De verwerking van persoonsgegevens, zeker wanneer het gevaar bestaat dat deze onrechtmatig plaatsvindt, speelt zich af in het verborgene, wanneer niet in het procedurele vlak aanvullende wettelijke voorzieningen worden getroffen. De schadetoebrengende actor is anders bezwaarlijk in beeld te brengen. De verschillende bepalingen gericht op de transparantie van de gegevensverwerking strekken ertoe dit euvel te keren. Ook die zijn echter ontoereikend wanneer niet ten minste wordt voorzien in een apart toezichthoudend orgaan. Ook elders binnen de wetgeving zijn voor de handhaving van regels waarvan de mate van naleving zich aan de waarneming in de openbaarheid onttrekt, toezichthoudende organen met bijzondere bevoegdheden in het leven geroepen. De transparantie omvat verder verschillende aspecten: de informatie aan de betrokkene dat gegevens over hem worden verwerkt, de melding aan de toezichthouder van niet vrijgestelde gegevensverwerkingen en het recht op kennisneming door de betrokkene van gegevens over hem. De regeling daarvan in een afzonderlijke wet, is een te rechtvaardigen keuze. Overigens gaat het hier om elementen die grotendeels uit de richtlijn voortvloeien.
Een aparte bespreking vergt de eis van helderheid. Wij pretenderen niet deze volledig te brengen. Het recht op bescherming van persoonsgegevens in de aanzwellende informatiemaatschappij vergt een zich geleidelijk ontwikkelende dogmatiek voor een nieuw rechtsgebied dat nog maar in de kinderschoenen staat. Het is een gelukkige omstandigheid dat de informatietechnologie de westerse landen in gelijke mate treft. De gebundelde expertise op Europees niveau kan worden aangesproken bij de ontwikkeling van dit jonge rechtsgebied. Dit is aanvankelijk gebeurd in het Verdrag inzake gegevensbescherming uit 1981 van de Raad van Europa. Dit heeft brede instemming gekregen van de Lid-staten. Een vervolg daarop is de EG-richtlijn die in het onderhavig wetsvoorstel wordt geïmplementeerd. Telkens blijkt onder experts dat de technische ontwikkelingen het recht voor uitdagingen stellen die slechts door de geleidelijke ontwikkeling van nieuwe rechtsbegrippen en daarmee verbonden rechten sui generis het hoofd kunnen worden geboden. Een uitgekristalliseerd juridisch begrippenapparaat en een heldere, dat wil zeggen vaststaande invulling daarvan in de juridische dogmatiek, zal pas beschikbaar zijn wanneer ook de informatietechnologische ontwikkelingen in een rustiger vaarwater zijn gekomen. Wij onderschrijven evenwel dat ook onder deze omstandigheden de regels zo helder mogelijk moeten zijn. Willen de regels echter meer zijn dan vrijblijvende, vrome beginselen, zonder de gerechtvaardigde gegevensverwerkingen onnodig te beperken, dan valt niet te ontkomen aan begrippen die een daadwerkelijk kristallisatiepunt voor rechtspraktijk en jurisprudentie kunnen zijn, met alle daaraan inherente rechtsonzekerheid.
Het tweede punt bepleit in de privacyregulering aan te sluiten bij potentiële risico's van gegevensverwerking in plaats van bij maatschappe-

lijke sectoren, zoals thans nog in het Afbakeningsbesluit, het Besluit genormeerde vrijstelling en het Besluit gevoelige gegevens gebeurt. De richtlijn biedt de mogelijkheid met dit aandachtspunt in vergaande mate rekening te houden. De wettelijke afbakening in het publieke en private recht is zowel op het gebied van de materiële normen als op dat van de meldings- en reglementsplicht opgeheven. Slechts keert deze terug bij de rechtsgang, doch dan wordt aangesloten bij de algemene regels van de Awb. Voorts worden de mogelijkheden om vrijgestelde verwerkingen nader te normeren beperkt.
Verder wordt conform de richtlijn bijzondere aandacht besteed aan gevoelige gegevens. Het betreft hier gegevens die naar hun aard een groter risico voor de persoonlijke levenssfeer betekenen. Verwezen zij naar paragraaf 2 van hoofdstuk 2 van het wetsvoorstel. Daarenboven wordt in artikel 31 aan de Registratiekamer de bevoegdheid toegekend om voorafgaand onderzoek te doen naar gegevensverwerkingen die een bijzonder risico opleveren voor de persoonlijke levenssfeer van de betrokkene. Deze bevoegdheid vloeit eveneens voort uit de richtlijn.
Het derde punt bepleit technologie-onafhankelijke en flexibele context-gebonden normering en beleidsinstrumentatie als uitgangspunt. Volledig technologie-onafhankelijke wetgeving behoort niet tot de reële mogelijkheden. Het enige dat kan worden nagestreefd is zo technologie-onafhankelijk mogelijke regelgeving. Dit kan echter slechts door de ontwikkeling van een eigen juridische dogmatiek, die zoveel mogelijk afstand neemt van de technische ontwikkelingen. Hierboven is echter reeds geschetst dat juist de juridische ontwikkelingen om enige greep te houden op de techniek voor zover deze de menselijke waardigheid bedreigt, zoveel aanleiding geven tot onzekerheid. Er moet daarom een tussenweg worden bewandeld tussen twee met elkaar onverenigbare uitersten. Aan de ene kant staat het ideaal van regelgeving die helder en duidelijk is: met een nieuwe technologie gelden de volgende gedrags-voorschriften. Aan de andere kant het ideaal van technologie-onafhankelijke regelgeving, die echter in het duister tast omdat nog volstrekt onduidelijk is hoe de techniek zich zal ontwikkelen.
Het vierde punt bepleit een meer omvattende invulling van de eigen verantwoordelijkheid van verantwoordelijken en bewerkers, met name via eigen toezichthouders. Elders is uiteengezet dat de optie in de richtlijn om eigen toezichthouders mogelijk te maken, in het onderhavige wetsvoorstel is uitgewerkt. De aanmelding van niet vrijgestelde registraties kan dan volgens intern te bepalen regels verlopen, terwijl de uitoefening door hem van zijn toezichthoudende taak minder als inmenging van buitenaf zal worden ervaren.
Het vijfde punt bepleit dat de sturingsinstrumenten om een betere privacybescherming te bereiken zich meer zouden moeten differentiëren, afhankelijk van de context waarin deze bescherming moet worden geboden. Wederom verwachten wij dat de eigen toezichthouder in dit opzicht als een nuttig intermediair tussen het eigen bedrijf of branche en de overheid zal kunnen functioneren. Ook de gedragscodes en de meldingen kunnen in dit opzicht een belangrijke functie vervullen.
Het zesde punt bepleit de positie van geregistreerden te versterken door meer betrokkenheid en medezeggenschap te stimuleren. Hoewel blijkens de totstandkoming van gedragscodes de participatie van geregistreerden moeizaam gestalte kon worden gegeven en ook gewezen is op gebrekkige jurisprudentievorming als gevolg van slechts schaarse klachten, zouden wij een verdergaande betrokkenheid van geregistreerden toejuichen. Het ligt echter niet op de weg van de wetgever om de burgers belangstelling voor een bepaald onderwerp af te dwingen. Dit ligt binnen de vrijheids-sfeer van het individu. Op een enkel, doch belangrijk aspect hebben wij evenwel aansluiting gezocht bij bestaande structuren. De betrokkenheid van werknemers bij de vormgeving van hun privacy in relatie tot de

werkgever hebben wij in al zijn aspecten neergelegd in de Wet op de ondernemingsraden.
Het zevende punt betreft de rol van de Registratiekamer. Met name de verbreding van het maatschappelijk draagvlak van dit zelfstandig bestuursorgaan werd bepleit. De beide evaluaties hebben duidelijk gemaakt dat de ontwikkeling van het privacyrecht tot dusver zich in relatief isolement heeft voltrokken. Daarmee is ook de Registratiekamer slechts in beperkte mate in maatschappelijke discussies betrokken. De verschillende in het onderhavige wetsvoorstel opgenomen extra bevoegdheden van de kamer, alsmede de mogelijkheid van rechterlijke toetsing op het gebruik daarvan, zullen het draagvlak van de rechtsvorming op dit gebied naar onze verwachting vergroten. Ook de interactie tussen de Registratiekamer en de eigen toezichthouders in verschillende bedrijven en branches, zal naar onze verwachting een verbreding van de groep van betrokken personen bij de rechtsontwikkelingen op dit gebied tot gevolg hebben.
Het achtste punt ten slotte betreft de inschakeling van informatietechnologie ter bescherming van de privacy. Een aantal regels zal stellig kunnen worden geëffectueerd met technische middelen. Daartoe moeten er wel dergelijke regels zijn. Van een substitutie van regels door techniek verwachten wij daarom weinig heil. Cryptografie zal in de naaste toekomst veel gebruik van informatie- en communicatietechnologie goed, zij het nooit absoluut, kunnen beschermen tegen onrechtmatige ingrepen. Het is nodig tevens te vermelden dat techniek niet alleen beschikbare persoonsgegevens goed kan beschermen, doch ook het vergaren van persoonsgegevens kan voorkomen. Het ontwerp van de EG-richtlijn van 13 juni 1994, COM (94) 128, SYN 288, over de bescherming van persoonsgebonden gegevens en van de persoonlijke levenssfeer in het kader van digitale telecommunicatienetwerken, bevat in dit opzicht een belangrijke bepaling. Artikel 8, eerste lid, verplicht telecommunicatie-organisaties abonnees een technische voorziening aan te bieden waardoor deze op eenvoudige wijze per oproep de identificatie van het nummer dat zij gebruiken, onmogelijk kunnen maken. Personen kunnen daardoor anoniem zaken doen via de elektronische snelweg. Deze voorziening kan slechts worden doorbroken in geval van een bevoegd gegeven bevel tot het onderscheppen en verstrekken van de desbetreffende gegevens met het oog op de opsporing van strafbare feiten of in het belang van de staatsveiligheid. Daar waar bij voorbeeld digitale betalingen in de naaste toekomst over de elektronische snelweg kunnen plaatsvinden, is bij contante betaling de uitwisseling van persoonsgegevens niet meer nodig. De persoonsgerichte serviceverlening van bedrijven aan hun klanten blijft mogelijk in situaties waarin deze klanten geen gebruik maken van de beschreven technische voorziening, noch op andere wijze daartegen bezwaar maken.

15. Verhouding tot andere wetten

In paragraaf 5 gingen wij in het algemeen reeds in op de verhouding van het wetsvoorstel tot andere wetten. Het is evenwel nodig aparte aandacht te besteden aan de verhouding tot enige bijzondere wetten. Voor een uitgebreidere beschouwing inzake de verhouding van het wetsvoorstel tot de Wet inzake de geneeskundige behandelingsovereenkomst zij verwezen naar de parlementaire behandeling van laatstgenoemde wet (kamerstukken II 1990/91, 21 561, nr. 6, blz. 6 e.v., en 1991/92, 21 561, nr. 11, blz. 4 e.v.). Hetgeen aldaar is opgemerkt over de verhouding tussen WGBO en WPR is van overeenkomstige toepassing.

15.1. Verhouding tot de Wet openbaarheid van bestuur

In beginsel geldt dat de WBP alleen niet van toepassing is in de gevallen

dat daarin uitdrukkelijk in de WBP is voorzien (bijvoorbeeld artikel 2 WBP). In een aantal gevallen bevat de bijzondere wet echter een uitputtende regeling ten aanzien van bijvoorbeeld de openbaarmaking van gegevens. In die gevallen zal de bijzondere wet kunnen worden aangemerkt als een specialis ten opzichte van de generalis WBP en prevaleert om die reden de regeling in de bijzondere wet. De in de WOB geregelde informatieverplichtingen van de bestuursorganen zijn een voorbeeld van een dergelijke uitputtende regeling. Deze regeling geeft als het ware uitvoering aan het meer algemene voorschrift van artikel 8, onderdeel c, van de WBP. Gezien het uitputtende karakter van de bepalingen in de WOB prevaleren zij boven artikel 8, onderdeel c, van de WBP. Het recht op kennisneming daarentegen is niet geregeld in de WOB. Ten aanzien van dit recht gelden derhalve de bepalingen van de WBP.
De WOB kent geen expliciete grondslag voor de verwerking van gevoelige gegevens. De huidige bepaling van artikel 10, tweede lid, onder e, van de WOB biedt onvoldoende passende waarborgen in die zin van artikel 8, vierde lid, van de richtlijn. Een aanvullende uitzonderingsgrond die specifiek op gevoelige gegevens ziet is noodzakelijk. Hierin zal worden voorzien in de ontwerp Aanpassingswet Wbp.

15.2. Verhouding tot de Archiefwet 1995

Bijzondere aandacht verdienen de archiefbescheiden die naar een archiefbewaarplaats zijn overgebracht ingevolge de Archiefwet 1995. Het gaat daarbij met name om geselecteerde archiefbescheiden van de Nederlandse overheid die in beginsel ouder zijn dan twintig jaar. De selectiecriteria zijn: de waarde die de bescheiden vertegenwoordigen voor het nationale culturele erfgoed, het belang van de bescheiden voor de overheidsorganen zelf, voor recht- of bewijszoekenden en voor historisch onderzoek.
Archiefbescheiden in een archiefbewaarplaats, afkomstig van de overheid of van particulieren, kunnen persoonsgegevens bevatten. Bij de totstandkoming van de WPR zijn de persoonsregistraties die zich in de overgebrachte archiefbescheiden bevinden, uitgesloten van de werking van de WPR (artikel 2, eerste lid, onder d, van de WPR). De reden daarvan was dat de Archiefwet 1962 bepalingen bevatte over de openbaarheid van archiefbescheiden die naar een archiefbewaarplaats zijn overgebracht. Eenzelfde regeling staat thans in de Archiefwet 1995. Op grond van artikel 15 van de Archiefwet 1995 kunnen aan die openbaarheid beperkingen worden gesteld, onder meer met het oog op de eerbiediging van de persoonlijke levenssfeer. Het was onnodig daarnaast de WPR van toepassing te verklaren. Artikel 3 van de richtlijn biedt echter geen ruimte meer persoonsgegevens die voorkomen in archiefbewaarplaatsen integraal uit te zonderen van het onderhavige wetsvoorstel. Uitgangspunt is dat met name de artikelen waarin de beginselen betreffende de rechtmatigheid van de gegevensverwerking zijn neergelegd, onverkort van toepassing zijn op iedere verwerking van persoonsgegevens, ongeacht waar deze zich afspeelt in de maatschappij. Daarentegen is het wel mogelijk bepaalde, andere artikelen buiten toepassing te verklaren indien deze in de praktijk onnodig beknellend zijn en met het oog op het belang dat ze dienen onevenredig zwaar belastend zijn. In dit kader kan worden gewezen op de informatieverplichtingen van de houder en de aanmeldingsplicht. Hieronder zal nader op het een en ander worden ingegaan.
Iedere verwerking van persoonsgegevens die deel uitmaken van archiefbescheiden als bedoeld in de Archiefwet 1995 valt onder artikel 8, onder c en e, van de WBP. Binnen de daar gestelde randvoorwaarden is het mogelijk zodanige persoonsgegevens te verwerken. De verwerkingshandelingen die bij archiefbescheiden in archiefbewaarplaatsen als essentieel moeten worden beschouwd, zijn: bewaren (voor in beginsel

onbepaalde tijd) en, desgevraagd, ter raadpleging verstrekken. Aan het langdurig bewaren van de in de archiefbewaarplaatsen opgenomen persoonsgegevens staat het onderhavige wetsvoorstel niet in de weg (artikel 10). Een goed functionerend «geheugen van de overheid» is een erkend publiek belang. De inspanning die het archiefwezen moet leveren ter bescherming van de persoonlijke levenssfeer van de betrokkenen dient tot deze publieke taak in een redelijke verhouding te staan. In dit verband geldt dat aan de inspanningsverplichtingen waar artikel 11, tweede lid, van het wetsvoorstel op doelt, is voldaan indien de bescheiden zijn geselecteerd volgens de archiefwettelijke selectiecriteria. De toetsing op de juistheid en nauwkeurigheid zal zelfs achterwege kunnen blijven wanneer de bescheiden (waaronder persoonsgegevens) worden geselecteerd op historisch-wetenschappelijke gronden. Ook onjuiste persoonsgegevens kunnen op die gronden interessant en behoudenswaardig zijn. De juistheid van gegevens moet in zekere zin worden beoordeeld in de context waarin ze worden verwerkt. Het hierboven geschetste publieke belang is een zwaarwegend algemeen belang als bedoeld in artikel 16.

In het ingevolge de aanpassingswetgeving nog voor te stellen nieuwe artikel 14, tweede lid, van de Archiefwet 1995 zal een uitdrukkelijke wettelijke grondslag worden neergelegd voor de verwerking van bijzondere gegevens als bedoeld in artikel 16 van dit wetsvoorstel in archiefbescheiden in de archiefbewaarplaatsen. Het eerder vermelde artikel 15 van de Archiefwet 1995 (mogelijke beperkingen met het oog op de eerbiediging van de persoonlijke levenssfeer van betrokkenen) wordt daarnaast gehandhaafd. Aangezien de doeleinden bij bewaring ingevolge de Archiefwet 1995 altijd dezelfde (wettelijke) doeleinden zijn, die bovendien geacht mogen worden bij het publiek bekend te zijn, zullen verwerkingen van persoonsgegevens in de archiefbescheiden worden vrijgesteld van de aanmeldingsplicht als bedoeld in artikel 29. Een aanmeldingsverplichting zou met het oog op het belang dat daarmee wordt gediend een onevenredig zware belasting betekenen voor de verantwoordelijke. Om die reden zijn de persoonsgegevens die deel uitmaken van archiefbescheiden die volgens de archiefwettelijke regels zijn overgebracht naar een archiefbewaarplaats (in de regel twintig jaar nadat zij zijn verzameld), eveneens uitgezonderd van de werking van artikel 34 (artikel 44, tweede lid).

De artikelen 35 e.v. van het wetsvoorstel zijn in beginsel wel op archiefbescheiden van toepassing. Voor zover het gaat om de toepassing van artikel 35 geldt in het algemeen dat verzoeken om kennisneming niet ongericht mogen zijn. Onder omstandigheden kan dit neerkomen op misbruik van recht. Zie in dit verband ook hetgeen hierover wordt opgemerkt in de toelichting bij artikel 1, onder d. Voor archiefbescheiden die naar een archiefbewaarplaats zijn overgebracht, geldt overigens dat zij in beginsel openbaar zijn. Van dergelijke bescheiden kan dus een ieder op grond van de Archiefwet 1995 kennisnemen. Hoewel het archiefwezen er volledig op ingericht is om aan dergelijke verzoeken tot kennisneming te voldoen, geldt ook hier dat die dienstverlening niet onbegrensd is. Dat geldt zowel voor verzoeken die op de Archiefwet 1995 zijn begaseerd als voor verzoeken die hun basis vinden in artikel 35 van het onderhavige wetsvoorstel.

De betrokkene heeft voorts op grond van artikel 36 van dit wetsvoorstel recht op correctie in geval van onrechtmatige verwerking. Ondanks het ontbreken van een wettelijke plicht daartoe zijn dergelijke verzoeken door het archiefwezen tot op heden altijd in behandeling genomen, zij het dat in geval van honorering van het verzoek, gegevens niet worden verwijderd of vernietigd, maar dat de mogelijkheid wordt geboden aan de betrokkene zijn eigen lezing aan de desbetreffende stukken toe te voegen. Deze praktijk zal onder artikel 36 van dit wetsvoorstel kunnen worden voortgezet.

16. Voorlichting

Verschillende geledingen van de maatschappij, waaronder het bedrijfsleven en de lagere overheden, zullen te maken krijgen met de voorgestelde wetgeving en zullen bestaande procedures dienen aan te passen aan de wijzigingen ten opzichte van de Wet persoonsregistraties.
Evenals ter gelegenheid van de invoering van de Wet persoonsregistraties is gebeurd, zal ook aan de invoering van dit wetsvoorstel ruime bekendheid via de media, waaronder de televisie en dagbladpers, worden gegeven. De Registratiekamer ontwikkelt een hiervoor plan. Verder zal een instructieve folder worden vervaardigd over verschillende aspecten van de wet, bij voorbeeld één voor personen over wie gegevens worden opgeslagen en die informatie willen hebben over hun rechten en één voor degenen die persoonsgegevens over anderen verwerken.
Vooruitlopend op de inwerkingtreding van de wet is het wetsvoorstel via de Justitie-site op Internet bekend gemaakt. Via een daarvoor geopend E-mailadres kunnen vragen over de toepassing van de wet worden gesteld. In overleg met de Registratiekamer zal worden bezien op welke wijze de gestelde vragen zullen worden beantwoord.
De voorbereiding van het een en ander is reeds ter hand genomen.
Helaas zal het niet mogelijk zijn de aanmeldingen van registraties die hebben plaatsgevonden onder de Wet persoonsregistraties, categoraal aan te merken als aanmeldingen onder de nieuwe wet, daar de elementen van de aanmelding niet dezelfde zijn. Zelfs voor de publieke sector, waar onder de Wet persoonsregistraties nog reglementen moesten worden opgesteld, dienen ook onder het voor deze sector vereenvoudigde regime van meldingen, andere elementen in de berichtgeving aan de Registratiekamer te worden opgenomen. Vergelijking van artikel 20 van de Wet persoonsregistraties (artikel 24, derde lid, verwijst voor de private sector wat betreft de te melden elementen naar dit artikel) met het voorgestelde artikel 28, eerste lid, van de Wet bescherming persoonsgegevens laat zien dat (1) de ontvangers of categorieën van ontvangers, (2) voorgenomen overdrachten naar landen buiten de Europese Unie en (3) een algemene beschrijving van de beveiliging moet worden gemeld, waar zulks onder de Wet persoonsregistraties nog niet het geval was. Daar staat tegenover dat een aantal elementen van de melding, onderscheidenlijk van de onderwerpen die in een reglement moesten worden geregeld, komen te vervallen. Hoewel op de langere duur aldus er een lastenverlichting optreedt, houdt dit evenwel voor de overgangsfase een hernieuwde melding in. De voorlichting zal in het bijzonder aan dit aspect aandacht moeten besteden.

ARTIKELSGEWIJZE TOELICHTING

HOOFDSTUK 1 ALGEMENE BEPALINGEN

Artikel 1

Onderdeel a

Het begrip «persoonsgegevens» wordt in artikel 2, onder a, van de richtlijn omschreven als «alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon». Deze omschrijving sluit aan bij die van het begrip «personal data» in het Dataprotectieverdrag waar wordt gesproken van «any information relating to an identified or identifiable individual».
Ten einde de terminologie ten opzichte van artikel 1 van de WPR niet onnodig te doorbreken is het begrip omschreven in het enkelvoud en is de term «gegeven» gehandhaafd om het begrip «informatie» van de richtlijn

om te zetten. Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon moeten als persoonsgegevens worden beschouwd. In de WPR was nog bepaald dat het moet gaan om een individuele natuurlijke persoon. Gezien de bewoordingen van de richtlijn lijkt de term «individueel» overbodig en is deze geschrapt zonder daarmee een wijziging te beogen ten opzichte van artikel 1 van de WPR.
De definitie bevat een aantal elementen die expliciet aandacht vragen. Allereerst moet het gaan om informatie «betreffende» een natuurlijke persoon («any information relating to»). Voorts moet deze persoon zijn geïdentificeerd of althans identificeerbaar zijn («identified or identifiable»). Als er aan één van beide elementen niet is voldaan, dan is er geen sprake van persoonsgegevens en is het wetsvoorstel niet van toepassing. Hoewel het gaat om twee onderscheiden beoordelingsmomenten, staan zij niet los van elkaar.
Het begrip «persoonsgegeven» van de WPR sluit inhoudelijk aan op de omschrijving in artikel 1 van de WBP, maar is wat anders omschreven, namelijk een gegeven dat herleidbaar is tot een individuele natuurlijke persoon. Bovengenoemde elementen liggen besloten in de term herleidbaar. Van herleiding is sprake indien een gegeven informatie verschaft over een identificeerbaar persoon. Omdat de term «herleidbaar» in de praktijk tot misverstanden heeft geleid, wordt – in aansluiting op het advies van de Registratiekamer – deze term in het onderhavige wetsvoorstel niet meer gehanteerd.
Hieronder wordt ingegaan op bovengenoemde elementen van het begrip «persoonsgegeven».

(1) Gegevens die betrekking hebben op een persoon

Allereerst is voor het begrip «persoonsgegeven» relevant of de gegevens informatie over een persoon bevatten. In veel gevallen, zoals bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen, zal dit uit de aard van de gegevens voortvloeien. In andere gevallen zal mede aandacht moeten worden besteed aan de context waarin het gegeven wordt vastgelegd en gebruikt. Als gegevens mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, moeten die gegevens als persoonsgegevens worden aangemerkt. Het (maatschappelijk) gebruik dat van gegevens wordt gemaakt is dus mede-bepalend voor de beantwoording van de vraag of sprake is van een persoonsgegeven.
De richtlijn biedt geen aanknopingspunt voor een beperking van het begrip «persoonsgegevens» tot rechtens relevante informatie, zoals soms wel is bepleit. In deze opvatting zou het bij persoonsgegevens slechts gaan om gegevens die juridische consequenties hebben voor de betrokkene. Daarmee wordt voorbijgegaan aan de mogelijke gevolgen van het gebruik van op individuele personen betrekking hebbende informatie voor de wijze waarop deze in het maatschappelijk verkeer worden bejegend. Deze gevolgen kunnen ook optreden zonder dat rechtstreeks wordt ingegrepen in de rechtspositie van de betrokkene. Om die reden dient het begrip «persoonsgegevens» ruimer te worden uitgelegd in de zin zoals in de vorige alinea reeds werd aangegeven. Een beperktere uitleg zou bovendien op gespannen voet komen met de richtlijn.
Gegevens die een neerslag vormen van een over een bepaalde persoon genomen beslissing, kunnen worden beschouwd als een deze persoon betreffend persoonsgegeven. Ook gegevens die niet direct betrekking hebben op een bepaalde persoon, maar bijvoorbeeld op een produkt of een proces, kunnen soms over een bepaalde persoon informatie verschaffen, bij voorbeeld wanneer daarmee de arbeidsproduktiviteit van een werknemer gemakkelijk in kaart kan worden gebracht. Tevens dienen telefoonnummers (Registratiekamer 8 juli 1993, 93.A.002), kentekens van

auto's (Registratiekamer 15 oktober 1993, 92.F.008) en postcodes met huisnummers (Registratiekamer 21 juni 1996, 95.O.043) onder omstandigheden als een persoonsgegeven te worden aangemerkt. Het gegeven dat een bepaalde persoon aangifte heeft gedaan van diefstal van een voertuig, wanneer hij daarmee als slachtoffer van een strafbaar feit wordt aangemerkt, zal ook als een op die persoon betrekking hebbend persoonsgegeven moeten worden aangemerkt.
Gegevens die naar hun aard niet op personen betrekking hebben noch – gezien de context waarin ze worden verwerkt – mede bepalend zijn voor de wijze waarop een persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, zijn geen persoonsgegevens. Gegevens die uitsluitend voorwerpen aanduiden, bijvoorbeeld gestolen goederen of identiteitsbewijzen, zijn geen persoonsgegevens indien deze geen informatie bevatten met behulp waarvan personen in hun maatschappelijke positie kunnen worden geraakt. Het gaat dan om zuivere objectgegevens. Hetzelfde geldt voor gegevens die onroerende zaken of andere registergoederen identificeren. Het feit dat deze zaken via een openbaar register zoals de kadastrale registratie tot een individuele natuurlijke persoon kunnen worden herleid, doet hieraan op zichzelf niet af. Het zou anders zijn indien bij een verstrekking van dergelijke objectgegevens (bijvoorbeeld overzichten van panden en erven met aanvullende informatie over de omvang en de aard ervan) op CD-ROM, een aanvullend gegeven omtrent personen is verbonden, waardoor de zoekbaarheid op personen mogelijk wordt. Gegevens van een netwerkbeheerder over het gebruik van het netwerk via aansluitpunten teneinde het goed functioneren van het netwerk te waarborgen, zijn geen persoonsgegevens zolang elke reële mogelijkheid is uitgesloten dat die gegevens worden gebezigd om het gebruik van het netwerk door individuele personen in ogenschouw te nemen.
Niet elk technisch of toevallig verband tussen een gegeven en een persoon is dus voldoende om dat gegeven een persoonsgegeven te doen zijn. Anders dan de Registratiekamer in haar advies stelt is niet vereist dat iedere mogelijkheid de gegevens met betrekking tot personen te gebruiken, is uitgesloten. Is deze mogelijkheid weliswaar theoretisch aanwezig maar is ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt. Indien het daarentegen mogelijk is de gegevens te gebruiken bij voorbeeld om fraude op te sporen, dan is er sprake van persoonsgegevens. Daarbij is niet relevant of de bedoeling de gegevens voor dat doel te gebruiken, ook aanwezig is. Er is reeds sprake van een persoonsgegeven wanneer het gegeven voor een dergelijk op de persoon gericht doel, kan worden gebruikt.
Gegevens die betrekking hebben op overledenen of rechtspersonen, zijn geen persoonsgegevens als bedoeld in het onderhavige artikel. Hebben deze gegevens echter eveneens betrekking hebben op nog levende, natuurlijke personen en kunnen zij mede bepalend zijn voor de wijze waarop deze in het maatschappelijk verkeer worden beoordeeld of behandeld, dan zijn zij wel weer een persoonsgegeven. Dit gold eveneens onder de WPR.

(2) De identificeerbaarheid van een persoon

De identificeerbaarheid van de persoon is het tweede element dat bepalend is voor de vraag of sprake is van een persoonsgegeven. Uitgangspunt is dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Twee factoren spelen hierbij een rol: de aard van de gegevens en de mogelijkheden van de verantwoordelijke om de identificatie tot stand te brengen.

a. De aard van de gegevens

Een persoon is identificeerbaar indien sprake is van gegevens die alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor een bepaalde persoon dat deze aan de hand daarvan kan worden geïdentificeerd. Artikel 2, onder a, van de richtlijn bepaalt dat als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

In dit kader kan worden onderscheiden tussen direct en indirect identificerende gegevens.

Van direct identificerende gegevens is sprake wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is. Direct identificerende gegevens zijn gegevens als naam, adres, geboortedatum, die in combinatie met elkaar dermate uniek en dus kenmerkend zijn voor een bepaalde persoon dat deze in brede kring met zekerheid of met een grote mate van waarschijnlijkheid, kan worden geïdentificeerd. Dergelijke gegevens worden in het maatschappelijk verkeer ook gebruikt om personen van elkaar te onderscheiden.

Anders ligt dit wanneer de gegevens niet direct tot identificatie van een bepaald persoon leiden maar via nadere stappen de gegevens in verband kunnen worden gebracht met een bepaalde persoon. Dit soort gegevens heten indirect identificerende gegevens. Zij kunnen zijn ontdaan van de naam, doch onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon.

Daarnaast zijn er gegevens die zodanig uniek zijn dat zij ook identificerend zijn, zoals het sociaal-fiscaal nummer of unieke biometrische gegevens zoals stem, vingerafdruk of DNA-profiel. Zo zijn biometrische kenmerken omtrent een persoon, wanneer deze zijn vastgelegd op een gegevensdrager en daaraan impliciet of expliciet aanvullende informatie is verbonden, persoonsgegevens. Deze aanvullende informatie kan immers met hem in verband kunnen worden gebracht, zodra de biometrische kenmerken worden vergeleken met de kenmerken van de persoon waarvan zij afkomstig zijn.

Bij sociaal-wetenschappelijk onderzoek zal onderscheid moeten worden gemaakt tussen enerzijds gegevens met een hoog onderscheidend karakter, zoals leeftijd, woonplaats en beroep, en anderzijds gegevens met een laag onderscheidend karakter, zoals leeftijdsklasse, woonregio en beroepsklasse. Het onderscheidend vermogen van dergelijke (combinaties van) gegevens is mede afhankelijk van de context, bij voorbeeld afhankelijk van de omvang van de bevolkingsgroep waarop de gegevensverwerking betrekking heeft. Het verwijderen van de direct identificerende kenmerken biedt op zichzelf niet altijd voldoende garantie dat geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit andere bron, kan immers desondanks, soms zonder bijzonder inspanning, identificatie tot stand worden gebracht. Is echter het risico van spontane herkenning redelijkerwijs uitgesloten, dan kan worden aangenomen dat er geen sprake is van persoonsgegevens. Het is niet nodig dat de mogelijkheid van spontane herkenning absoluut wordt uitgesloten.

b. De mogelijkheden van de verantwoordelijke om identificatie tot stand te brengen

De verantwoordelijke beschikt over mogelijkheden tot identificatie en de bekendheid of beschikbaarheid van aanvullende informatie. Een absolute maatstaf is niet aan de orde: gekeken moet worden naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren. Uitgegaan moet worden van een redelijk

toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste verantwoordelijke en anderzijds om subjectivering naar bijzondere expertise (Registratiekamer 27 maart 1995, 95.V.029). Een onderzoeksinstituut als het CBS zal bijvoorbeeld gelet op zijn expertise, contacten en technische outillage, eerder in staat zijn gegevens te identificeren dan een individuele onderzoeker. Deze omstandigheid dient in de beoordeling of sprake is van een persoonsgegeven te worden meegewogen.
Wat blijkens het voorgaande voor de verantwoordelijke geldt, geldt bij het verstrekken van gegevens aan een derde uiteraard ook voor de ontvanger. Dat betekent dat de verantwoordelijke zich in een dergelijk geval zal moeten afvragen of de bewuste gegevens in handen van de ontvanger al dan niet als identificeerbaar zullen moeten worden aangemerkt. Bepalend is wat in de gegeven situatie redelijkerwijs mag worden verwacht. Naarmate een verstrekker over meer mogelijkheden beschikt om de risico's van identificatie door de ontvanger te voorzien of te beperken, mag van hem in dit opzicht meer zorgvuldigheid worden verwacht.
Bij het voortschrijden van informatietechnologie moet rekening worden gehouden met het feit dat waar voorheen wellicht nog sprake is was van een onevenredige inspanning (en dus niet van een persoonsgegeven), deze inspanning geringer wordt met het beschikbaar komen van nieuwe technieken. De desbetreffende gegevens kunnen daardoor onder het bereik van het wetsvoorstel komen te vallen. Het begrip is dus tot op zekere hoogte technologie-onafhankelijk in die zin dat technische ontwikkelingen leiden tot een andere toepassing van hetzelfde begrip, teneinde de ratio van de regelgeving – de bescherming van het individu – te behouden. Wat dus bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding.
Een gegeven is geen persoonsgegeven indien doeltreffende maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. Deze maatregelen kunnen bijvoorbeeld zijn gegevenscodering in combinatie met nadere bewerkingen of bijzondere besluitvormingsprocedures. Een verantwoordelijke kan bij voorbeeld gegevens ontdoen van de direct identificerende gegevens en deze onderbrengen bij een derde dan wel een derde de sleutel geven die toegang geeft tot deze gegevens. De vraag of in een dergelijk geval al dan niet gesproken kan worden van persoonsgegevens is afhankelijk van de mate waarin medewerking van de betrokken derde verwacht mag worden. Indien bijvoorbeeld degene die de code heeft opgesteld is onderworpen aan een geheimhoudingsplicht die naar uit de praktijk is gebleken daadwerkelijk wordt gehandhaafd, kan in de regel ervan worden uitgegaan dat er onvoldoende feitelijke mogelijkheden zijn tot daadwerkelijke identificatie. Is de code echter zonder veel moeite of met eenvoudige omzeiling van waarborgen te verkrijgen door de verantwoordelijke, dan is er sprake van identificeerbaarheid en dus van persoonsgegevens in de zin van het wetsvoorstel. De feitelijke situatie, niet de juridische constructie, is bepalend voor de toepasselijkheid van het wetsvoorstel.
Onder omstandigheden zullen de gegevens tevens nader moeten worden bewerkt om identificatie tegen te gaan. Aggregatie kan bijvoorbeeld het onderscheidend vermogen van gegevens doen verminderen. Zolang identificatie van gegevens met behulp van andere bestanden een reële mogelijkheid is, is het wetsvoorstel van toepassing en moeten de daarin opgenomen spelregels worden nageleefd.
Waarborgen om daadwerkelijke identificatie via codering en bewerking

van gegevens tegen te gaan, kunnen zijn opgenomen in een gedragscode of als voorwaarde gelden in de contractuele sfeer. In een gedragscode of een contract kunnen indicaties zijn gegeven omtrent de middelen waarmee de gegevens anoniem kunnen worden gemaakt en kunnen worden bewaard in een vorm die identificatie van de betrokkene feitelijk niet langer mogelijk maakt. Hiervan is bij voorbeeld sprake indien de codes worden beheerd door een ander op wie een geheimhoudingsplicht rust. Wanneer dergelijke regels met zorg zijn vastgesteld en ook daadwerkelijk handhaafbaar zijn, kan worden aangenomen dat het wetsvoorstel niet van toepassing is, zelfs al zou niet geheel zijn uitgesloten dat op enigerlei wijze toch herkenning van individuele personen plaatsvindt.
Wat betreft het gebruik van persoonsgegevens voor wetenschappelijke en statistische doeleinden kan in deze verwezen worden naar het advies van de Commissie Kordes «Privacywetgeving en het gebruik van persoonsgegevens voor wetenschappelijke en statistische doeleinden» van januari 1997 aan de Minister van Onderwijs, Cultuur en Wetenschappen.
De definitie van een persoonsgegeven omvat niet alleen de informatie omtrent een bepaalde persoon in geschreven tekst, doch tevens in beeld en geluid. Dit roept vragen op met betrekking tot de werkingssfeer van de regeling. In de toelichting op artikel 2 komen wij hierop terug.
Gegevens van overleden personen vallen niet onder de definitie van persoonsgegevens zoals in artikel 1, onder a, gehanteerd en blijven daarmee buiten het bereik van dit wetsvoorstel. Daarbij wordt aangesloten bij hetgeen gold onder de WPR (zie kamerstukken I, 1988/89, 19 095, nr. 36a, blz. 6/7). Indien maatschappelijk onzorgvuldig is omgegaan met gegevens van een overleden persoon, is er sprake van een onrechtmatige daad in de zin van artikel 6:162 BW en kunnen diens nabestaanden – indien is voldaan aan de voorwaarden in laatstgenoemde bepaling – schadevergoeding vorderen. Indien iemand overlijdt en diens gegevens daarmee overbodig worden ligt het in de rede dat deze gegevens verwijderd worden. De bestanden zouden anders «vervuild» raken met gegevens die voor het doel niet meer noodzakelijk zijn. De verantwoordelijke is hiertoe weliswaar niet gedwongen op grond van artikel 11 van het wetsvoorstel, maar zal om pragmatische redenen toch tot verwijdering overgaan. Hij zal bovendien niet het risico willen lopen onzorgvuldig jegens (de nabestaanden van) de overledenen te handelen, waarvan met name bij gevoelige gegevens eerder sprake zal kunnen zijn.
Ten overvloede zij er op gewezen dat de in bovenbedoelde zin beperkte reikwijdte van het wetsvoorstel het algemene uitgangspunt dat het medisch beroepsgeheim ook na de dood werkt onverlet laat.

Onderdeel b

Het object van regeling is de verwerking van persoonsgegevens. Het is conform de richtlijn gedefinieerd als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, uitwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. In plaats van het begrip «bewerking of elk geheel van bewerkingen» wordt gesproken van «handeling of elk geheel van handelingen» teneinde rekening te houden met de omstandigheid dat verwerkingen kunnen plaatsvinden door verschillende personen, zoals de verantwoordelijke, bewerker en derde.
Een uitbreiding ten opzichte van de bestaande regelgeving ligt in het onderdeel «verkrijgen». Tot dusver komt de rechtmatigheid eerst in beeld nadat gegevens in een registratie waren ondergebracht. Blijkens artikel 5, eerste lid, van de Wet persoonsregistraties mogen persoonsgegevens

slechts worden opgenomen in een registratie wanneer deze rechtmatig zijn verkregen. Dit sluit aan bij artikel 5, onder a, van het Verdrag inzake gegevensbescherming dat stelt dat persoonsgegevens slechts mogen worden verwerkt indien zij op eerlijke en rechtmatige wijze zijn verkregen. Het begrip «verwerken» in het Verdrag omvat blijkens deze regeling evenmin de fase van het verzamelen van gegevens. Dit laat de mogelijkheid open dat gegevens zijn verkregen, doch nog niet aan enige verwerking zijn onderworpen. Deze onttrekken zich aan normering. De richtlijn maakt aan deze situatie een einde en normeert reeds de fase van het verkrijging van gegevens. Het verkrijgen van gegevens is een vorm van verwerken van gegevens. Dit leidt er bij voorbeeld toe dat voorafgaand aan het verkrijgen van persoonsgegevens reeds een doel moet zijn vastgesteld, de aanmelding bij het toezichthoudend orgaan moet zijn voltooid en, wanneer het gaat om een verwerking met bijzondere risico's, het toezichthoudend orgaan een voorafgaand onderzoek moet hebben ingesteld.
De opsomming beoogt blijkens de zinsnede «waaronder in ieder geval» een illustratie te geven van het begrip gegevensverwerking en is derhalve niet uitputtend. Zo is in overweging 14 van de richtlijn mede sprake van het opvangen, doorsturen en manipuleren van gegevens. Ook de vorm van verstrekking en openbaarmaking, alsmede het genereren van gegevens valt onder de begripsomschrijving van «gegevensverwerking». Het ruime bereik van het begrip is cruxiaal voor de bescherming die dit wetsvoorstel beoogt te bieden.
Het naast elkaar vermelden van «elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens» impliceert, dat iedere bepaling in het wetsvoorstel waarin het begrip «verwerking» wordt gebruikt zowel betrekking heeft op elke handeling afzonderlijk als op elk geheel van handelingen. Onder «elk geheel van handelingen met betrekking tot persoonsgegevens» kan worden verstaan een bundeling van verwerkingshandelingen die in het maatschappelijk verkeer als een eenheid wordt beschouwd. Dit kan bijvoorbeeld verschillende handelingen in een samenhangende reeks betreffen: de verzameling, de opslag en het gebruik van een bepaald type persoonsgegevens. Daarnaast is denkbaar dat dezelfde verwerkingshandelingen met betrekking tot bepaalde persoonsgegevens naar de wettelijke maatstaven als een geheel van verwerkingen moet worden aangeduid: bijvoorbeeld een groot aantal verstrekkingen van dezelfde gegevens aan verschillende derden.
Onder «handelingen met betrekking tot persoonsgegevens» dienen alle verwerkingen waaraan persoonsgegevens kunnen worden onderworpen, te worden verstaan. Een nader onderscheid op basis van het doel of de methode van verwerking speelt geen rol. Ook niet op individuele personen gerichte verwerkingen waarbij gebruik wordt gemaakt van persoonsgegevens, vallen dus onder de begripsomschrijving. Indien bijvoorbeeld voor verschillende doeleinden aangelegde bestanden binnen een instelling worden doorzocht op een bepaald criterium (bijvoorbeeld een bepaalde inkomenspositie) dan kan dit al als een vorm van gegevensverwerking worden beschouwd, ongeacht het feit dat het bij voorbaat om een niet op voorhand te bepalen aantal personen gaat.
Zowel geautomatiseerde als niet geautomatiseerde handelingen met betrekking tot persoonsgegevens vallen onder het begrip «gegevensverwerking» met dien verstande dat ten aanzien van de niet geautomatiseerde verwerkingen het wetsvoorstel slechts van toepassing is voor zover deze in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen (artikel 2, eerste lid).
Zodra er enige feitelijke macht over persoonsgegevens is, is het wetsvoorstel van toepassing. Hiervoor hoeft niet altijd sprake te zijn van menselijke tussenkomst. Ook volledig geautomatiseerde vormen van verwerking kunnen onder de wettelijke regeling vallen. Cruxiaal blijft dat de verwerking gepaard moet gaan met de mogelijkheid daarop (enige)

invloed uit te kunnen oefenen. Niet relevant is of de invloed ook daadwerkelijk wordt uitgeoefend. Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, verwerkt daarmee geen persoonsgegevens. Wanneer echter bijvoorbeeld een Internet service provider de mogelijkheid heeft het verspreiden van onrechtmatige berichten tegen te gaan, is er wel sprake van mogelijke invloed en daarmee van gegevensverwerking en is daarom de wet volledig van toepassing.
Dat wil niet zeggen dat een telecomoperator niet gehouden is beveiligingsvoorschriften na te komen. Deze verplichting volgt echter uit de Wet op de telecommunicatievoorzieningen en heeft een ruimer bereik dan het enkel beschermen van persoonsgegevens. Anders wordt het wanneer een telecommunicatiebedrijf persoonsgegevens in het kader van een toegevoegde waardedienst met het oog op raadpleging of ander gebruik vastlegt. Dan is er geen sprake meer van een eenvoudige overdracht van gegevens.
Een andere vraagstuk betreft de vraag of er zodanige feitelijke macht kan worden uitgeoefend dat er sprake is van verantwoordelijkheid. Daarvan is eerst sprake indien de bevoegdheid bestaat het doel van de verwerking en de middelen waarmee deze geschiedt, te bepalen. Is dit niet het geval dan gelden de regels voor de bewerker.
Het begrip gegevensverwerking omvat het gehele proces dat een gegeven doormaakt vanaf het moment van verzamelen van een gegeven tot aan het moment van vernietiging. Iedere handeling of geheel van handelingen met betrekking tot het gegeven, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, valt daaronder. Hieruit vloeit voort dat iedere «losse» verwerking van geheel of gedeeltelijk geautomatiseerde gegevens onder het bereik van dit wetsvoorstel valt. Gedacht kan worden aan het opslaan van een persoonsgegeven op een (optisch-)magnetische gegevensdrager als de tekstverwerker of een chipcard. Ook de verwerking van persoonsgegevens voor datamining of de uitvoering van bepaalde zoekopdrachten (queries) met behulp van daartoe geschreven programma's, al dan niet verricht door de verantwoordelijke zelf, valt onder de algemene normering van gegevensverwerking.
Daarbij moet echter worden opgemerkt dat niet alle voorschriften van dit wetsvoorstel ook steeds moeten worden toegepast op iedere «losse» geautomatiseerde verwerking van een persoonsgegeven. De aanmeldingsprocedure is bijvoorbeeld blijkens de formulering van artikel 27, eerste lid, jo. artikel 1, onderdeel b, zo ingericht dat de verantwoordelijke de vrijheid heeft een geheel van op persoonsgegevens betrekking hebbende handelingen aan te melden, die voor de verwezenlijking van één doeleinde of verscheidene samenhangende doeleinden zijn bestemd. Hetzelfde geldt voor de procedure van voorafgaand onderzoek. Een melding of een onderzoek van iedere verwerking, bij voorbeeld iedere verstrekking, zou in die gevallen leiden tot onwerkbare situaties. Er wordt dan uitgegaan van een bundeling van gegevensverwerkingen naar gelang de doelstelling van die gegevensverwerkingen.
Niet elke verwerking van persoonsgegevens behoeft dus afzonderlijk te worden aangemeld. De artikelen waarin de gronden voor het verwerken van gegevens geregeld zijn – met name de bepalingen van hoofdstuk II – gelden daarentegen wel op iedere «losse» geautomatiseerde gegevensverwerking. Dit leidt ertoe dat bijvoorbeeld de opslag van het gegeven niet onverenigbaar mag zijn met het doel waarvoor het gegeven oorspronkelijk is verzameld, en het gegeven niet mag worden verwerkt voor doeleinden van direct marketing als de betrokkene daartegen bezwaar heeft gemaakt, ongeacht of de verantwoordelijke zelf dan wel een derde uiteindelijk de direct marketing verricht. Met betrekking tot de handmatig gevoerde gegevens volgt uit artikel 2 dat de voorschriften van dit wetsvoorstel enkel betrekking hebben op een verwerking van

handmatig gevoerde gegevens voor zover deze deel uitmaken van een bestand.
Het begrip «gegevensverwerking» dient op één lijn te worden gesteld met het ook in deze toelichting gehanteerde begrip «verwerken van persoonsgegevens».
Omdat ten aanzien van enkele, specifieke vormen van gegevensverwerking in dit wetsvoorstel afzonderlijke normen zijn opgenomen, zijn specifieke vormen van gegevensverwerking nader gedefinieerd, zoals het verzamelen en verstrekken van persoonsgegevens. Gewezen kan worden op de afzonderlijke voorschriften met betrekking tot bijvoorbeeld het verzamelen en verstrekken van gegevens. Ook in bijzondere regelgeving kunnen regels over bepaalde aspecten van verwerking worden gegeven. De vernietiging van gegevens die in overeenstemming met de Archiefwet 1995 worden bewaard, vindt plaats met inachtneming van de regels van die wet.
Door het enkel wettelijke definiëren van het begrip «gegevensverwerking» wordt onderstreept dat het uitgangspunt van dit wetsvoorstel is uniforme regels te stellen voor alle vormen van gegevensverwerking.

Onderdeel c

De omschrijving van het begrip «bestand» is overgenomen uit artikel 2 van de richtlijn en sluit aan bij die van het begrip «persoonsregistratie» in artikel 1 van de WPR. De richtlijn laat de lid-staten een zekere marge voor de invulling van dit begrip (zie ook overweging 15).
Het begrip «bestand» is in het onderhavige wetsvoorstel enkel van belang als criterium voor de afbakening van de reikwijdte van het wetsvoorstel en bepaalde onderdelen daarvan. Wat betreft de niet-geautomatiseerde verwerkingen vallen alleen bestanden, en dus bijvoorbeeld niet ongestructureerde dossiers onder het toepassingsbereik van dit wetsvoorstel (artikel 2, eerste lid). Het wetsvoorstel beoogt in deze geen wijziging aan te brengen ten opzichte van hetgeen geldt onder de WPR. Voorts behoeven niet geautomatiseerde verwerkingen niet te worden aangemeld als ze geen onderdeel uitmaken van een bestand dat is onderworpen aan een voorafgaand onderzoek (bijvoorbeeld artikel 27, tweede lid). Onder de WPR geldt in beginsel een aanmeldingplicht voor niet geautomatiseerde verwerkingen die deel uitmaken van een bestand. Een «bestand» kan zowel geautomatiseerde als niet geautomatiseerde verwerkingen bevatten. Van een bestand is sprake als de persoonsgegevens onderdeel uitmaken van een gestructureerd geheel dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen. In overweging 27 van de richtlijn is aangegeven dat de nationale wetgeving een nadere invulling kan geven aan deze omschrijving.
Op grond van artikel 1 van de WPR is voor de vraag of er sprake is van een persoonsregistratie van belang dat het gaat om een «samenhangende verzameling». Bij handmatige verwerkingen gaat het eveneens om de vraag of de verzameling «met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd». Beiden vereisten – een samenhangend geheel en systematische toegankelijkheid – zijn eveneens bepalend voor de vraag of er sprake is van een bestand in de zin van het onderhavige artikel. In de begripsomschrijving van «bestand» hebben de vereisten echter een ruimer bereik: ook de geautomatiseerde gegevensverwerkingen moeten aan beide vereisten voldoen wil er sprake zijn van een bestand. Materieel leidt dit niet tot een wijziging ten opzichte van hetgeen onder de WPR geldt. Bij geautomatiseerde verwerkingen wordt de systematische toegankelijkheid in de WPR steeds aanwezig geacht. Wat handmatige verwerkingen betreft komt de reikwijdte van het begrip «bestand» overeen met die van het begrip «persoonsregistratie» in de WPR.

Hieronder zal nader worden ingegaan op beide vereisten.

1. Een (gestructureerd) geheel

Het vereiste van een samenhangend geheel komt in de begripsomschrijving van «bestand» in artikel 1 van de WBP terug in het woord «geheel». Het vereiste «gestructureerd geheel» of «samenhangende verzameling» houdt in dat de gegevensverwerkingen of de verzameling op grond van meer dan één kenmerk een onderlinge samenhang moet(-en) vertonen. Onderlinge samenhang kan blijken uit een gemeenschappelijke bestemming of uit het feit dat de verzameling in de praktijk als een geheel worden beschouwd. De samenhang kan zitten in een vooraf aangebrachte structuur van de verzameling of in een raadpleegmethodiek die samenhang brengt in ogenschijnlijk willekeurige gegevensverwerkingen. Daarnaast zijn, vooral bij geïntegreerde systemen, het doel of de doelen van de verwerkingen en het feitelijk gebruik van de gegevens van belang voor het antwoord op de vraag of er sprake is van één of meerdere bestanden (Registratiekamer, 25 februari 1994, 93.A.012).
Het criterium «gestructureerd geheel» is eveneens van belang om vast te stellen of er sprake is van één of wellicht meerdere bestanden. Alsdan is niet zozeer de fysieke verschijningsvorm als wel de logische samenhang van de verzameling van belang. Dit brengt met zich dat back-ups en schaduwbestanden niet als een afzonderlijk bestand moeten worden aangemerkt maar zijn te beschouwen als hulpmiddelen bij het voeren van het bestand ten dienste waarvan zij zijn aangelegd. Een zelfde opmerking kan worden gemaakt ten aanzien van een geheel van handmatige bestanden die op verschillende lokaties worden bijgehouden. Een bestand dat zich bevindt op verschillende lokaties kan als één bestand worden aangemerkt indien de verschillende onderdelen van het bestand logisch als één geheel kunnen worden beschouwd.

2. Systematische toegankelijkheid

Het vereiste van een systematische toegankelijkheid komt in de begripsomschrijving van «bestand» in artikel 1 van de WBP terug in de woorden «gestructureerd» geheel «dat volgens bepaalde criteria toegankelijk is». Het gaat hierbij vooral om de vraag of verzamelingen een duidelijke, vooraf met het oog op raadpleging aangebrachte structuur bezitten. De methode van gegevensopslag en -verwerking is van belang. De inhoud van het bestand moet met het oog op doeltreffende raadpleging volgens bepaalde criteria aangelegd zijn. Door de systematische structuur zijn de persoonsgegevens gemakkelijk toegankelijk. Kaartsystemen en gegevensverzamelingen die in hoofdzaak bestaan uit voorbedrukte formulieren voldoen aan deze eis. Dossierverzamelingen kunnen aan de eis van systematische toegankelijkheid voldoen, bijvoorbeeld in combinatie met een al dan niet geautomatiseerd bestand met een verwijsfunctie naar de dossiers. Dossierverzamelingen die uitsluitend bestaan uit een hoeveelheid op alfabet gerangschikte dossiers, met losse aantekeningen en min of meer chronologisch geordende documenten van velerlei aard, zullen niet voldoen aan het vereiste van systematische toegankelijkheid. De vraag of handmatige dossierverzamelingen aan deze criteria voldoen, is afhankelijk van de feitelijke omstandigheden.
Naast bovenstaande vereisten dient tot slot – wil er sprake zijn van een bestand – het gestructureerd geheel van gegevens betrekking te hebben op verschillende personen. Deze voorwaarde werd ook in de WPR gesteld. Het advies van de Registratiekamer dit vereiste te schrappen wordt niet overgenomen. De reikwijdte van het begrip bestand met het oog op dossierverzamelingen is thans in de jurisprudentie enigszins uitgekristalliseerd. Het is onwenselijk daarin nu weer wijziging te brengen.
Gegevens die op grond van de hierboven omschreven criteria niet worden

geacht te zijn opgenomen in een bestand, vallen bijvoorbeeld onder de bescherming van artikel 6:162 BW (onrechtmatige daad). Daarnaast is voor de overheid de Wet openbaarheid van bestuur van toepassing. Dat betekent, dat een verzoek van iemand tot kennisneming van hem betreffende informatie uit dossiers die niet deel uitmaken van een gestructureerd geheel en daarom niet onder de definitie van een bestand vallen, kan worden gebaseerd op de Wet openbaarheid van bestuur c.q. het BW in verband met een onrechmatige daad.

Onderdeel d

Bij de definitie van het begrip «verantwoordelijke» is nauw aangesloten bij de omschrijving van artikel 2, onderdeel d, van de richtlijn. In tegenstelling tot de WPR gaat het wetsvoorstel niet meer uit van het begrip «houder», maar van het begrip «verantwoordelijke». «Houden» is een overgankelijk werkwoord: onder de WPR werd een zekere zaak, te weten, de registratie «gehouden». Nu het object van regelgeving niet de zaak «registratie» maar het proces «gegevensverwerking» betreft, is taalkundig een overgankelijk werkwoord niet meer op zijn plaats. Het begrip uit artikel 2 van de richtlijn «voor de verwerking verantwoordelijke» is in dit wetsvoorstel omgezet als «verantwoordelijke». De relatie tussen «houder» en «registratie» onder de WPR is echter in beginsel dezelfde als die tussen «verantwoordelijke» en «gegevensverwerking» onder dit wetsvoorstel. Overeenkomstig artikel 2, onderdeel d, van de richtlijn wordt in de begripsomschrijving niet meer gesproken van de natuurlijke persoon enz. die bevoegd is doel van en middelen voor de verwerking vast te stellen. Indien onbevoegd gegevens worden verwerkt dient immers eveneens een verantwoordelijke te kunnen worden aangewezen en op zijn handelen te kunnen worden aangesproken.
Het begrip «verantwoordelijke» knoopt in eerste instantie aan bij de vaststelling van het doel van de verwerking. De vraag is wie uiteindelijk bepaalt of er gegevens worden verwerkt en zo ja, welke verwerking, van welke persoonsgegevens en voor welk doel. Tevens is van belang wie beslist over de middelen voor die verwerking: de vraag op welke wijze de gegevensverwerking zal plaatsvinden. De richtlijn gaat ervan uit dat deze bevoegdheden in de regel in dezelfde hand liggen. Is dit niet het geval, dan is er sprake van gezamenlijke verantwoordelijkheid.
Met de aldus gegeven omschrijving kan evenwel niet worden volstaan. Op grond van de praktijk van de huidige WPR moet worden aangenomen dat het – gegeven de tekst van de richtlijn – niet altijd eenvoudig zal zijn om in concrete gevallen te bepalen wie verantwoordelijke is en aan de hand van welke criteria dat moet worden vastgesteld. Op grond van de ervaringen in de praktijk en de recent verrichte evaluaties moet een en ander daarom verder worden ingevuld.
Bij de beantwoording van de vraag wie de verantwoordelijke is, dient enerzijds te worden uitgegaan van de formeel-juridische bevoegdheid om doel en middelen van de gegevensverwerking vast te stellen, anderzijds – in aanvulling daarop – van een functionele inhoud van het begrip. Het laatste criterium speelt met name een rol als er verschillende actoren bij de gegevensverwerking betrokken zijn en de juridische bevoegdheid onvoldoende helder is geregeld om te kunnen bepalen wie van de betrokken actoren als verantwoordelijke in de zin van de wet moet worden aangemerkt. In dergelijke situaties zal aan de hand van algemeen in het maatschappelijk verkeer geldende maatstaven moeten worden bezien aan welke natuurlijke persoon, rechtspersoon of bestuursorgaan de betreffende verwerking moet worden toegerekend. Een en ander kan als volgt nader worden toegelicht.
Uit de juridische evaluatie blijken als gevolg van de bestaande diversiteit in zeggenschap bij de toepassing van de WPR in de praktijk een aantal problemen. Door zowel bij de invulling van het houderschapsbegrip aan

te sluiten bij bestaande (formele) privaatrechtelijke en publiekrechtelijke rechtsverhoudingen, als rekening te houden met feitelijke verhoudingen en maatschappelijke verkeersopvattingen, is een dogmatische onduidelijkheid ontstaan. Het houderschapsbegrip is een koepelterm geworden voor uiteenlopende vormen van zeggenschap en verantwoordelijkheid inzake de gegevensverwerking. Deze onduidelijkheid leidt in de praktijk tot problemen op het punt wie aanspreekbaar is voor de wettelijke verplichtingen van de houder. De geregistreerde loopt het risico de onjuiste persoon of instelling aan te spreken op zijn verplichtingen. Voor een inzage- of correctieverzoek dient hij zich in bepaalde gevallen, eerst op de hoogte te stellen van feitelijke zeggenschapsverhoudingen binnen een orgaan of instelling, bij voorbeeld wanneer het gaat om een registratie die is vrijgesteld van de aanmeldingsplicht. Bovendien biedt het element «feitelijke macht» de ruimte om het houderschap zo te kiezen dat voor de houder zo groot mogelijke ruimte ontstond om gegevens te gebruiken. De geregistreerde moest onderzoek doen, wie als houder kon worden aangesproken. Met name bij de vrijgestelde registraties werd daardoor afbreuk gedaan aan de rechtspositie van de geregistreerden
Het onderhavige wetsvoorstel beoogt om die reden bij de invulling van het begrip «verantwoordelijke» nauwer aan te sluiten bij bestaande privaatrechtelijke en publiekrechtelijke rechtsverhoudingen. Deze zijn voor de betrokkene beter kenbaar. Het is wenselijk duidelijk te stellen dat het begrip «verantwoordelijke» doelt op degene die formeel-juridisch de zeggenschap over de verwerking heeft. Daar het begrip «zeggenschap» onder de WPR een ruimere dimensie had, is er voor gekozen uit te gaan van degene die bevoegd is doel en middelen vast te stellen. Het begrip «verantwoordelijke» is in artikel 1, onderdeel d, in deze zin ingevuld. Dat laat onverlet dat het feitelijk beheer over de gegevensverwerking aan een ander kan worden gemandateerd. In de meeste gevallen zal deze ander wat betreft het geheel van de gegevensverwerking hiërarchisch ondergeschikt zijn aan de verantwoordelijke. De handelingen van deze ondergeschikten worden dan volgens de gewone regels van het burgerlijk recht of het staatsrecht aan de verantwoordelijke toegerekend.
Uitgangspunt bij de invulling van het begrip «verantwoordelijke» is derhalve de bestaande struktuur van het civielrechtelijke en bestuursrechtelijke personen- en organisatierecht. Voor de private sector betekent dit dat de formeel-juridische organisatie van de onderneming doorslaggevend is. In de private sector is of de natuurlijke persoon of de rechtspersoon rechtssubject. Bij eenmanszaken zal de natuurlijke persoon als verantwoordelijke zijn aan te merken.
Het bovenstaande vindt ook toepassing bij concernverhoudingen. Verantwoordelijke is de rechtspersoon onder wiens bevoegdheid de operationele gegevensverwerking plaatsvindt. De feitelijke macht of invloed van een andere rechtspersoon binnen het concern is niet van belang. De ratio is dat de betrokkene in het maatschappelijk verkeer kan weten ten aanzien van wie hij zijn rechten desgewenst kan uitoefenen. De rechtspersoon is de juridische entiteit die daartoe in het recht is geschapen. Dat die door de moeder- of een dochtermaatschappij verrichte gegevensverwerking (mede) ten dienste staan van het concern als zodanig is op zichzelf niet van belang voor het vaststellen van verantwoordelijkheid. Het wetsvoorstel staat evenwel niet in de weg aan een regeling waarbij in de statuten van de betrokken rechtspersonen of via een overeenkomst aan een bepaalde rechtspersoon binnen het concern de bevoegdheid wordt toegekend om doel en middelen van de gegevensverwerkingen binnen het concern te bepalen. De genoemde rechtspersoon – bijvoorbeeld de moedermaatschappij – is dan verantwoordelijke in de zin van het wetsvoorstel voor alle gegevensverwerkingen die binnen het concern plaatsvinden, omdat de juridische zeggenschap krachtens de getroffen regeling bij die rechtspersoon berust. Een dergelijke regeling valt ook binnen de grenzen van een functionele

invulling van het begrip «verantwoordelijke». Het is in overeenstemming met maatschappelijke verkeersopvattingen om de verantwoordelijkheid voor de gegevensverwerking toe te rekenen aan de rechtspersoon die krachtens een interne regeling binnen het concern als de bevoegde rechtspersoon is aangewezen. Blijft evenwel een regeling als hiervoor bedoeld achterwege, dan is conform de hoofdregel elke rechtspersoon binnen het concern verantwoordelijke voor de gegevensverwerking die binnen die rechtspersoon plaatsvindt.
In de publieke sector geldt het krachtens het geldende staats- en bestuursrecht bevoegde bestuursorgaan als de verantwoordelijke. Deze bevoegdheid is te vinden in de Grondwet en in de bestuursrechtelijke wetgeving. Daarbij komt in de eerste plaats de Awb in beeld. Met het begrip «bestuursorgaan» in dit wetsvoorstel is bedoeld aan te sluiten bij de in de Awb geregelde betekenis van dit begrip. Het begrip sluit in aanvulling daarop eveneens aan bij de algemene inrichtings- en beheersbevoegdheden, bij voorbeeld de hiërarchische bevelsbevoegdheid ten opzichte van het ambtelijk apparaat. Binnen de overheid zullen als verantwoordelijke te kwalificeren zijn: de afzonderlijke ministers op rijksniveau, het college van gedeputeerde staten en de commissaris van de Koningin op provinciaal niveau en het college van burgemeesters en wethouders en de burgemeester op gemeentelijk niveau. Bij zelfstandige bestuursorganen op rijksniveau en funktionele commissies op provinciaal en gemeentelijk niveau zal het orgaan, belast met de taken en uitoefening van bevoegdheden waarvoor de gegevens worden verwerkt, als verantwoordelijke zijn aan te merken. Bij instellingen met een zodanige zelfstandigheid dat zij vergelijkbaar zijn met zelfstandige bestuursorganen zoals het Centraal bureau voor de statistiek, zal de verantwoordelijkheid volgen uit het instellingsbesluit van deze instellingen.
Met een aldus in te vullen begrip «verantwoordelijke» zal in elk geval een deel van de bestaande onduidelijkheid bij de WPR worden weggenomen. De Registratiekamer heeft er evenwel terecht op gewezen dat dit niet geldt voor alle gevallen. In situaties waarin meerdere natuurlijke personen, rechtspersonen of bestuursorganen betrokken zijn bij een keten van gegevensverwerkingen en in verband met de aard van die betrokkenheid in aanmerking komen om als verantwoordelijke in de zin van de wet te worden aangeduid, bestaat behoefte aan een aanvullend criterium. Problemen kunnen zich met name voordoen als de juridische zeggenschap over de verwerking onvoldoende duidelijk is, dan wel geen regeling voorhanden is op grond waarvan een bepaalde persoon of instantie daadwerkelijk door de betrokkene kan worden aangesproken. Burgers mogen daarvan niet de dupe worden. In zodanige situaties behoort aan het begrip «verantwoordelijke» een functionele invulling te worden gegeven. Aan de hand van in het maatschappelijk verkeer geldende maatstaven moet in dergelijke gevallen worden bezien aan welke natuurlijke persoon, rechtspersoon of bestuursorgaan de betreffende verwerking moet worden toegerekend.
De Registratiekamer wijst erop dat wat betreft de functionele inhoud van belang is of de verantwoordelijke voor zichzelf persoonsgegevens verwerkt of doet verwerken. Doet hij dit ten behoeve van een ander, dan is hij «bewerker». Wij zijn het hiermee eens. In de wettekst is de definitie van de richtlijn evenwel gehandhaafd. De verdere rechtsontwikkeling op Europees gebied, bij voorbeeld naar aanleiding van jurisprudentie van het Europese Hof van Justitie, kan daardoor gemakkelijker worden gevolgd. Iemand die voor zichzelf verwerkt of doet verwerken, is verantwoordelijke. Hieraan doet niet af dat hij daarmee derden van dienst wil zijn. Van belang is dat hij zelf bepaalt welke soort gegevens hij verwerkt, hoe lang en met welke middelen. Degene daarentegen die krachtens een contract dat blijkens zijn aard betrekking heeft op de gegevensverwerking ten behoeve van een derde, waarbij de wederpartij bepaalt welke gegevens, waartoe, hoelang enz. worden verwerkt, moet worden aangemerkt als bewerker.

Een belangrijke nuancering is voorts dat in bepaalde situaties ook sprake kan zijn van gezamenlijke of gedeelde verantwoordelijkheid. De richtlijn houdt hier rekening mee. Het Europees Parlement heeft door een amendement in de definitie van «voor de verwerking verantwoordelijke» door de toevoeging daarin van de zinsnede «alleen of te zamen met anderen» de mogelijkheid van een regeling voor samenwerkende verantwoordelijken getroffen. Deze clausule is overgenomen in het wetsvoorstel. Ten aanzien van een geheel van gegevensverwerkingen is het mogelijk dat meerdere personen of instanties, dus een pluraliteit van verantwoordelijken, als zodanig worden aangemerkt. Daarbij kunnen drie vormen van verantwoordelijkheid onderscheiden worden.

1. Aan de verwerkingen nemen verschillende organisaties deel, er is echter één gemeenschappelijke verantwoordelijke. Deze is aansprakelijk voor de verwerkingen als geheel. Daarnaast zijn de deelnemende organisaties aansprakelijk voor de aangeleverde gegevens. De verantwoordelijke is voor de inhoud daarvan slechts verantwoordelijk naar de mate waarop hij daarover juridische zeggenschap heeft. Te denken valt aan de gegevensverwerking van een ziekenhuis, waarbij de leiding van het ziekenhuis als verantwoordelijke wordt aangemerkt, terwijl de deelnemende medici verantwoordelijk zijn voor de juistheid van de opgenomen gegevens. De betrokkene kan in rechte slechts de ziekenhuisdirectie aanspreken. Heeft de betrokkene schade geleden door een fout van één van de deelnemende medici dan heeft de ziekenhuisdirectie op hem een recht van regres. De betrokkene kan dit evenwel niet worden tegengeworpen.
2. Verschillende verwerkingen zijn min of meer geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van afzonderlijke verantwoordelijkheid per (deel-)verwerking. De betrokkene kan slechts één van de afzonderlijke verantwoordelijken aanspreken. Te denken valt aan persoonsgegevens die via Internet kunnen worden geconsulteerd. In gevallen waarin geen verantwoordelijke kan worden geïdentificeerd, gelden de gewone regels van het Wetboek van Strafrecht voor de strafbare verspreiding van bepaalde vormen van informatie voor daders en medeplichtigen. Bij persoonsgegevens kan het daarbij bij voorbeeld gaan om smaad en belediging.
3. Verschillende verwerkingen zijn geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van gezamenlijke verantwoordelijkheid. Elk van de verantwoordelijken is aansprakelijk voor het geheel van de gegevensverwerkingen.

De aansprakelijkheid is gerelateerd aan de omvang van de verantwoordelijkheid. In de eerst genoemde samenwerkingsconstructie is de verantwoordelijke in beginsel aansprakelijk voor de verwerkingen als geheel. Is echter sprake van een afzonderlijke verantwoordelijkheid voor deelverwerkingen, dan is elke verantwoordelijke in beginsel aansprakelijk voor zijn deel. Bij gezamenlijke verantwoordelijkheid zijn alle in het samenwerkingsverband participerende personen c.q. instellingen hoofdelijk aansprakelijk. Uit de artikelen 6:6 e.v.BW vloeit voort dat iedere verantwoordelijke tegenover de betrokkene voor het geheel aansprakelijk is. Dit laat onverlet de mogelijkheid van regres wanneer bij voorbeeld de schuld bij één van de andere verantwoordelijken ligt.

De derde vorm biedt rechtspersonen die samenwerken in een concernverband, de mogelijkheid geïntegreerde cliëntregistraties gezamenlijk te voeren en als een geheel van verwerkingen met verscheidene, doch samenhangende doeleinden aan te melden. Een dergelijke melding staat los van de vraag of het gebruik van de aldus in een geïntegreerd systeem opgenomen gegevens, voor elk van de samenhangende doeleinden, verenigbaar is met het doel waarvoor de daarin opgenomen gegevens oorspronkelijk zijn verkregen. De vraag van de inhoudelijke normering, wordt immers niet beantwoord met de keuze voor één of meer (gezamen-

lijke) verantwoordelijken. Verwezen zij op dit punt naar de toelichting op artikel 27, eerste lid.
Het feit dat er meer, al dan niet gezamenlijk optredende, verantwoordelijken zijn, laat de mogelijkheid onverlet dat, wanneer zij bij voorbeeld in concernverband optreden, zij een regeling treffen voor een gemeenschappelijke klachtenbehandeling, waar expertise op het gebied van de bescherming van persoonsgegevens kan worden geconcentreerd. Een dergelijke gemeenschappelijke organisatie treedt dan telkens op namens de desbetreffende verantwoordelijke. Voorts is denkbaar dat binnen het concern een regeling wordt getroffen waarbij de bevoegdheid om doel en middelen van de gegevensverwerking te bepalen, aan een bepaalde rechtspersoon binnen het concern wordt toegekend. Hiervoor is reeds op die mogelijkheid ingegaan.
Met behulp van de hiervoor verwoorde uitgangspunten dient het begrip «verantwoordelijke» zich verder uit te kristalliseren. Met het oog daarop kan hier nog worden ingegaan op een aantal praktijkvragen die zich reeds hebben voorgedaan.
Een van deze vragen heeft betrekking op de gang van zaken in het betalingsverkeer. Banken zijn verantwoordelijke met betrekking tot de financiële gegevens die zij voor hun cliënten verwerken (bijvoorbeeld het overmaken van een geldsom van de ene rekening naar een andere). Dit geldt ook voor gegevens die clinten bij financiële transacties in het berichtenveld laten opnemen (bijvoorbeeld dat een betaling de contributie van een derde voor een politieke partij betreft). De verantwoordelijkheid voor de juistheid van deze gegevens, bestaat in deze context daaruit, dat de banken de gegevens verwerken in overeenstemming met de gegevens die de cliënt heeft aangeboden. In het voorontwerp van het wetsvoorstel werd op dit punt een ander standpunt ingenomen. Naar aanleiding van het advies van de Registratiekamer, is daarop teruggekomen. Wat betreft de vraag naar de zorgplicht van de bank als verantwoordelijke voor de juistheid van de gegevens, geldt dat deze niet verder reikt dan de juridische mogelijkheden en de reguliere bancaire praktijk om deze te beïnvloeden. Wat betreft de gegevens in het berichtenveld betekent dit dat de bank verantwoordelijk is dat de daarin opgenomen gegevens in overeenstemming zijn met de gegevens die door degene die de betalingsopdracht gaf, zijn aangeleverd.
Hetzelfde geldt voor de aanbieder van een telecommunicatiedienst waarbij elektronische post of voicemail op de markt wordt aangeboden. Zolang de gegevens zijn opgeslagen en daardoor feitelijke macht daarover kan worden uitgeoefend, is de dienstaanbieder verantwoordelijk. Wat betreft de juistheid van de gegevens beperkt zich deze verantwoordelijkheid tot de zorg te waarborgen dat de gegevens in overeenstemming zijn met de gegevens zoals deze zijn aangeleverd door degene die van deze dienst gebruik maakt. Dienstaanbieders zijn daarentegen wel onbeperkt als verantwoordelijke aan te merken, ook wat betreft hun inhoud, voor de gegevens die noodzakelijk zijn om dat berichtenverkeer tot stand te brengen (de z.g. dienstgegevens) en vervolgens bij gebruik van het dienstaanbod de rekening te kunnen presenteren (de z.g. verkeersgegevens).
Wat betreft de opdrachtgever van een betaling of de gebruiker van E-mailservice, geldt dat deze voor de inhoud van de boodschap zelf als verantwoordelijke dient te worden aangemerkt. Er is dan sprake van «geschaalde» verantwoordelijkheid (zie blz. 24 van het rapport «Chipcards en privacy» van september 1995 «Achtergrondstudies en verkenningen» nr 6 van de Registratiekamer). Gaat het om persoonlijk of huishoudelijk gebruik, dan is daarop het wetsvoorstel niet van toepassing. Dit zal vaak het geval zijn. Wanneer echter sprake is van boodschappen waar ten behoeve van zakelijk gebruik door meerdere personen persoonsgegevens worden overgedragen via elektronische post of als onderdeel van een betalingsopdracht, dan is de afzender separaat als verantwoordelijke,

naast degene die de gegevens overdraagt en daartoe enige tijd vastlegt, aan te merken, ieder voor de volle omvang van dat deel waarover zijn bevoegdheid zich uitstrekt.
Wanneer het gaat om de inhoud van de gegevens, ligt het in de rede dat het recht op kennisneming dus ook tegenover de verantwoordelijke die de persoonsgegevens heeft aangeleverd, wordt uitgeoefend. Deze is immers verantwoordelijk voor de inhoudelijke juistheid van de gegevens. De bank of de Internet service provider die persoonsgegevens op het berichtenveld van een betalingsopdracht verwerkt onderscheidenlijk de persoonsgegevens in het E-mailbericht verwerkt, heeft niet de bevoegdheid de gegevens te wijzigen. Dat laat onverlet dat er ook een recht op kennisneming bestaat tegenover de verantwoordelijke die de persoonsgegevens verwerkt in die zin dat hij verantwoordelijk is voor de verwerking van de gegevens precies zoals zij zijn aangeleverd. De betrokkene heeft het recht na te gaan of de op hem betrekking hebbende gegevens in deze laatste zin «juist» door de verantwoordelijke worden verwerkt, uiteraard voor zover deze juridisch en technisch toegang heeft tot de desbetreffende gegevens. Dit leidt er overigens niet toe dat de betrokkene aan een bank of een Internet service provider ongericht kan vragen na te gaan of over hem gegevens in enig bericht zijn opgenomen. Dat zou onder omstandigheden neerkomen op misbruik van recht, daar dit een volstrekt onevenredige inspanning van de verantwoordelijke zou vergen om, althans met de thans ter beschikking staande technische middelen, alle berichten hierop na te gaan.
Het bovenstaande maakt ook duidelijk in hoeverre de eigenaar of bezitter van een faxapparaat of een personal computer als verantwoordelijke in de zin van dit wetsvoorstel moet worden aangemerkt. Gaat het om de simpele overdracht van persoonsgegevens dan ontbreekt feitelijk de mogelijkheid de gegevens voor enig doel te gebruiken, en is er daarom geen sprake van verwerking in de zin van het wetsvoorstel. Zodra daarentegen op enig randapparaat, ongeacht of dit een computer is, een fax, een antwoordapparaat of wat dies meer zij, persoonsgegevens met het oog op raadpleging op een door de mens nader te bepalen tijdstip, worden vastgelegd, is het wetsvoorstel van toepassing zodra het niet gaat om louter persoonlijk of huishoudelijk gebruik. Zie de toelichting op artikel 2, tweede lid, onder a. De technische ontwikkelingen leiden tot een convergentie van de verschillende apparatuur. Een technologie-onafhankelijke benadering eist de regelgeving niet te preciseren naar wat nu nog naar verschillende functie wordt onderscheiden. Het ligt overigens wel in het voornemen dergelijke apparaten in beginsel vrij te stellen van een aanmeldingsplicht.
Papieren documenten die gedrukt zijn op een faxapparaat of met behulp van een personal computer, vallen, indien zij persoonsgegevens bevatten, onder de voorschriften die van toepassing zijn op de niet-geautomatiseerde verwerking van persoonsgegevens. De wettelijke bepalingen zijn slechts van toepassing indien deze papieren bestemd zijn om in een bestand te worden opgenomen. Wanneer in een personal computer een kopie wordt bewaard van het verzonden document, zijn de bepalingen weer wel van toepassing.
Iemand die persoonsgegevens heeft vastgelegd en gebruikt, bijvoorbeeld door deze ter raadpleging aan te bieden, ook al zijn deze anoniem door een derde via Internet aangeleverd, is aanspreekbaar op naleving van dit wetsvoorstel en kan zich niet verschuilen achter het adagium «geen boodschap aan de boodschap». Zodra opslag met het oog op raadpleging plaatsvindt, bijvoorbeeld in de vorm van een «cache-service[1]», is er sprake van verwerking.
De verantwoordelijke moet worden onderscheiden van de eigenaar van de voorwerpen waarop de persoonsgegevens zijn vastgelegd. Wanneer om redenen van vermogensrecht deze voorwerpen niet (meer) onder de beheersmacht van de verantwoordelijke vallen, bijvoorbeeld omdat zij

[1] Dit is een geautomatiseerde functie in de computer van een aanbieder van toegang op een netwerk (accessprovider). De functie kopieert bij herhaalde raadpleging van een elders opgeslagen bestand, dit bestand in de computer van de toegangsaanbieder teneinde op de kosten van telecommunicatie te besparen.

worden vervreemd wegens faillissement, rust toch op de verantwoordelijke de plicht te zorgen voor de juiste omgang met de daarop vastgelegde gegevens. Een eventueel civielrechtelijk of strafrechtelijk beslag waarbij de beheersmacht over de materiële voorwerpen wordt opgeschort, ontslaat de verantwoordelijke niet van de verplichtingen die op hem rusten ten aanzien van de op deze voorwerpen vastgelegde persoonsgegevens. In het geval de persoonsgegevens zelf, naast de voorwerpen waarop zij zijn vastgelegd, een vermogenswaarde vertegenwoordigen, dan is mogelijk dat het beslag zich mede uitstrekt tot deze gegevens.
Artikel 8, onder c, laat gegevensverwerking toe indien dit noodzakelijk is om een wettelijke verplichting na te komen. Deze bepaling stelt de verantwoordelijke in staat zijn verplichtingen na te komen die voortvloeien uit het beslag.
Artikel 1, onder d, van de richtlijn laat de mogelijkheid open dat een bijzondere wet bepaalt wie de verantwoordelijke is dan wel volgens welke criteria deze wordt aangewezen. Dit ligt met name in de rede indien het doel en de middelen voor de verwerking worden vastgesteld bij wet (zie artikel 2, onderdeel d, tweede volzin, van de richtlijn). Zo zal in de Kadasterwet de Raad van Bestuur van het Kadaster als verantwoordelijke worden aangewezen. Uitgangspunt is steeds dat geen persoonsgegevens geautomatiseerd worden verwerkt, waarvoor niet iemand aanspreekbaar is en dat deze laatste ook zonder nader onderzoek door de betrokkene kan worden gekend.

Onderdeel e

Bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder dat hij diens ondergeschikte is. Hoewel het bewerkersbegrip van de WPR zich inhoudelijk onderscheidt van die van dit wetsvoorstel is desalniettemin ook in dit wetsvoorstel voor deze term gekozen in plaats van de in de richtlijn gebruikte term «verwerker». De term «bewerker» brengt immers duidelijker tot uitdrukking dat verwerkingen kunnen plaatsvinden door verschillende personen, zoals de verantwoordelijke, bewerker en derde.
In tegenstelling tot de WPR waarin het bewerkersbegrip is gerelateerd aan de beschikking over verwerkingsapparatuur, is in het wetsvoorstel, in het verlengde van de richtlijn, gekozen voor een begripsinhoud die is losgekoppeld van de middelen waarmee de verwerking wordt gevoerd. Daarmee wordt beter ingespeeld op toekomstige technologische ontwikkelingen, die ertoe leiden dat het medium waarmee of waarlangs (geautomatiseerd gevoerde) gegevens worden gevoerd minder relevant wordt.
De bewerker verwerkt gegevens ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. Bepalend voor de afbakening van het begrip is de relatie met de verantwoordelijke voor de gegevensverwerking en de mate van zeggenschap waarmee de verwerking van persoonsgegevens gepaard gaat. De bewerker is allereerst een buiten de organisatie van de verantwoordelijke staande persoon of instelling. Het zal veelal gaan om een persoon of instelling die niet in een hiërarchische relatie tot de verantwoordelijke staat. Daar waar een hiërarchische relatie bestaat met de verantwoordelijke moet worden gesproken van (intern) beheer. De verantwoordelijke die gegevens te zijner behoeve buiten zijn rechtstreeks gezag verwerkt wil hebben is op grond van artikel 14, tweede lid, verplicht een overeenkomst met de bewerker aan te gaan.
Daarnaast beperkt de bewerker zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens

enz. Zou hij immers deze zeggenschap wel verwerven dan dient hij als verantwoordelijke te worden aangemerkt.
Hieronder zal nader worden ingegaan op het bereik van het bewerkersbegrip.
Hoewel de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking door de bewerker (zie artikel 12), is ook de bewerker drager van rechten en plichten. Hij dient niet alleen de instructies van de verantwoordelijke op te volgen maar is eveneens zelfstandig aansprakelijk voor de naleving van de beginselen met betrekking tot de verwerking van persoonsgegevens (hoofdstukken 1 en 2 van dit wetsvoorstel). Deze aansprakelijkheid is expliciet neergelegd in artikel 49, derde lid. Indien de verantwoordelijke niet aansprakelijk is op grond van artikel 49, vierde lid, kan de bewerker aansprakelijk worden gesteld voor de schade die is ontstaan door zijn werkzaamheid. Hiermee blijft het acquis van de WPR (artikel 10) behouden.
Het bewerkersbegrip is in principe van toepassing op verschillende vormen van dienstverlening. Uitgangspunt is daarbij dat de dienstverlening betrekking heeft op het verwerken van persoonsgegevens. Zodra de gegevensverwerking een uitvloeisel is van een andere vorm van dienstverlening, is de dienstverlener daarvoor zelf verantwoordelijk. Een advocaat die namens een cliënt optreedt of een telemarketingbedrijf dat in opdracht van een derde onderzoek verricht, is bijvoorbeeld zelf verantwoordelijk voor de verwerking van persoonsgegevensdie in het kader van hun taak plaatsvindt.
Bestaat de dienstverlening uit het verwerken van persoonsgegevens als zodanig, dan zijn verschillende varianten van het bewerkerschap mogelijk. Het bereik van het begrip wordt afgegrensd door enerzijds de interne beheerder die onder rechtstreeks gezag van de verantwoordelijke de gegevens verwerkt en daarom niet als bewerker kan worden aangemerkt en anderzijds het externe bureau dat zelfstandig in het kader van een opdracht van een bedrijf gegevens verwerkt en daarmee ook zelf als verantwoordelijke kan worden aangemerkt. De verantwoordelijke kan de verwerking opdragen aan een binnen zijn organisatie werkzaam persoon, de verwerking kan geschieden als een vorm van vertegenwoordiging van de verantwoordelijke, door een bewerker buiten de organisatie van de verantwoordelijke of door een extern bureau dat zelf als verantwoordelijke kan worden aangemerkt. Voor de afgrenzing van het begrip «bewerker» ten opzichte van het begrip «verantwoordelijke» is de inhoud van de overeenkomst die de bewerker sluit met de verantwoordelijke van belang. Daarnaast is echter ook van belang hoe zich het één en ander vervolgens in de praktijk feitelijk ontwikkelt. Als een extern bureau werkzaamheden verricht voor de verantwoordelijke en zich daarbij volledig aan de instructies van de verantwoordelijke onderwerpt en uitsluitend onder diens verantwoordelijkheid gegevens opslaat, is het extern bureau bewerker (Registratiekamer 20 september 1993, 93.C.052). Een pensioenadviesbureau kan echter niet meer als bewerker worden beschouwd indien zij de gegevens tevens gebruikt voor een informatiesysteem dat zich onttrekt aan de onderliggende contractuele relatie. In dat geval verkrijgt het bureau immers de gegevens (mede) ten behoeve van zichzelf en wordt het (mede) verantwoordelijke. Soms blijkt de uitvoeringsadministratie nagenoeg geheel aan een adviesbureau te zijn uitbesteed. De opdrachtgever oefent dan geen zeggenschap meer uit. Ook in een dergelijk geval is het adviesbureau (mede)verantwoordelijke en geen bewerker[1]. De Registratiekamer noemt in haar advies een aantal vormen van dienstverlening met betrekking tot gegevensverwerking. Er is sprake van facilities management indien gebruik wordt gemaakt van de diensten van een serviceverlenend bedrijf op het gebied van de automatisering.[2] Dit bedrijf zet bijvoorbeeld een informatieverwerkend systeem ten aanzien van de salarisadministratie van de opdrachtgever onder eigen verantwoordelijkheid op, implementeert het en voert het uit ten huize van de

[1] Jaarverslag Registratiekamer 1989–1991, blz. 41–42).
[2] Handboek Bestuurlijke Informatiekunde, D1510–3.

opdrachtgever. Indien de opdrachtgever enkel de automatiseringsfunktie heeft uitbesteed en deze heeft losgekoppeld van de beleidsfunctie met betrekking tot de informatievoorziening (de aansturing, de zeggenschap over bijvoorbeeld welke gegevens worden opgenomen) en dit zodanig heeft neergelegd in zijn overeenkomst met het bureau, zal van het servicebureau niet kunnen worden gezegd dat het persoonsgegevens verwerkt. Brengt het ontwikkelen van het informatiesysteem met zich dat persoonsgegevens wel moeten worden verwerkt dan zal het bureau als bewerker moeten worden beschouwd. Soortgelijke opmerkingen kunnen worden gemaakt ten aanzien van de netwerkbeheerder. Een netwerkbeheerder is in de regel belast zijn met het inrichten, aanpassen en onderhouden van transmissienetten, inclusief de storingsbewaking.
Het is mogelijk dat de verantwoordelijke de verwerking van persoonsgegevens uitbesteed aan meerdere bewerkers. Zo kan een servicebureau zorg dragen voor de automatisering van de financiële administratie van de opdrachtgever verzorgen terwijl de opdrachtgever de daadwerkelijke uitvoering van de administratie aan een ander bureau heeft toevertrouwd. Uit de verantwoordelijkheid van de opdrachtgever – die in de zin van de wet geldt als verantwoordelijke voor de gegevensverwerking – vloeit voort dat hij uitdrukkelijk heeft ingestemd met het subbewerkersschap. Indien de opdrachtgever daarvoor in zijn overeenkomst met de bewerker uitdrukkelijk ruimte heeft gegeven, kan de bewerker – met behoud van zijn volle aansprakelijkheid voor de naleving van zijn contract met de verantwoordelijke – delen van de verwerking uitbesteden aan «subbewerkers». De bewerker dient dan wel contractueel verzekerd te hebben dat de subbewerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt. De verantwoordelijke dient hiervan wel op de hoogte te worden gesteld opdat deze in staat is toe te zien op de naleving van zijn afspraken met de bewerker (artikel 14).
Het is eveneens mogelijk dat in de overeenkomst tussen de dienstverlener en de opdrachtgever deze laatste zich de zeggenschap over de verwerking van persoonsgegevens voorbehoudt. Deze afspraak kan echter niet tot gevolg hebben dat de verantwoordelijkheid voor die verwerking anders komt te liggen dan uit de aard van de dienstverlening zou voortvloeien. Gelet op het feit dat een overeenkomst in principe alleen partijen kan binden, geldt dat de verantwoordelijke zich in dat geval alleen de verplichting aanvaardt om zich volgens de aanwijzingen van de opdrachtgever te gedragen. Aan de verantwoordelijkheid van de dienstverlener doet dit geen afbreuk. Dit geldt eveneens voor de wettelijke verplichtingen waaraan de verantwoordelijke zich moet houden.

Onderdeel f

De betrokkene is degeen waarover de gegevens informatie bevatten. In de WPR wordt deze persoon aangeduid als de «geregistreerde». Nu de registratie als object van regelgeving is verlaten, is ook het gebruik van de term, die naar een registratie verwijst, niet meer goed mogelijk. Het begrip «betrokkene» krijgt daardoor in dit wetsvoorstel een technische betekenis, die niet zonder meer strookt met het gewone taalgebruik. Het is de term die ook in de richtlijn wordt gebruikt. In de andere talen van de Unie doet zich hetzelfde voor, met uitzondering van de Engelse taal, waar het woord «data subject» wordt gebruikt. Een voor de hand liggende Nederlandse vertaling van dit woord is er niet. Daar het gaat om een technische term, is een afzonderlijke definitie vereist.
In de praktijk kan het voorkomen dat een gegeven op meer personen tegelijk betrekking heeft. Elk is dan betrokkene voor zichzelf en derde ten opzichte van de anderen. Te denken valt aan samenlevingsverhoudingen, begunstiging bij verzekeringen en aangifte van strafbare feiten.

Onderdeel g

De derde is degene, die niet de betrokkene, noch de verantwoordelijke, noch de bewerker en noch de persoon is die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om de gegevens te verwerken.
De begripsomschrijving van «derde» sluit inhoudelijk aan bij hetgeen reeds onder de WPR gold. De kring van «personen die onder rechtstreeks gezag van de verantwoordelijke gemachtigd zijn om gegevens te verwerken» sluit aan bij de personen die «binnen de organisatie van de houder» gegevens mogen ontvangen(zie de omschrijving van «verstrekken van gegevens aan een derde» in artikel 1, in samenhang gelezen met artikel 6, tweede lid, WPR). Uit de omschrijving van «derde» in het onderhavige artikel blijkt nu expliciet dat personen binnen de organisatie van de verantwoordelijke die niet onder zijn rechtstreeks gezag staan, als derden moeten worden aangemerkt. Verschillende rechtspersonen binnen een concern kunnen om die reden ten opzichte van elkaar in beginsel als derden worden beschouwd.
Het onderscheid tussen verantwoordelijke, bewerker en derde uit zich in de relatie die ze onderling hebben. Kent de persoon een hiërarchische relatie tot verantwoordelijke dan zal gesproken moeten worden van (intern) beheer. Gegevensverwerking vindt dan plaats binnen de organisatie van de verantwoordelijke en onder diens rechtstreeks gezag. Valt de persoon niet onder rechtstreeks gezag van de verantwoordelijke (geen hiërarchische relatie) echter is wel sprake van een relatie met de verantwoordelijke met betrekking tot de te verwerken gegevens (contractuele relatie), dan kan die persoon worden aangemerkt als bewerker. Valt de persoon niet onder rechtstreeks gezag van de verantwoordelijke en kent hij evenmin een contractuele relatie met betrekking tot de te verwerken gegevens met de verantwoordelijke, dan zal de persoon als derde zijn aan te merken. In tegenstelling tot de bewerker zal de derde de gegevens veelal voor eigen behoefte verwerken.
Het begrip «derde» speelt in dit wetsvoorstel een minder centrale rol dan in de WPR. In paragraaf 3 van de WPR is het begrip cruxiaal in het verstrekkingenregime dat van toepassing is. In paragraaf 9.2 van het algemeen deel van de toelichting is hier reeds op ingegaan. In de WBP speelt het begrip alleen nog een rol bij het verstrekken van bepaalde gevoelige gegevens (artikelen 17, derde lid, 19, tweede lid, en 20, tweede lid), het moment waarop een informatieplicht ontstaat (artikel 34, eerste lid, onder b) en in bepaalde gevallen als rechtvaardigingsgrond voor het verwerken van gegevens (bijvoorbeeld artikelen 8, onder f, en 22, vierde lid).

Onderdeel h

Ontvanger is degene aan wie de gegevens worden medegedeeld. De ontvanger kan zowel een persoon binnen de organisatie van de verantwoordelijke zijn als een persoon buiten de organisatie van de verantwoordelijke (bewerker of derde).
Het begrip «ontvanger» heeft in dit wetsvoorstel met name betekenis ten aanzien van de informatieverplichtingen van de verantwoordelijke. De verantwoordelijke moet de betrokkene onder bepaalde omstandigheden op de hoogte stellen van de bij de verwerking betrokken ontvangers of categorieën van ontvangers indien de betrokkene daarvan niet reeds op de hoogte is. Daarnaast speelt het begrip een rol bij de aanmeldingsverplichting: op grond van artikel 28 moeten ontvangers of categorieën ontvangers aan wie de gegevens kunnen worden verstrekt worden aangemeld bij de Registratiekamer.

Onderdeel i

De omschrijving van het begrip toestemming als «elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt» in onderdeel h komt overeen met die in artikel 2, onder h, van de richtlijn.
Om te kunnen spreken van een daadwerkelijk toestemming van de betrokkene zijn drie punten essentieel. Allereerst moet de betrokkene in vrijheid zijn wil kunnen uiten. Ten tweede moet de wilsuiting betrekking hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen en ten derde moet de betrokkene voor van een goede oordeelsvorming over de noodzakelijk inlichtingen beschikken[1]. Hieronder zal op de verschillende criteria nader worden ingegaan.
Allereerst geldt dat de betrokkene in vrijheid zijn wil met betrekking tot de betreffende gegevensverwerking moet kunnen uiten en dat deze wil ook daadwerkelijk geuit moet zijn. De artikelen 3:33 en 3:35 BW zijn in deze van overeenkomstige toepassing. Artikel 3:59 BW bepaalt immers dat deze bepalingen op een overeenkomstige wijze worden toegepast voor zover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet. Er kan bijvoorbeeld niet van een rechtsgeldige toestemming worden gesproken als de betrokkene onder druk van omstandigheden waarin hij verkeert of de relatie waarin hij staat tot de verantwoordelijke, tot toestemming is overgegaan. Van de sollicitant die op verzoek van de aspirant werkgever gegevens over zijn strafrechtelijk verleden bekend maakt, kan bezwaarlijk gezegd worden dat hij in vrijheid deze gegevens heeft verstrekt. Hij handelde immers onder druk van de wens aangenomen te worden door de werkgever. Als tweede voorwaarde geldt dat de wilsuiting van de betrokkene betrekking moet hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevens-verwerkingen. Duidelijk moet zijn welke verwerking, van welke gegevens, voor welk doel zal plaatsvinden, en als het daarbij gaat om een verstrekking aan derden, ook aan welke derden. In aansluiting op artikel 12 WPR betekent dit dat een zeer brede en onbepaalde machtiging tot het verwerken van gegevens niet als zodanig kan worden aangemerkt. De ondertekening door de betrokkene van een formulier voldoet niet aan dit criterium, als in het formulier een algemeen geformuleerde machtiging voor de verantwoordelijke is opgenomen, om de persoonsgegevens van de betrokkene te verwerken zonder nadere specificatie van bijvoorbeeld de categorieën van derden aan wie de verantwoordelijke de gegevens voornemens is te verstrekken en de soorten van gegevens die aan deze personen zullen worden verstrekt. Zo is ook de zinsnede in een contract met een reisagentschap, waarin de betrokkene toestemming geeft voor de verstrekking van persoonsgegevens aan een willekeurige derde voor de toezending van reclame, onvoldoende specifiek. De betrokkene moet weten om welke gegevensverwerking het gaat en hiervoor gerichte toestemming geven. Er kan evemin van een rechtsgeldige toestemming worden gesproken wanneer de betrokkene geconfronteerd wordt met een geheel andere gegevensverwerking dan waarvoor hij toestemming had verleend.
Als derde voorwaarde geldt het «informed consent»: de betrokkene kan slechts verantwoord zijn toestemming geven wanneer hij zo goed mogelijk is ingelicht. Dit houdt in dat indien de betrokkene onvoldoende geïnformeerd zijn toestemming verleent, de bepalingen van dit wetsvoorstel zijn overschreden. Het vragen van de toestemming van de betrokkene impliceert dat hij op de hoogte moet worden gesteld van de gang van zaken met betrekking tot de gegevensverwerking. Deze (informatie-)plicht berust in beginsel bij de verantwoordelijke c.q. bewerker. De betrokkene moet voldoende en begrijpelijk door de verantwoordelijke wordt geïnformeerd over de verschillende aspecten van

[1] In de angelsaksische literatuur ook wel aangeduid met de term «informed consent».

de gegevensverwerking die voor hem van belang zijn. De informatieplicht van de verantwoordelijke wordt begrensd door de feiten die de betrokkene reeds kent of zou moeten kennen. De informatieplicht van de verantwoordelijke impliceert niet dat de betrokkene geen enkele verantwoordelijkheid draagt. De betrokkene heeft een zekere onderzoeksplicht voor hij een oordeel geeft.
Bepalend voor de mate waarin de verantwoordelijke de betrokkene moet informeren dan wel de betrokkene zelf op onderzoek moet uitgaan is wat in het maatschappelijk verkeer redelijkerwijs mag worden verwacht. Dit zal moeten worden bepaald aan de hand van een weging van alle omstandigheden van het concrete geval. Factoren die bij weging een rol kunnen spelen zijn de betreffende soort gegevens, de verwerkingen die verantwoordelijke wil verrichten alsmede de context waarin deze verwerkingen zullen plaatsvinden, de eventuele derden aan wie de gegevens kunnen worden verstrekt enz., maar ook de maatschappelijke positie en onderlinge verhouding tussen de verantwoordelijke en de betrokkene alsmede de wijze waarop zij met elkaar in contact zijn getreden.
Artikel 12, eerste lid, WPR bepaalde dat indien voor de verstrekking van gegevens uit een persoonsregistratie toestemming van de geregistreerde is vereist, deze slechts schriftelijk kan worden gegeven. In het het wetsvoorstel is er vanaf gezien om voor de derdenverstrekkingen een extra voorwaarde te stellen met betrekking tot de toestemming die door de betrokkene moet worden gegeven. Evenmin is in het algemene toestemmingsvereiste zoals verwoord in de begripsomschrijving opgenomen de voorwaarde dat de betrokkene zijn toestemming slechts schriftelijk kan verlenen. Deze voorwaarde wordt te beknellend geacht met het oog op allerlei technologische ontwikkelingen, waarbij met name gedacht kan worden aan het gegevensverkeer via EDI[1]. Deze ontwikkelingen maken het immers mogelijk bij interactieve diensten toestemming geauthenticeerd elektronisch te verlenen: «met een simpele druk op de knop».
In het verlengde van de richtlijn wordt in het onderhavige wetsvoorstel naast het begrip «toestemming», eveneens de begrippen «ondubbelzinnige toestemming» en «uitdrukkelijke toestemming» gehanteerd. Zo wordt als algemene grond voor gegevensverwerking in artikel 8 onder a, de ondubbelzinnige toestemming van de betrokkene aanvaard. In artikel 23, eerste lid, onder a, wordt voorzien in een uitzondering op het verbod gevoelige gegevens te verwerken indien de betrokkene uitdrukkelijk heeft toegestemd in een hem betreffende verwerking, tenzij in de wetgeving van de Lid-Staat is bepaald dat het verbod niet door toestemming van de betrokkene ongedaan kan worden gemaakt. Deze begrippen stellen extra vereisten aan de toestemming die van de betrokkene verwacht wordt.
Als de verantwoordelijke de ondubbelzinnige toestemming van de betrokkene moet verkrijgen, mag hij niet uitgaan van toestemming indien deze geen opmerkingen maakt over de gegevensverwerking, daarbij uitgaande van de kennis die hij op grond van maatschappelijke opvattingen redelijkerwijs bij de betrokkene aanwezig mag achten. Elke twijfel moet bij hem zijn uitgesloten over de vraag òf de betrokkene zijn toestemming heeft gegeven en voor welke specifieke verwerkingen deze toestemming is gegeven. In de Duitstalige versie van de richtlijn luidt artikel 7, onder a, gesproken van «... dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn .. die betroffene Person ohne Zweifel ihre Einwilligung gegeben hat». Ten einde alle twijfel ten aanzien van de toestemming van de betrokkene uit te sluiten zal doorgaans op de verantwoordelijke een verdergaande informatieverplichting rusten dan in het geval de betrokkene heeft toe te stemmen in de hem betreffende gegevensverwerking. Er is sprake van een verschuiving van de bewijslast in de richting van de verantwoordelijke: als er twijfel is over de vraag of de betrokkene zijn toestemming heeft verleend dient hij te verifiëren of hij

[1] Electronic Data Interchange: elektronische communicatie waarbij juridisch bindende contracten ontstaan.

er terecht vanuit gaat dat de betrokkene er mee heeft toegestemd. Tot op zekere hoogte is hier een vergelijkbare situatie als bij de informatieverplichtingen van de verantwoordelijke op grond van de artikelen 33 en 34. Dit verifiëren hoeft niet noodzakelijkerwijs te leiden tot het vragen van een uitdrukkelijke toestemming. Ook anderszins kan de verantwoordelijke informatie verwerven die zijn twijfel dienaangaande wegneemt. Het is bijvoorbeeld mogelijk dat het gedrag van de betrokkene zodanig duidelijk is dat daaruit expliciet blijkt dat hij zijn toestemming verleent en voor welke specifieke verwerkingen deze toestemming geldt. Bij interactieve diensten zal bijvoorbeeld de klik met de muis of een aanslag op het toetsenbord van de computer ten einde de (koop-) overeenkomst te sluiten (veelal nog gevolgd door een aparte klik voor de bevestiging van de koopovereenkomst), als zodanig kunnen worden aangemerkt. Indien de betrokkene in het kader van de financiële afwikkeling van een transactie zijn smart card overhandigt aan de verantwoordelijke, dan zal de verantwoordelijke dit bijvoorbeeld mogen aanmerken als de ondubbelzinnige toestemming van de betrokkene voor de verwerking van zijn persoonsgegevens voor de financiële afwikkeling van deze transactie.
In geval de verantwoordelijke de uitdrukkelijke toestemming van de betrokkene dient te verkrijgen, dient de betrokkene expliciet zijn wil daaromtrent te hebben geuit. Een stilzwijgende of impliciete toestemming is onvoldoende: de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking. Deze expliciete wilsuiting kan op verschillende wijzen tot stand komen. Het meest voor de hand liggend is uiteraard de expliciete mondelinge of schriftelijke toestemming van de betrokkene voor de verwerking. Maar ook uit het gedrag van de betrokkene kan onder omstandigheden diens uitdrukkelijke toestemming worden afgeleid. Het invullen van een formulier ten behoeve van het aanvragen van een bepaalde dienst zal bijvoorbeeld onder omstandigheden als het verlenen van uitdrukkelijke toestemming door de betrokkene mogen worden beschouwd, namelijk indien het voor de betrokkene uit de context waarin hij het formulier invult, duidelijk is dat zijn persoonsgegevens worden verwerkt en voor welk doel. Ook indien de betrokkene in het kader van een specifieke gegevensverwerking om zijn persoonsgegevens wordt gevraagd en hij vervolgens zijn smart card overhandigt, mag de verantwoordelijke ervan uit gaan dat de persoonsgegevens op deze card mogen worden verwerkt enkel en alleen voor zover dat noodzakelijk is ten behoeve van die verwerking. Bij interactieve diensten zal deze uitdrukkelijke toestemming eerst aanwezig mogen worden geacht als de betrokkene zijn verzoek voor een specifieke dienst nog eens middels een aparte klik heeft bevestigd.
De verantwoordelijke heeft rekening te houden met een dubbele bewijslast. In de eerste plaats moet bij twijfel bewezen kunnen worden, dat een bepaalde toestemming is verleend en waarvoor. Daarnaast zal zo nodig bewezen moeten kunnen worden, dat de toestemming aan de gestelde eisen voldoet. Daarbij zal de verantwoordelijke ook moeten kunnen aantonen, dat hij bijvoorbeeld op het punt van informatieverstrekking aan de betrokkene, alles heeft gedaan wat redelijkerwijs van hem mocht worden verwacht.
Als de toestemming niet aan bovenstaande vereisten voldoet is zij nietig. Het grondrecht op de bescherming van de persoonlijke levenssfeer is een zaak van openbare orde. Artikel 3:40, eerste lid, BW bepaalt dat een rechtshandeling die door inhoud of strekking in strijd is met de goede zeden of de openbare orde, nietig is. De toestemming die met betrekking tot een bepaalde gegevensverwerking niet rechtsgeldig is gegeven, dient als nietig te worden beschouwd.
Een eenmaal gegeven toestemming tot het verzamelen van gegevens kan te allen tijde worden ingetrokken. Een dergelijke intrekking heeft echter geen consequenties voor gegevensverwerkingen die vóór het moment

van de intrekking hebben plaatsgevonden. Dit geldt voor alle soorten van verwerkingen. Gezien het dwingende karakter van dit voorschrift is dit expliciet bepaald in artikel 5, tweede lid.
De vraag kan worden gesteld in hoeverre toestemming, door de betrokkene verleend onder de werking van de WPR, rechtsgeldig is onder deze nieuwe wetsvoorstel. Dit is het geval indien deze toestemming voldoet aan alle voorwaarden die de nieuwe wetsvoorstel stelt, niet is verlopen of ingetrokken. Daarbij kan het eveneens gaan om een toestemming voor de verstrekking van gegevens aan een derde, als bedoeld in artikel 12 van de WPR, of een niet in de WPR geregelde toestemming. Daarbij moet er echter wel rekening mee worden gehouden dat de toestemming die de betrokkene onder het vigeur van de WPR heeft verleend, in verband met de reikwijdte van dit wetsvoorstel, geen betrekking hebben op bijvoorbeeld de verwerking van «losse» geautomatiseerd verwerkte gegevens noch op het verzamelen van gegevens zonder dat een registratie van deze gegevens wordt beoogd. Door het ruime begrip gegevensverwerking vallen deze verwerkingen wel onder de onderhavige wetsvoorstel. Zie ook de toelichting op artikel 5.

Onderdeel n

Het begrip «verstrekken van persoonsgegevens» moet ruim worden opgevat: het omvat iedere vorm van het bekend maken of ter beschikking stellen van persoonsgegevens, ongeacht de wijze waarop dit gebeurt. Het kan mondeling, schriftelijk of langs elektronische weg gebeuren maar ook door het overhandigen van een magneetband met gegevens. Ook het raadplegen van gegevens, bijvoorbeeld op cd-rom, valt onder verstrekken. Van verstrekken is ook sprake als een persoon over de schouder van een ander meekijkt naar bijvoorbeeld een bestand persoonsgegevens (zie Registratiekamer, 6 maart 1995, 94.V.177).

Onderdeel o

Het verzamelen van persoonsgegevens omvat het verkrijgen van die gegevens. Gegevens kunnen worden verkregen doordat ze bijvoorbeeld worden opgevraagd of worden gegenereerd door ordening van reeds aanwezige gegevens. Het enkele vragen naar persoonsgegevens, bijvoorbeeld een persoon benaderen met de vraag om zijn persoonsgegevens te mogen vernemen, valt niet onder het begrip «verzamelen». In dat geval is immers nog geen sprake van een «verkrijging van persoonsgegevens». Er is pas sprake van verzamelen van persoonsgegevens wanneer een of meer persoonsgegevens daadwerkelijk worden verworven. Alsdan gelden de normen van dit wetsvoorstel. Dat wil niet zeggen dat deze voorschriften geen effect hebben op de wijze waarop de gegevens worden verkregen, bijvoorbeeld een persoon wordt benaderd voor de gegevens. Indien dit op een onbehoorlijke wijze gebeurt zal geen sprake zijn van een rechtmatige verkrijging van gegevens in de zin van artikel 6. Artikel 33 schrijft voorts voor dat bij het benaderen van de betrokkene (dus vóór het moment van de verkrijging van de gegevens) de betrokkene in ieder geval op de hoogte wordt gesteld van de identiteit van de verantwoordelijke en de doeleinden van de verwerking waarvoor de gegevens bestemd zijn.
Het verzamelen van gegevens hoeft niet gepaard te gaan met de vastlegging van deze gegevens. Van verzameling is reeds sprake indien de gegevens worden verkregen en vervolgens terstonds worden vernietigd. De begrippen «verzamelen» en «verkrijgen» worden in (de toelichting bij) dit wetsvoorstel vaak als synoniemen gebruikt.

Artikel 2

Eerste lid

Het eerste lid brengt tot uitdrukking dat het wetsvoorstel ziet op iedere geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens alsmede op handmatig gevoerde gegevens, voor zover deze in een bestand voorkomen of bestemd zijn om daarin te worden opgenomen.
Van een geautomatiseerde verwerking is sprake indien gebruik wordt gemaakt van middelen en methoden van geautomatiseerde gegevensverwerking. Van een «gedeeltelijke geautomatiseerde verwerking» is sprake als bij een onderdeel van de verwerking tevens gebruik wordt gemaakt van andere middelen. Het onderscheid tussen handmatig en geautomatiseerde verwerkte of te verwerken gegevens is niet altijd in alle scherpte te maken. In de praktijk komt het voor dat een gegeven deels geautomatiseerd wordt gevoerd en deels handmatig wordt bijgehouden. Een handmatig bijgehouden hulpbestand van bron-documenten dat met betrekking tot de geautomatiseerd gevoerde gegevens een bewijsfunctie toekomt, valt onder hetzelfde regime als de op basis daarvan geautomatiseerd verwerkte gegevens. Ook komt het voor dat geautomatiseerd gevoerde gegevens en een handmatige gegevensverzameling onderling zodanig zijn verweven dat zij als één bestand moeten worden aangemerkt, bijvoorbeeld als met behulp van de geautomatiseerd gevoerde gegevens toegang kan worden verkregen tot het handmatige bestand. Er is sprake van één vorm van verwerking van persoonsgegevens als geautomatiseerde en niet geautomatiseerde gegevens een gemeenschappelijke bestemming hebben.
In tegenstelling tot de WPR is het wetsvoorstel ook van toepassing op handmatig verwerkte gegevens die nog niet in een bestand zijn opgenomen maar wel bestemd zijn om daarin te worden opgenomen. Uit de begripsomschrijving van een «persoonsregistratie» in de WPR volgt dat dit wetsvoorstel van toepassing is op de handmatig gevoerde gegevensverzameling die systematisch is aangelegd met het oog op een doeltreffende raadpleging van de persoonsgegevens. Onder het bereik van het wetsvoorstel valt ook de fase van vergaring van gegevens die in handmatige bestanden zullen worden opgenomen.
In navolging van het advies van de Registratiekamer is in het tweede gedeelte van de begripsomschrijving de verwerking van persoonsgegevens beperkt tot «de niet geautomatiseerde verwerking van persoonsgegevens...». Aangezien het eerste gedeelte van de omschrijving op de geautomatiseerde verwerkingen ziet en het begrip «bestand» in artikel 1 mede geautomatiseerde verwerkingen omvat, is deze beperking noodzakelijk. Dit heeft tot gevolg dat tevens de volledig handmatige verzameling van gegevens die bestemd zijn om in een geautomatiseerd bestand te worden opgenomen, onder het bereik van dit wetsvoorstel valt.

Tweede lid

Het tweede lid bevat de uitzonderingen op de toepasselijkheid van het wetsvoorstel.
Onderdeel a bevat een uitzondering voor gegevensverwerkingen die naar hun aard voor persoonlijk of huiselijk gebruik bestemd zijn. Dit is dezelfde uitzondering als die ook in de WPR voorkomt. Bij de totstandkoming van de richtlijn hebben de Raad van Ministers en de Europese Commissie hierover voor de notulen verklaard dat deze formulering er niet toe mag leiden dat de verwerking van persoonsgegevens door een natuurlijke persoon, waarbij deze gegevens niet worden verstrekt aan één of meer

personen, doch aan een onbepaald aantal personen, kan worden uitgesloten van de richtlijn.
Het «persoonlijk gebruik» ziet zowel op de situatie buiten het werk als daarbinnen. Veel beroepsbeoefenaars houden registraties in het kader van hun normale bedrijfsvoering. Deze vallen onder de werking van het wetsvoorstel, ook wanneer het om eenmansbedrijven gaat. Deze verwerkingen zullen in de regel van de meldingsplicht worden vrijgesteld, maar de materiële normen van het wetsvoorstel blijven van toepassing. Daarnaast houden vele beroepsbeoefenaren, ook in het kader van hun werk, eigen lijstjes bij, bijvoorbeeld adresbestanden van personen met wie zij regelmatig contact onderhouden. Zij hebben het karakter van persoonlijke aantekeningen, dienend als geheugensteun. Deze laatste zijn van de werking van het wetsvoorstel uitgezonderd. Dit wordt niet anders wanneer bij voorbeeld een secretaresse van de beroepsbeoefenaar in bijzondere gevallen ook daarvan kennis neemt. Zodra evenwel een verwerking beoogd is voor gebruik door meerdere personen, is het wetsvoorstel van toepassing.
Het «huiselijk gebruik» ziet op de situatie dat in een gezinssituatie persoonsgegevens worden verwerkt. Ook wanneer meerdere personen die gezamenlijk een huishouden voeren, gebruik maken van deze gegevens, is het wetsvoorstel niet van toepassing. Voorwaarde is wel dat het moet gaan om een duidelijk bepaalbare groep van personen.
De verwerkingen die uitsluitend ten dienste staan van de openbare informatievoorziening door pers, radio of televisie alsmede boeken en andere schriftelijke publikaties, en catalogiseringen daarvan vallen nu wel onder het bereik van het wetsvoorstel. Ten aanzien van de gegevensverwerkingen ten behoeve van de openbare informatievoorziening door pers, radio of televisie, zullen zoals blijkt uit artikel 3 een beperkt aantal artikelen van het wetsvoorstel van toepassing zijn. Verder vallen ook de persoonsregistraties in een archiefbewaarplaats als bedoeld in de Archiefwet 1962, in het kader van de uitvoering van de Kieswet en de openbare registers die bij wet zijn ingesteld[1] onder het bereik van de richtlijn.
De onderdelen b tot en met f maken, in overeenstemming met artikel 2, derde lid, WPR, verdere uitzonderingen op de toepasselijkheid van het wetsvoorstel. Het is de bedoeling dat wetten over gegevensverwerkingen waarop de WBP niet van toepassing is uitdrukkelijk in artikel 2 worden vermeld. Voor zover deze verwerkingen onder het bereik van de communautaire wetgeving vallen of kunnen komen te vallen, dienen zij wel in overeenstemming te zijn met de richtlijn.
Ten aanzien van de uitgezonderde gegevensverwerkingen zal de thans geldende specifieke wetgeving, te weten de Wet op de inlichtingen- en veiligheidsdiensten en de Wet politieregisters, blijven gelden. In de bestaande situatie zal daarom geen verandering optreden. Daarbij moet worden aangetekend dat niet kan worden uitgesloten dat de EG-richtlijn gegevensbescherming te zijner tijd een reflexwerking zal hebben op de verdere rechtsvorming op deze gebieden. De verschillen moeten worden gerechtvaardigd door de aard van de materie, niet door de herkomst van de regelgeving.

Beeld en geluid

Een afzonderlijke vraag kan rijzen over de toepasselijkheid van het wetsvoorstel in verband met de al dan niet geautomatiseerde verwerking van gegevens over bepaalde personen in de vorm van beeld en geluid. Blijkens artikel 33, tweede lid, van de richtlijn zal de Europese Commissie in het bijzonder op dit terrein in 2001 nadere voorstellen doen. Het volgende geldt in afwachting van deze voorstellen.
Het is duidelijk dat een verzameling van losse foto's van personen, bewaard in een oude schoenendoos of ingeplakt in een fotoboek niet valt

[1] artikel 2, eerste en tweede lid, WPR.

onder de reikwijdte van het wetsvoorstel. De verwerking vindt niet plaats langs geautomatiseerde weg en het gaat evenmin om een gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn. Hierbij is ook niet relevant of de foto's al dan niet zijn voorzien van een naam, want zolang de personen op de foto herkenbaar zijn gaat het immers om een persoonsgegeven. Wordt een fotoverzameling echter geordend volgens bepaalde criteria zodat de daarop weergegeven personen makkelijker kunnen worden teruggevonden bij raadpleging van het aldus aangelegde bestand, dan wordt daardoor het wetsvoorstel van toepassing.
Wat aldus geldt voor foto's, geldt meer in het algemeen voor geluid- of beeldmateriaal dat op de klassieke wijze is vastgelegd. Cassettebandjes, film- of videobanden, grammofoonplaten, televisie etc. zijn vormen van dergelijke vormen van klassieke vastlegging van informatie. Niet relevant is of het gaat om stilstaande of bewegende beelden. Zodra evenwel het materiaal min of meer toegankelijk is voor latere raadpleging, is het wetsvoorstel van toepassing. Het gaat daarbij telkens om geluid of beeld waaraan bepaalde informatie omtrent een persoon kan worden ontleend[1]. Een geluidsband bijvoorbeeld waarop een stem van een bepaalde persoon herkenbaar is, ook al is deze band niet voorzien van een naam, is ook informatie over die persoon.
In het bijzonder speelt dit bij digitaal verwerkt of te verwerken geluid of beeld. Bij digitale verwerking vormen de elementaire bouwstenen van het signaal waarin het gegeven is verwerkt een discrete waarde: een één of een nul, een plus of een min, een lichtpuls of geen lichtpuls. Tussenliggende waarden komen niet voor. Zodra informatie digitaal is vastgelegd is er in ieder geval sprake van geautomatiseerde verwerking van gegevens. In een geautomatiseerd systeem is immers het zoeken naar digitale gegevens mogelijk. Bijvoorbeeld iemands stem kent unieke informatie. Als de stem digitaal is vastgelegd is hij vergelijkbaar met een op een ander moment opgenomen en digitaal vastgelegde stem. In de toekomst is het in toenemende mate waarschijnlijk dat met gebruikmaking van geautomatiseerde beeld- en spraakherkenningstechnieken langs geautomatiseerde weg eenvoudig vast te stellen is of het om dezelfde persoon gaat. Hetzelfde geldt min of meer voor beeldmateriaal.
Hierdoor valt een digitale databank met beeltenissen of stemafdrukken op naam, bruikbaar voor de vaststelling van de identiteit van anonieme personen onder het bereik van het wetsvoorstel. Hetzelfde geldt voor de langs geautomatiseerde weg vastgelegde digitale informatie van een anonymus, waarvan de identiteit met behulp van een dergelijke databank mogelijk kan worden vastgesteld. Het feit dat langs geautomatiseerde weg geluid- of beeldvergelijking van digitaal vastgelegde informatie over iemand onvergelijkbaar veel sneller en nauwkeuriger kan plaatsvinden dan wanneer dit handmatig zou moeten geschieden, rechtvaardigt een aangescherpt juridisch regime.
In de praktijk betekent dit vooral dat betrokkenen op de hoogte moeten worden gesteld van het feit dat van hen opnamen worden gemaakt. De identiteit van de verantwoordelijke kan blijken uit de bevestiging van een videocamera aan een bepaald pand, waarvan de eigenaar, bijvoorbeeld omdat het een winkel betreft, duidelijk is. In andere gevallen zal bijvoorbeeld middels een duidelijke sticker de identiteit van de verantwoordelijke moeten worden kenbaar gemaakt. Wanneer het in bijzondere gevallen noodzakelijk zou zijn op één van de gronden van artikel 43 af te zien van een dergelijke informatieverstrekking vooraf, kan daarvan uiteraard worden afgezien.
Het bovenstaande geldt uiteraard evenzeer voor de vastlegging van gegevens van gedragingen van personen als zij iets, bijvoorbeeld een catalogus van een postorderbedrijf, consulteren op de elektronische snelweg en die tot die personen herleidbaar zijn. Bij een dergelijke on-line consultatie is het mogelijk om vast te leggen op welke plaatsen de

[1] Vgl. HR 30-10-1987, NJ 1988, 277.

gebruiker zich op de snelweg begeeft en de tijdspanne tussen elke klik van de muis van de computer vast te leggen. Dit geeft een vrij nauwkeurig beeld van iemands belangstelling. Wanneer deze gegevens anoniem zijn en niet meer tot een persoon te herleiden zijn, bijvoorbeeld opgeslagen met het oog op bijvoorbeeld marktonderzoek, dan valt de verwerking buiten de reikwijdte van het wetsvoorstel. Vindt de opslag evenwel plaats om individuele personen te benaderen met commerciële aanbiedingen, dan is het wetsvoorstel wel van toepassing.
Het bovenstaande heeft tot gevolg dat ook elke multimediale opslag van gegevens voor artistieke of journalistieke doeleinden of voor divertissement, zodra daar herkenbaar personen in voorkomen onder het wetsvoorstel vallen. Ook onder de WPR vielen overigens deze gegevens al onder het wetsvoorstel, omdat het daar ging om tot individuele personen herleidbare gegevens. De pers was echter in artikel 2, eerste lid, onder a, van de werking van deze wet. In artikel 3 is voorzien in een uitzondering voor bepaalde artikelen van dit wetsvoorstel, indien voor deze doeleinden gegevensverwerking plaatsvindt[1]. Voor het overige zal worden bezien in hoeverre dergelijke vormen van gegevensverwerking kunnen worden vrijgesteld van de aanmeldingsplicht.

Derde lid

Het derde lid voorziet in een voorwaardelijke uitzondering voor gegevensverwerkingen door de krijgsmacht in geval van daadwerkelijk operationeel optreden door Nederlandse militairen in het buitenland. Gedacht dient te worden aan de inzet van de krijgsmacht bij internationale crisisbeheersingsoperaties. Hoewel gegevensverwerkingen in dat kader veelal buiten Nederland zullen worden verricht, blijft de minister van Defensie hiervoor verantwoordelijk. Mede gelet op artikel 4 zou de wet zonder nadere voorziening van toepassing zijn.
Bij inzet in internationale crises kan evenwel niet altijd worden gevergd dat de wet onverkort wordt toegepast. De omstandigheden waarin de krijgsmacht dan soms moet functioneren laten zulks in bepaalde gevallen niet toe. Om die reden wordt in het derde lid de bevoegdheid toegekend aan de minister van Defensie om te bepalen dat de wet buiten toepassing kan blijven. De minister kan daartoe slechts beslissen indien dit met het oog op de inzet van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde nodig is. Met deze laatste formulering is aangesloten bij het nieuwe artikel 97 van het recent ingediende voorstel van Rijkswet tot wijziging van de bepalingen van de Grondwet inzake de verdediging. Ten slotte is bepaald dat de Registratiekamer van de beslissing van de minister – zo nodig achteraf doch zo spoedig mogelijk – in kennis dient te worden gesteld. Deze voorziening is er op gericht om een adequate controle op de toepassing van de wet mogelijk te maken. Met het oog daarop zal de beslissing van de minister om de wet buiten toepassing te laten, van een adequate motivering moeten zijn voorzien.

Artikel 3

Eerste lid

Deze bepaling is gebaseerd op artikel 9 van de richtlijn en is gericht op gegevensverwerkingen die uitsluitend op journalistieke, artistieke en literaire doeleinden zijn gericht. Voor zover het de journalistiek betreft worden dergelijke verwerkingen thans in artikel 2 WPR geheel uitgezonderd. Als gevolg van artikel 9 richtlijn kan een dergelijke algehele uitzondering niet zonder meer worden gecontinueerd. In genoemd artikel wordt bepaald dat de lid-staten voor de verwerking van persoonsgegevens moeten voorzien in de uitzonderingen op of afwijkingen van de bepalingen van de hoofdstukken II, IV en VI die nodig blijken om het recht

[1] Zie ook overweging 17 bij de richtlijn: «overwegende dat wat betreft de verwerkingen van geluid- en beeldgegevens voor journalistieke literaire of artistieke doeleinden, de beginselen van de richtlijn overeenkomstig artikel 9, met name audiovisuele, met een aantal beperkingen van toepassing zijn;»

op persoonlijke levenssfeer te verzoenen met de vrijheid van meningsuiting. Dit betekent dat, anders dan krachtens de WPR het geval is, de verwerking van persoonsgegevens voor genoemde doeleinden in beginsel onder het regime van de richtlijn valt. De lidstaten dienen nader te bezien in hoeverre uitzonderingen op dat regime noodzakelijk zijn met het oog op het waarborgen van de vrijheid van meningsuiting.
In de situatie waarin persoonsgegevens voor journalistieke, artistieke of literaire doeleinden worden verwerkt zal sprake kunnen zijn van een botsing van grondrechten. Het algemene uitgangspunt bij de beoordeling van dergelijke botsingen is dat er tussen grondrechten geen rangorde bestaat. Dat is in overeenstemming met vaste jurisprudentie. De rechter pleegt binnen de algemene privaatrechtelijke kaders aan de hand van de omstandigheden van het concrete geval een afweging te maken tussen het belang dat gediend is met de vrijheid van meningsuiting en het belang van het recht op eerbiediging van de persoonlijke levenssfeer. Geen van beide rechten heeft in algemene zin voorrang. Vanuit deze algemene optiek dient de wetgever af te wegen welke uitzonderingen voor de journalistiek moeten worden gecreëerd.
De vrijheid van meningsuiting is neergelegd in artikel 10 EVRM, artikel 19 IVBPR en artikel 7 van de Grondwet. De vrijheid van meningsuiting is met het oog op het goed functioneren van een democratische samenleving van grote betekenis. Dit laatste vindt nadrukkelijk bevestiging in de jurisprudentie van het Europese Hof voor de Rechten van de Mens. Hieruit volgt dat de wetgever buitengewoon terughoudend dient te zijn met het stellen van beperkingen aan dit recht. Beperkingen zijn alleen mogelijk indien bij de wet voorzien en noodzakelijk in een democratische samenleving in het belang van een aantal limitatief opgesomde doeleinden.
Tegen deze achtergrond is het ongewenst om de richtlijn onverkort van toepassing te laten zijn op journalistieke activiteiten. De beperkende voorschriften die voortvloeien uit de richtlijn zijn veelal een te vergaande belemmering voor dergelijke activiteiten. De in de richtlijn voorgeschreven meldings- en informatieverplichtingen zouden tot gevolg hebben dat de journalistieke vrijheid om gegevens te vergaren, te registreren en te analyseren als voorbereiding op eventuele publicaties, te zeer wordt beknot. Datzelfde geldt voor de uitoefening van het inzage- en correctierecht, het recht van verzet en de bevoegdheden van de Registratiekamer om bijvoorbeeld voorafgaand onderzoek te doen. De betreffende onderdelen van het wetsvoorstel zijn dan ook uitgezonderd.
Anderzijds brengt de toenemende betekenis van het recht op eerbiediging van de persoonlijke levenssfeer mee dat andere onderdelen van het wetsvoorstel wel van toepassing zullen zijn. De richtlijn geeft daarvoor een aantal indicaties. Artikel 9 en de daaraan ten grondslag liggende overweging 37 laten zien dat in elk geval geen uitzonderingen mogelijk zijn op de regels inzake aansprakelijkheid, sancties, beroep op de rechter, gedragscodes en beveiliging. Afgezien van de bepalingen van hoofdstuk 1, achten wij het daarnaast gewenst dat de pers gebonden is aan de algemene beginselen inzake gegevensverwerkingen zoals neergelegd in artikel 6 en 7 van de richtlijn. Deze beginselen geven enerzijds algemene zorgvuldigheidsgrenzen die ook degene die de gegevens verwerkt voor de hiervoor bedoelde doeleinden in acht heeft te nemen en bevatten anderzijds voldoende ruimte voor afwegingen waarbij de vrijheid van meningsuiting op toereikende wijze aan bod kan komen. De binnen dit kader te maken afwegingen zullen in belangrijke mate aansluiten bij de huidige jurisprudentie.
In Europees verband omvat de grondrechtelijke bescherming meer dan de persvrijheid. Zoals ook blijkt uit overweging 37 van de richtlijn beschermt artikel 10 EVRM de uitingsvrijheid in brede zin, in het bijzonder de vrijheid om inlichtingen te ontvangen of te verstrekken. In het verlengde hiervan bevat artikel 9 van de richtlijn niet alleen een afwijkingsbevoegdheid voor verwerkingen voor journalistieke, maar ook voor artistieke en literaire

doeleinden. Daarbij valt tevens te denken aan bepaalde gegevensverwerkingen die plaatsvinden bij bibliotheken en musea. Conform de richtlijn worden dergelijke gegevensverwerkingen op één lijn geplaatst met journalistieke gegevensverwerkingen.
Een en ander leidt tot de conclusie dat conform artikel 3, eerste lid, het wetsvoorstel niet van toepassing zal zijn op gegevensverwerkingen voor uitsluitend journalistieke, artistieke en literaire doeleinden, behoudens de bepalingen van het eerste hoofdstuk, alsmede de artikelen 6 tot en met 11, 13 tot en met 15, 25 en 49. In genoemde bepalingen worden de hiervoor aangeduide onderdelen geregeld. De formulering van artikel 3, eerste lid, is overigens grotendeels gebaseerd op het huidige artikel 2 WPR waar een vergelijkbare terminologie wordt gehanteerd.
Anders dan in het huidige artikel 2 WPR wordt niet meer geregeld dat het dient te gaan om gegevensverwerkingen door pers, radio of televisie. Krachtens de richtlijn gaat het er niet om wie de gegevens verwerkt, maar voor welke doeleinden zulks geschiedt. In dit licht bezien vormt artikel 3 ten opzichte van het geldende recht een verruiming van de afwijkingsmogelijkheid, aangezien ook anderen dan vertegenwoordigers van pers, radio of televisie gegevens voor de genoemde doeleinden kunnen verwerken. Het laatste vergt wel nauwkeurige interpretatie. Afhankelijk van de feitelijke omstandigheden zal moeten worden beoordeeld of een verwerking uitsluitend voor een van de genoemde doeleinden plaatsvindt. De exploitatie van op basis daarvan aangelegde gegevensbestanden voor andere dan journalistieke, artistieke of literaire doeleinden valt buiten de reikwijdte van de in artikel 3 geregelde uitzondering.

Tweede lid

Voorts is in het tweede lid bepaald dat gevoelige gegevens als bedoeld in artikel 16 van het wetsvoorstel, mogen worden verwerkt voor zover dit voor de in het eerste lid genoemde doeleinden noodzakelijk is. Gevoelige gegevens vormen een bijzondere categorie die krachtens de richtlijn extra bescherming dienen te krijgen. Publicatie ten behoeve van journalistieke, artistieke en literaire doeleinden moet echter worden beschouwd als een «zwaarwegend algemeen belang» in de zin van artikel 8, vierde lid, van de richtlijn ten behoeve waarvan ook verwerking van gevoelige gegevens noodzakelijk kan zijn. Artikel 3, tweede lid, stelt dit buiten twijfel. De bevoegdheid tot een zodanige gegevensverwerking is echter niet onbeperkt. Bij de toepassing van de noodzakelijkheidsnorm zal degene die de gegevens verwerkt steeds moeten afwegen of de betreffende verwerking voldoen aan beginselen van proportionaliteit en subsidiariteit. Voor zover het gaat om verwerking voor journalistieke doeleinden gaat de begrenzing van de noodzakelijkheidseis niet zover dat verwerking van gevoelige gegevens alleen is toegestaan indien vaststaat dat deze uitmondt in een publicatie. In de praktijk is soms tot het laatste moment onzeker of journalistieke werkzaamheden zullen leiden tot een publicatie. In dit licht bezien kan dan ook slechts de enkele verzameling van gegevens al noodzakelijk zijn als in dit artikel bedoeld.

Artikel 4

Dit artikel geeft uitvoering aan artikel 4 van de richtlijn en hieraan zijn de overwegingen 19 tot en met 21 gewijd. Het grenst de toepasselijkheid van de Nederlandse wet af tegenover de wetgeving van andere landen, ongeacht of deze al dan niet deel uitmaken van de Europese Unie. Dit onderwerp wordt thans in de WPR geregeld in de artikelen 47 tot en met 49. De WPR gaat uit van de gedachte dat het mogelijk is een uitspraak te doen over de plaats van een registratie. Op het moment van de totstandkoming van deze wet, was dat nog een zinnig uitgangspunt. Bevindt deze plaats zich binnen de Nederlandse rechtsmacht, dan is het wetsvoorstel

van toepassing. De artikelen 47 tot en met 49 geven aanvullende voorschriften wanneer enige voor Nederland van belang zijnde vormen van gegevensverwerking plaatsvinden.
In artikel 4 van het onderhavige wetsvoorstel wordt het voorwerp van regelgeving gevormd door de niet meer aan een bepaalde plaats toe te schrijven «gegevensverwerking». Het gevolg hiervan is dat, voor zover gegevensverwerking nog in verband staat met een bestand, de toepasselijkheid van de wettelijke voorschriften niet meer afhankelijk is van de plaats waar het betreffende bestand zich bevindt. In plaats daarvan is het aangrijpingspunt van het wetsvoorstel de plaats waar de verantwoordelijke is gevestigd. Heeft een verantwoordelijke meerdere vestigingen in de Europese Unie, dan dient hij ervoor zorg te dragen dat elk van de vestigingen voldoet aan de regels van het land waar de vestiging zich bevindt.
Deze regeling sluit beter aan bij de informatietechnologische ontwikkeling waarbij gegevens in toenemende mate een immaterieel karakter krijgen en daarmee een plaatsbepaling komen te ontberen. De klassieke regels voor de bepaling van het toepasselijk recht zijn dan niet toepasbaar. Niet meer de plaats van de gegevens of van het bestand, maar de plaats van vestiging van de verantwoordelijke voor deze gegevens wordt het aanknopingspunt voor jurisdictie. Slechts in het eerste lid, onder b, bleek een concessie aan deze benadering onontkoombaar. Wanneer de verantwoordelijke niet gevestigd is binnen de Europese Unie en met behulp van in Nederland zich bevindende middelen persoonsgegevens verwerkt, dan vindt de toepasselijkheid van het Nederlands recht zijn aanknopingspunt in de locatie van de voor de gegevensverwerking gebruikte fysieke middelen. De onderwerpen die worden geregeld in de artikelen 47 tot en met 49 WPR vinden daardoor voor een deel impliciet een regeling in dit artikel.
Uit de tekst van artikel 4 van de richtlijn blijkt dat onder het begrip «vestiging» in de richtlijn wordt verstaan: één of meerdere centra van economische activiteit, die zich in verschillende staten van de Unie kunnen bevinden. Uit overweging 19 blijkt ook dat niet relevant is of het nu gaat om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid. De vestiging op het grondgebied van een Lid-Staat veronderstelt het effectief en daadwerkelijk uitoefenen van activiteiten voor een onbepaalde periode. De rechtsvorm van een dergelijke vestiging, of het nu gaat om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid, is niet doorslaggevend. In een concreet geval zal dus aan de hand van de feiten moeten worden vastgesteld of sprake is van een vestiging in de zin van de richtlijn en derhalve sprake is van toepasselijkheid van het nationale recht. Is er een uitoefening van economisch activiteit van tijdelijke en voorbijgaande aard, waartoe wellicht zelfs een tijdelijk onderkomen is verworven, dan kan niet worden gesproken van een vestiging en is het recht van toepassing op de vestiging van de verantwoordelijke.[1]
Jurisprudentie van het Europese Hof van Justitie op dit punt is onder meer te vinden in de zaak 205/84, Duitse verzekeringen[2]. De keerzijde van deze jurisprudentiële precisering is, dat het Nederlandse recht niet van toepassing is op vormen van gegevensverwerking in Nederland door verantwoordelijken die niet over een dergelijke vaste vestiging in Nederland beschikken. Wanneer er geen sprake is van «vestiging», is er sprake van het aanbieden van diensten in de zin van artikel 59 van de EG-verdrag en hierop is het recht van de vestigingsplaats van de verantwoordelijke die deze diensten aanbiedt van toepassing[3]. Uit het oogpunt van bescherming van de persoonlijke levenssfeer verbiedt artikel 1, tweede lid, van de richtlijn aan een dergelijk aanbod van diensten beperkingen op te leggen, indien op de verantwoordelijke het recht van één van de andere lid-staten van de Europese Unie van toepassing is. In dat geval moet in Nederland vreemd recht worden toegepast, zoals dit

[1] zie overweging 19 van de richtlijn.
[2] Jur. 1986, blz. 3755, r.o. 21.
[3] zie de uitspraak van het Europese Hof van Justitie van 10 mei 1995, NJ 1995, 703.

ook bijvoorbeeld in het internationaal privaatrecht voorkomt. Dit vreemde recht kan afwijken van het Nederlandse, doch slechts binnen de marges die de richtlijn toestaat. Wanneer het echter gaat om de aantasting van de Nederlandse openbare orde, dan wijkt de toepassing van vreemd recht. Worden bijvoorbeeld door een verantwoordelijke vanuit het buitenland in Nederland strafbare feiten gepleegd, dan is het Nederlands strafrecht van toepassing.
Wat betreft het aanbod van diensten uit landen van buiten de Unie kan het volgende worden opgemerkt. Wanneer dit aanbod bestaat uit de verwerking van persoonsgegevens binnen Nederland, daaronder begrepen het verzamelen van gegevens, is ingevolge de algemeen geldende regels het Nederlandse recht van toepassing. Het voorwerp van regelgeving is immers het ruime begrip «gegevensverwerking». Het wetsvoorstel eist van de verantwoordelijke van buiten de Unie dat hij in Nederland een vertegenwoordiger aanwijst die daardoor op Nederlands territoir aansprakelijk is voor de naleving van de wettelijke regels met betrekking tot de van buiten de Unie verrichte verwerking van persoonsgegevens op Nederlands territoir. Daarenboven stellen de artikelen 76 tot en met 78 bijzondere eisen wanneer sprake is van vormen van gegevensverwerking die leiden tot de doorgifte van persoonsgegevens aan landen buiten de Europese Unie.
Het bovenstaande geldt niet met betrekking tot andere landen, zowel binnen als buiten de Unie, voor wat betreft de toepasselijkheid van de in artikel 75 strafbaar gestelde gedragingen. Hetzelfde geldt met betrekking tot de regeling van de bevoegdheden van de Registratiekamer (zie artikel 28, zesde lid, van de richtlijn) en de beveiligingsverplichting, bedoeld in artikel 17, eerste lid (zie artikel 17, derde lid, tweede gedachtenstreepje, van de richtlijn).
Overweging 21 van de richtlijn stelt buiten twijfel dat de territorialiteitsregels inzake het strafrecht door de richtlijn onverlet worden gelaten. Daar waar bij de implementatie van de richtlijn bepaalde gedragingen zijn strafbaar gesteld, zijn de artikelen 1 tot en met 8 van het Wetboek van Strafrecht in samenhang met artikel 91 van het Wetboek van Strafrecht van toepassing. Dit betekent bijvoorbeeld dat wanneer een verantwoordelijke, gevestigd binnen of buiten de Unie, persoonsgegevens verzamelt zonder de betrokkene daarvan in kennis te stellen in geval van raadpleging of dienstverlening via telecommunicatie langs geautomatiseerd weg naar Nederlands recht strafbaar is. Volgens de vaste jurisprudentie van de Hoge Raad is namelijk het Nederlands strafrecht van toepassing op een gedraging waarvan het gevolg in Nederland zich afspeelt, ook al bevindt de dader zich in het buitenland. Het strafbaar feit wordt dan geacht (mede) in Nederland te zijn begaan.
In veel gevallen zal een eventuele strafvervolging bij verstek worden afgedaan, en de veroordeelde zal in het opsporingsregister vermeld worden. Wanneer de veroordeelde bijvoorbeeld op Schiphol aankomt en de termijn van verjaring nog niet is ingetreden, kan de straf ten uitvoer worden gelegd. Ditzelfde geldt wanneer het strafbaar feit met een bestuursrechtelijke boete afgedaan is. De alternatieven om een verzoek tot overneming van de strafvervolging te doen of om uitlevering te vragen, komen bij deze categorie van strafbare feiten minder snel in beeld en zijn daarom van meer theoretische aard.
Overigens is het Nederlandse strafrecht eveneens van toepassing als vanuit Nederland een verantwoordelijke in het buitenland een dergelijk strafbaar feit pleegt. Zou een Nederlandse verantwoordelijke via telecommunicatie in het buitenland onopgemerkt persoonsgegevens vergaren, dan kan in Nederland een strafvervolging tegen hem worden ingesteld, bijvoorbeeld naar aanleiding van een klacht uit dat buitenland als reactie op het gebruik van de aldus vergaarde gegevens.
Artikel 4, eerste lid, onder b, van de richtlijn bepaalt «Elke Lid-Staat past zijn nationale, ter uitvoering van deze richtlijn vastgestelde bepalingen toe

op elke verwerking van persoonsgegevens: ... «b) waarvan de voor de verwerking verantwoordelijke niet gevestigd is op het grondgebied van de Lid-Staat, maar in een plaats waar de nationale wet uit hoofde van het internationale publiekrecht van toepassing is;».
Deze bepaling behoeft geen bijzondere implementatie. Uit het volkenrecht – daaraan kan een nationale wet niets veranderen – vloeit voort dat de Nederlandse wetgeving van toepassing is op bijvoorbeeld schepen, luchtvaartuigen en Nederlandse ambassades of andere diplomatieke vertegenwoordigingen in het buitenland. Daar de WBP deel zal uitmaken van het Nederlandse recht, heeft dit automatisch tot gevolg dat het met dit onderdeel van de richtlijn beoogde resultaat wordt bereikt.
Het derde lid[1] geeft ten slotte uitvoering aan artikel 4, tweede lid, van de richtlijn en moet worden gezien in samenhang met de bepalingen over het verkeer van persoonsgegevens met landen buiten de Europese Unie. De algemene gedachte is dat de regelgeving zo moet zijn ingericht dat deze niet gemakkelijk met de moderne informatietechnologische middelen kan worden omzeild. De bepaling vormt het sluitstuk op de regelgeving in die zin dat een verantwoordelijke van buiten de Europese Unie geen gegevens mag verwerken, zonder in in de vorm van een vertegenwoordiger een aangrijpingspunt voor rechtstoepassing te bieden. Overeenkomstig het advies van de Registratiekamer is in artikel 75 de overtreding van dit voorschrift strafbaar gesteld.
Uit de samenhang met artikel 4, tweede lid, blijkt dat wanneer slechts sprake is van doorvoer van gegevens, deze bepaling niet van toepassing is. In die gevallen is er immers niemand in Nederland die enige feitelijke macht over de gegevens kan uitoefenen. Zodra daarentegen sprake is van opslag van gegevens onder verantwoordelijkheid van iemand van buiten de Unie, dient deze een vertegenwoordiger aan te wijzen in Nederland.

Artikel 5

In artikel 5 zijn nadere voorschriften opgenomen ten aanzien van het toestemmingsvereiste. In het eerste lid is een aan artikel 11, vierde lid, van de WPR vergelijkbare regeling getroffen voor handelingsonbekwamen. Het tweede lid is ontleend aan artikel 12, derde lid, van de WPR. Zie ook de toelichting op artikel 1, onder h.

HOOFDSTUK 2 BEGINSELEN BETREFFENDE DE RECHTMATIGHEID VAN DE GEGEVENSVERWERKING

PARAGRAAF 1 ALGEMENE BEGINSELEN BETREFFENDE DE GEGEVENSVERWERKING

Artikel 6

Dit voorschrift bepaalt dat persoonsgegevens in overeenstemming met de wet, behoorlijk en zorgvuldig moeten worden verwerkt. Het geeft uitvoering aan artikel 6, eerste lid, onder a, van de richtlijn dat voorschrijft dat persoonsgegevens op eerlijke en rechtmatige wijze moeten worden verwerkt. Een dergelijke algemene norm was niet opgenomen in de WPR maar vloeide voort uit hetgeen in het ongeschreven recht in het maatschappelijk verkeer betaamt en – voor zover het de overheidssector betrof – uit de algemene beginselen van behoorlijk bestuur.
In de authentieke Engelse en Franse tekst van de richtlijn wordt gesproken van «processed fairly en lawfully» onderscheidenlijk «traitées loyalement et licitement». Deze terminologie sluit aan bij de authentieke teksten van het Verdrag inzake gegevensbescherming. De term «fair» heeft in het buitenland gediend als een bron voor de ontwikkeling van nieuwe behoorlijksregels op het terrein van de gegevensbescherming. De herkomst van «fair» sluit bijvoorbeeld aan bij Angelsaksische begrippen

[1] In de tekst die om advies is aangeboden aan de Registratiekamer werd deze bepaling aangeduid als artikel 5.

over een behoorlijke en fatsoenlijke omgang met medeburgers en hun belangen en heeft in de Angelsaksiche jurisprudentie een uitgekristalliseerde betekenis gekregen. In de Duitse wetgeving is bepaald dat – wil er sprake zijn van een eerlijke gegevensverkrijging – persoonsgegevens bij de betrokkene zelf dienen te worden verzameld tenzij aan specifieke voorwaarden is voldaan (artikel 13 BDSG). De Nederlandse vertaling «eerlijk en rechtmatig» van de genoemde bepalingen is in het onderhavige artikel 6 niet overgenomen om de volgende redenen. Zouden persoonsgegevens «oneerlijk» worden verwerkt, dan is dit in het Nederlands recht in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt. Blijkens artikel 6:162 BW is er dan al sprake van onrechtmatigheid. Daardoor wordt het begrippenpaar «eerlijk en rechtmatig» een tautologie. Bovendien heeft het woord «eerlijke gegevensverwerking» in het Nederlands recht geen specifieke juridische betekenis. Daaraan doet geen afbreuk het feit dat er jurisprudentie is ontwikkeld met betrekking tot het begrip «eerlijke behandeling» in artikel 6 EVRM. Het advies van de Registratiekamer om het begrip op te nemen in artikel 6 wordt daarom ook niet opgevolgd. Belangrijker is in deze aansluiting te zoeken bij reeds bestaande Nederlandse wetgeving. Het voorschrift dat gegevens op een behoorlijke en zorgvuldige wijze moeten worden verwerkt, sluit beter aan bij de vereiste maatschappelijke zorgvuldigheid die men in acht heeft te nemen ten einde een onrechtmatige daad te voorkomen.
Artikel 6 keert zich dus onder meer tegen die vormen van gegevensverwerking die naar Angelsaksische traditie als «unfair» of «oneerlijk» worden beschouwd. Voorwaarde voor een eerlijke verwerking van gegevens is – zo stelt een overweging 38 bij de richtlijn – dat de betrokkenen van het bestaan van de verwerkingen kennis kunnen hebben en, wanneer van hen gegevens worden verkregen, daadwerkelijk en volledig worden ingelicht over de omstandigheden waaronder deze gegevens worden verkregen. Praktijken waarbij bij voorbeeld onopgemerkt gegevens omtrent personen worden vergaard en verwerkt, al dan niet met behulp van technische hulpmiddelen, zijn dus ongeoorloofd. In het Nederlands strafrecht hebben deze noties een neerslag gekregen in 1971 (artikelen 139a e.v. Wetboek van Strafrecht[1]. Daarbij zijn de strafbepalingen opgenomen tegen het illegaal afluisteren van (telefoon)gesprekken en het illegaal maken van afbeeldingen van personen met heimelijk opgestelde camera's in niet voor het publiek toegankelijke ruimten.
Het woord «wet» heeft mede betrekking op andere wetgeving inzake de verwerking van persoonsgegevens. Het gaat hier dus om een schakelbepaling die verzekert, dat de betrokken regelingen in onderling verband van toepassing zijn.

Artikel 7

Artikel 7 schrijft voor dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. In dit voorschrift is naar de inhoud artikel 4 WPR overgenomen: er moet sprake zijn van een welbepaald doel dat echter tevens gerechtvaardigd dient te zijn (waartoe het belang van de verantwoordelijke redelijkerwijs aanleiding geeft en dat niet in strijd is met de wet, openbare orde of de goede zeden).
Artikel 9, eerste lid, bepaalt in aansluiting hierop dat de gegevens (vervolgens) niet mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Dit voorschrift sluit aan bij artikel 6, eerste lid, WPR (de in een registratie opgenomen gegevens worden slechts gebruikt voor doeleinden die met het doel van de registratie verenigbaar zijn).
Beide voorschriften geven uitdrukking aan het beginsel van de doelbinding. De doelbinding dient reeds bij het verzamelen van gegevens

[1] Wet van 7 april 1971, houdende enige strafbepalingen tot bescherming van de persoonlijke levenssfeer (Stb. 180).

aanwezig te zijn. Niet alleen dient er dan sprake te zijn van een uitdrukkelijk en welbepaald doel waarvoor de gegevens worden verzameld. Ook dient dat doel gerechtvaardigd te zijn (artikel 7).
Artikel 8 bevat een limitatieve opsomming van gronden voor toelaatbare gegevensverwerking. Van «gerechtvaardigde doeleinden» kan alleen sprake zijn als deze met inachtnemingvan artikel 8 kunnen worden bereikt. Indien op grond van artikel 8 kan worden gesproken van een «gerechtvaardigd doeleinde» is daarmee voldaan aan het vereiste van artikel 7 dat persoonsgegevens moeten zijn verkregen voor een gerechtvaardigd doeleinde. Daarnaast vereist artikel 7 dat dit doeleinde welbepaald en uitdrukkelijk moet zijn omschreven. De realisering van deze doeleinden zal in alle stadia van de gegevensverwerking moeten kunnen steunen op één of meer van de in artikel 8 genoemde gronden voor gegevensverwerking. Indien bijvoorbeeld een doel alleen bereikbaar is als persoonsgegevens in strijd met artikel 8 worden bewaard of aan een derde verstrekt, is niet voldaan aan het vereiste van een «gerechtvaardigd doel» en mogen de betrokken gegevens op grond van artikel 7 ook niet worden verzameld. Dit geldt ook indien de realisering van het doel anderszins in strijd zou zijn met het geschreven of ongeschreven recht. De vergaring van gegevens met het doel daarmee illegale activiteiten te verrichten, zal – wegens strijd met artikel 8 – dan ook op artikel 7 afstuiten. Ten aanzien van gevoelige gegevens gelden specifieke eisen (paragraaf 2 van hoofdstuk 2).
Artikel 9 bevat het sluitstuk van het doelbindingsvereiste. Dit artikel schrijft het doel waarvoor de gegevens zijn verkregen als uitgangspunt en toetsingskader voor voor iedere vorm van (verdere) gegevensverwerking. Gegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Gegevens mogen dus wel worden gebruikt voor andere doeleinden dan waarvoor zij zijn verzameld. Doch dit andere doel dient verenigbaar te zijn met het oorspronkelijke.
Persoonsgegevens mogen enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen. «Welbepaald en uitdrukkelijk omschreven» houdt in dat men geen gegevens mag verzamelen zonder een precieze doelomschrijving. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat. «Welbepaald» houdt in dat deze doelomschrijving duidelijk moet zijn, niet zo vaag of ruim bij voorbeeld dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden over de gegevens nodig zijn voor dat doel of niet. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. Uitdrukkelijk omschreven houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven bij de melding die hij op grond van artikel 27 verplicht is te doen. In de gevallen dat hij op grond van artikel 29 van de melding is vrijgesteld, geldt het doel dat bij algemene maatregel van bestuur is omschreven op grond van artikel 29 tweede lid, onder a.
In aansluiting op artikel 6 van de richtlijn wordt in artikel 7 uitdrukkelijk gesproken van «doeleinden». In artikel 4 WPR is sprake van «een bepaald doel». In de praktijk komt het niettemin geregeld voor dat een doelomschrijving uit meerdere onderdelen bestaat. In dat verband kan sprake zijn van één hoofddoel met nevendoelen, één hoofddoel met subdoelen, of enkele naast elkaar staande doelen. In het eerste geval zal het hoofddoel als de eigenlijke doelstelling kunnen worden beschouwd terwijl de nevendoelen slechts aangeven voor welke doeleinden de gegevens tevens zullen worden gebruikt. Op grond van artikel 9 van dit wetsvoorstel zullen deze nevendoeleinden verenigbaar moeten zijn met het hoofddoel. In de twee andere gevallen worden de onderdelen van de doelstelling elk afzonderlijk getoetst aan artikel 7 van dit wetsvoorstel, waarbij wordt gelet op de onderliggende rechtsverhouding. Dit kan zich met name voordoen bij bedrijven en instellingen die uiteenlopende diensten leveren en die met hun cliënten dus ook uiteenlopende rechtsverhoudingen kunnen hebben. In dergelijke gevallen wordt de doelstelling

of het betrokken onderdeel daarvan onder meer ingekleurd door wat uit de onderliggende verhouding voortvloeit. Tegen die achtergrond is ook van belang dat de onderdelen van de doelstelling onderling verenigbaar zijn. Dit om te voorkomen dat gegevens die voor een bepaald doel zijn verzameld in strijd met artikel 9 van dit wetsvoorstel voor andere onderdelen worden gebruikt. Met een abstracte formulering van de hoofddoelstelling kan derhalve de verenigbaarheidseis van artikel 9 niet worden omzeild.

Artikel 8

Artikel 8 bevat een limitatieve opsomming van de gronden die een gegevensverwerking rechtvaardigen. Het artikel behelst bovendien dat bij elke verwerking moet zijn voldaan aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het subsidiariteitsbeginsel mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kunnen worden verwerkelijkt.

Onderdeel a

Onderdeel a brengt de beschikkingsmacht van de betrokkene over hem betreffende gegevens tot uitdrukking: in geval van een ondubbelzinnige toestemming van de betrokkene is het toegestaan gegevens te verwerken. Deze grond is echter niet exclusief. Daarnaast kunnen ook op andere gronden gegevens worden verwerkt, terwijl de wet ook de toestemming van de betrokkene als rechtvaardigingsgrond kan uitsluiten, bij voorbeeld in situaties waarin sprake is van ongelijke machtsverhoudingen tussen verantwoordelijke en betrokkene.
In de toelichting bij artikel 1 is al ingegaan op de betekenis van dit toestemmingsvereiste. Bij de verantwoordelijke dient elke twijfel te zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven. Als er twijfel is over de vraag of de betrokkene zijn toestemming heeft verleend dient de verantwoordelijke te verifiëren of hij er terecht vanuit gaat dat de betrokkene er mee heeft ingestemd.
Met betrekking tot de derdenverstrekking borduurt het voorschrift voort op artikel 11, eerste lid, WPR (uit een persoonsregistratie worden slechts gegevens aan een derde verstrekt voor zover zulks geschiedt met toestemming van de geregistreerde). In de toelichting bij artikel 1 is ingegaan op het feit dat in dit wetsvoorstel niet meer de voorwaarde is opgenomen dat de toestemming van de betrokkene schriftelijk moet worden verleend (artikel 12, eerste lid, WPR). In deze zin is er sprake van een verruiming ten opzichte van de WPR met betrekking tot het verstrekken van gegevens aan derden.

Onderdeel b

Een gegevensverwerking is toelaatbaar indien deze noodzakelijk is om contractuele verplichtingen na te komen. Daarbij geldt als voorwaarde dat de betrokkene partij is bij de desbetreffende overeenkomst. Met het begrip «partij» wordt gedoeld op een bewuste deelneming van de betrokkene aan de overeenkomst. Achterliggende gedachte is dat de betrokkene zelf in principe kan overzien met welke verwerkingen hij heeft rekening te houden en de mogelijkheid heeft objectief vast te stellen welke verwerkingen in dit kader toelaatbaar zijn. Partijen bij de overeenkomst zijn zij die hetzij rechtstreeks, hetzij door middel van een vertegenwoordiger, de overeenkomst hebben gesloten. Meestal is de persoon die

in feite de voor het tot stand komen van de overeenkomst nodige wilsverklaringen aflegt, partij bij de overeenkomst, namelijk indien hij deze verklaringen aflegt namens zichzelf, ten einde voor zichzelf iets te bedingen of zichzelf te verbinden. Het is echter ook mogelijk dat de handelende persoon optreedt namens een ander. Bijvoorbeeld de wettelijke vertegenwoordiger, de gevolmachtigde of het tot vertegenwoordigen bevoegde orgaan van een rechtspersoon (Asser-Hartkamp II, blz. 349 e.v.). Rechtverkrijgenden van de partijen (rechtsverkrijgenden onder algemene of bijzondere titel) vallen niet onder het begrip «partij» in dit voorschrift. Bij het aangaan van de overeenkomst is immers niet bekend wie later rechtverkrijgenden zullen zijn, dit hangt af van op dat moment toekomstige en onzekere feiten. Het bijzondere karakter van het voorschrift verzet zich er tegen hen met de oorspronkelijke partij te vereenzelvigen. Evenmin kan de begunstige als partij worden beschouwd. Hij geldt als derde jegens wie een der partijen gehouden is tot een prestatie.
De verantwoordelijke behoeft zelf geen partij te zijn bij de overeenkomst. Het gaat voorts om een situatie waarin de bedoelde overeenkomst niet is gericht op de verwerking van persoonsgegevens, maar waarbij deze een noodzakelijk uitvloeisel daarvan is.
Tevens is een gegevensverwerking geoorloofd indien deze noodzakelijk is in de precontractuele fase. Het moet allereest gaan om handelingen die op verzoek van de betrokkene worden verricht ten einde een overeenkomst te kunnen sluiten. Het verzoek hoeft niet dermate gespecificeerd te zijn dat aan elke handeling een verzoek van de betrokkene ten grondslag ligt. Wel moeten de handelingen logischerwijze voortvloeien uit het verzoek en moet het voor de betrokkene redelijkerwijs te verwachten zijn dat deze handelingen worden verricht. In dit verband kan nog op het volgende worden gewezen. Ingevolge de Wet op het Consumentenkrediet (Stb. 1990, 395) dient in bepaalde gevallen – voordat consumptieve kredieten kunnen worden verstrekt – de schuldenpositie van de kredietaanvrager te worden getoetst. De Stichting Bureau Kredietregistratie toetst deze kredietwaardigheid van particulieren. De gegevensverwerkingen die voortvloeien uit deze toetsingstaak gelden weliswaar als zijnde noodzakelijke precontractuele stappen teneinde een kredietovereenkomst met de betrokkene te kunnen aangaan maar kunnen bezwaarlijk worden aangemerkt als handelingen die op verzoek van de betrokkene worden verricht. Deze handelingen beoogen meer het gerechtvaarigd belang van de bank te dienen enige informatie te hebben over de financiële positie van de betrokkene alvorens met hem bepaalde overeenkomsten te sluiten. De gegevensverwerkingen die in het kader van deze handelingen plaatsvinden worden daarom ook gerechtvaarigd door artikel 8, onder f. De handelingen moeten voorts noodzakelijk zijn teneinde de overeenkomst te kunnen sluiten. De formulering van het voorschrift is aangepast overeenkomstig het advies van de Registratiekamer.
In jurisprudentie is reeds erkend dat in het kader van precontractuele verhoudingen verbintenissen uit de wet tussen de aspirant-contractpartijen kunnen ontstaan (HR 18 juni 1992, NJ 1983, 723). Afhankelijk van het stadium waarin de onderhandelingen worden afgebroken, kan de partij die de onderhandelingen staakt verplicht zijn tot vergoeding van de in het kader van de voorafgaande onderhandelingen gemaakte kosten of tot vergoeding van de gederfde winsten. Deze optiek is doorgetrokken in onderdeel b van artikel 8 in die zin dat het gegevensverkeer in het kader van de precontractuele fase een expliciete wettelijke grondslag heeft gekregen.
Het is denkbaar dat de betrokkene zijn toestemming verleent om in het kader van de uitvoering van de overeenkomst of in een precontractuele fase gegevens van hem te verwerken. De gegevensverwerking steunt dan op artikel 8, onder a, indien althans de toestemming rechtsgeldig is

verleend. De betrokkene heeft dan te allen tijde het recht zijn toestemming in te trekken, ten gevolge waarvan de rechtsgrondslag aan de gegevensverwerking komt te ontvallen. Het is dan de verantwoordelijke niet toegestaan alsnog op grond van artikel 8, onder b, tot verwerking over te gaan. Dit stuit op de norm van artikel 6: de verwerking geldt dan als onbehoorlijk en onzorgvuldig ten opzichte van de betrokkene. Wel zal de verantwoordelijke in dat geval ontheven zijn van de verplichting zijn overeenkomst met de betrokkene na te komen en deze op wanprestatie kunnen aanspreken. Wordt de toestemming ingetrokken ten aanzien van verwerkingen die noodzakelijk zijn in de precontractuele fase, dan zal de verantwoordelijke van de betrokkene schadevergoeding kunnen claimen (zie hierboven).
Het komt voor dat de uitvoering van de overeenkomst met betrokkene eveneens vergt dat gegevens van derden, niet zijnde partij bij de overeenkomst, moeten worden verwerkt. Als iemand bijvoorbeeld zijn bank opdracht geeft een bepaalde geldsom over te maken naar de rekening van een derde, geldt de daarvoor noodzakelijke verwerking door de bank van de persoonsgegevens van de betrokkene als een uitvloeisel van de rekeningcourantovereenkomst die deze persoon heeft met zijn bank. Deze verwerkingsgrond geldt echter niet ten aanzien van de gegevens van de derde (te weten de derde aan wie het geld wordt overgemaakt) die de bank ter uitvoering van deze betalingsopdracht moet verwerken. Met de begunstigde heeft de bank van de opdrachtgever immers geen contractuele relatie. Deze gegevensverwerking is daarentegen noodzakelijk voor de bank om zijn reguliere bancaire werkzaamheden te kunnen verrichten. Dergelijke gegevensverwerkingen gelden als noodzakelijk voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke en kunnen om die reden worden gebaseerd op onderdeel f van artikel 8. Onderdeel b vergt niet dat degene die de gegevens verwerkt contractspartij is.

Onderdeel c

De verantwoordelijke is gerechtigd gegevens te verwerken indien dit noodzakelijk is ter uitvoering van een wettelijke verplichting die op hem rust. Deze norm bevat twee toetsingscriteria: allereerst dient de gegevensverwerking noodzakelijk te zijn ter uitvoering van een wettelijke verplichting, voorts dient de verantwoordelijke te zijn belast met de uitvoering van de wettelijke verplichting.
Allereerst dient de wettelijke verplichting noodzakelijkerwijs met zich te brengen dat de desbetreffende gegevens worden verwerkt. Zonder verwerking van de gegevens moet het uitvoeren van de wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Er moet een evident verband bestaan tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting. Een aantal voorbeelden mogen dit verduidelijken. Ingevolge artikel 56 van de Algemene wet bijzondere ziektekosten is een ieder verplicht aan onder meer de ziekenfondsen alle inlichtingen te geven die deze behoeven ter behoeve van de uitvoering van deze wet. Deze informatieplicht ziet slechts op informatie die benodigd is voor de vaststelling van de eigen bijdrage. Ze ziet bij voorbeeld niet op het verstrekken van informatie aan ziekenfondsen ten behoeve van het informeren van verzekerden over de verstrekkingen en betalingen. Zo is bij voorbeeld een bank op grond van dit voorschrift niet verplicht aan een ziekenfonds gegevens te leveren die deze nodig heeft ten behoeve van een informatieve mailing. Voorts geldt, indien ingevolge de artikelen 1 tot en met 3 van de Wet openbaarheid van bestuur een verplichting bestaat tot het verstrekken van informatie, waaronder persoonsgegevens, dat deze gegevensverstrekking onder artikel 8, onder c, valt. Op de verhouding tussen de Wet bescherming persoonsgegevens en de Wet openbaarheid van bestuur is reeds in het algemene deel van de

toelichting ingegaan. Ook de gegevensverstrekking als gevolg van de openbaarheidsbepalingen van de Archiefwet 1995 valt onder artikel 8, onder c.
De term «wettelijke verplichting» heeft betrekking op iedere verplichting tot gegevensverwerking die krachtens een algemeen verbindend voorschrift wordt opgelegd. Uiteraard dient wel te zijn voldaan aan het bepaalde in artikel 10, eerste lid, van de Grondwet en artikel 8 van het EVRM. Dat betekent dat een dergelijke verplichting alleen bij of krachtens een wet in formele zin in het leven kan worden geroepen voor zover dit in een democratische samenleving noodzakelijk is onder meer in het belang van het economische welzijn van het land. Of aan deze voorwaarde is voldaan, zal uiteindelijk door de rechter kunnen worden getoetst.
De wettelijke verplichting behoeft geen expliciete opdracht tot de gegevensverwerking te bevatten. Een voorwaarde bij een financiële regeling kan als regel echter niet als zodanig worden opgevat. Dit kan anders zijn als de informatieverplichting die als voorwaarde aan de financiële regeling is verbonden, een toereikende wettelijke grondslag kent.
De taak een wettelijke verplichting uit te voeren rechtvaardigt niet iedere gegevensverwerking. De verantwoordelijke mag ter uitvoering van de wettelijke verplichting bij voorbeeld niet meer of andere gegevens verwerken dan noodzakelijk is voor de uitvoering van de wettelijke verplichting. Gelet op de aard van de inbreuk op de privacy is een belangenafweging van geval tot geval nodig. Daarbij dient onder meer gelet te worden op de aard van de in het geding zijnde taak en de aard van de betrokken gegevens.
Als tweede voorwaarde geldt dat alleen een beroep op onderdeel c kan worden gedaan in het geval de verantwoordelijke is onderworpen aan de nakoming van de wettelijke verplichting. Onderdeel f van artikel 8 biedt basis voor het geval de verantwoordelijke gegevens verwerkt ter voldoening van een wettelijke verplichting van een ander (te weten een «gerechtvaarigd belang van een derde aan wie de gegevens worden verstrekt»).
In zekere zin bouwt onderdeel c – althans voor zover het gaat om een persoonsregistratie in de publieke en semi-publieke sector betreft – voort op de norm van artikel 18, eerste en tweede lid, WPR: de gegevensverwerking dient noodzakelijk te zijn voor een goede vervulling van de (wettelijke) taak van de verantwoordelijke. De verwerkingsgrond van onderdeel c is beperkter in die zin dat het moet gaan om de vervulling van een wettelijke verplichting van de verantwoordelijke. Er buiten valt een verwerking die uitsluitend dient ter uitvoering van een wettelijk recht. Een dergelijke gegevensverwerking zal moeten kunnen worden gebaseerd op onderdeel e of f van artikel 8.
Met betrekking tot de derdenverstrekking borduurt het voorschrift voort op artikel 11, eerste lid, WPR. Hierin wordt bepaald dat uit een persoonsregistratie slechts gegevens aan een derde worden verstrekt voor zover zulks wordt vereist ingevolge een wettelijk voorschrift.
De wettelijke verplichting waarop onderdeel c ziet, zal in de praktijk doorgaans betrekking hebben op het vastleggen of bewaren van gegevens of het verstrekken daarvan aan derden. Als voorbeeld kan worden gewezen op de verplichting ingevolge artikel 47 van de Algemene wet inzake rijksbelastingen de inspecteur te voorzien van alle gegevens die van belang kunnen zijn voor de belastingheffing te zijnen aanzien.

Onderdeel d

Een gegevensverwerking is gerechtvaardigd indien deze noodzakelijk is ter bestrijding van een ernstig gevaar voor de gezondheid van de betrokkene. Artikel 7, onder d, van de richtlijn spreekt van een verwerking die noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene.

In overweging 31 wordt hierover opgemerkt dat «een verwerking ook als geoorloofd moet worden beschouwd wanneer zij wordt uitgevoerd ter bescherming van een belang dat voor het leven van de betrokkene essentieel is». De formulering van onderdeel d sluit hier op aan.
De verwerkingsgrond van onderdeel d dient eng te worden geïnterpreteerd: er moet een dringende medische noodzaak aanwezig zijn de gegevens van de betrokkene te verwerken. Het moet gaan om een zaak van leven of dood. Als voorbeeld kan de situatie gelden dat terstond medische hulp nodig is naar aanleiding van een ongeval van de betrokkene waarbij deze buiten bewustzijn is geraakt. Voorts moet de noodzaak dringend zijn omdat anders aan de betrokkene zijn ondubbelzinnige toestemming (artikel 8, onder a) moet worden gevraagd.
Het subsidiariteitsbeginsel brengt met zich dat – in het geval toestemming van de betrokkene kan worden gevraagd – dit de voorkeur verdient. Het is niet altijd noodzakelijk dat de betrokkene niet in staat is overeenkomstig onderdeel a van artikel 8 toestemming te verlenen. Ook indien de noodzaak om op te treden zo dringend is dat in redelijkheid van de verantwoordelijke niet kan worden gevraagd toestemming van de betrokkene(n) te vragen, kan een gegevensverwerking op grond van dit voorschrift geoorloofd zijn. Gedacht kan worden aan het geval van een grootschalige ramp waarbij terstond maatregelen in de sfeer van de hulpverlening moeten worden getroffen. Het is dan ondoenlijk eerst alle betrokkenen te informeren en toestemming te vragen alvorens de hulpverlening te starten. Hetzelfde geldt voor hulpverlening aan bewoners van een in brand staand huis.

Onderdeel e

Artikel 8, onder e, maakt gegevensverwerking mogelijk voor zover deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het betreffende bestuursorgaan dan wel het bestuursorgaan aan wie de gegevens worden verstrekt. De bepaling vormt de implementatie van artikel 7, onder e, van de richtlijn. Ten opzichte van laatstgenoemde bepaling zijn enkele preciseringen aangebracht die zijn gericht op een adequate toepassing in het Nederlandse recht. Aangezien de bepaling betrekking heeft op de publieke sector is getracht zo veel mogelijk aan te sluiten bij de systematiek van de Algemene wet bestuursrecht.
De bepaling stelt als voorwaarde voor de rechtmatigheid van de gegevensverwerking dat zij toegespitst moet zijn op een goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan aan wie de gegevens worden verstrekt. Een taak is publiekrechtelijk indien deze is gebaseerd op een speciaal voor het openbaar bestuur bij of krachtens de wet geschapen grondslag. In de regel gaat een uitoefening van een overheidstaak gepaard met op een publiekrechtelijke grondslag gebaseerde bevoegdheden. Het begrip «publiekrechtelijk» sluit aan bij de terminologie van de Awb, zoals onder meer gehanteerd in de definitie van het besluit-begrip in artikel 1:3. Voorts wordt met de formulering van dit onderdeel aangesloten bij de zinsnede «taak van algemeen belang» uit artikel 7, onder e, van de richtlijn.
Daarnaast gaat het in onderdeel e om een gegevensverwerking in het belang van een publiekrechtelijke taak die wordt uitgeoefend door het desbetreffende bestuursorgaan of het bestuursorgaan waaraan de gegevens worden verstrekt. Met het begrip «bestuursorgaan» is eveneens aansluiting gezocht bij de Awb. Dit begrip wordt in artikel 1:1 Awb omschreven als een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld of een ander persoon of college met enig openbaar gezag bekleed. Deze omschrijving sluit aan bij artikel 7, onder e, van de richtlijn waar eveneens van de uitoefening van openbaar gezag wordt gesproken. Het bestuursorgaan-begrip wordt in de bestuursrechtelijke jurisprudentie nader begrensd. In bepaalde gevallen worden

ook privaatrechtelijke rechtspersonen als «bestuursorgaan» beschouwd, namelijk in het geval zij bevoegd zijn in het kader van de uitoefening van openbaar gezag rechtshandelingen te verrichten. Een bijzondere school geldt bijvoorbeeld als bestuursorgaan voor zover zij belast is met de uitgifte van diploma's.
Niet alle verwerkingen die worden verricht door bestuursorganen vallen onder de reikwijdte van het onderhavige onderdeel. In sommige gevallen verrichten bestuursorganen activiteiten die zich niet wezenlijk onderscheiden van activiteiten die ook door particulieren worden verricht. Te denken valt aan de verkoop van onroerend goed of het sluiten van een arbeidsovereenkomst. Om die reden hebben beide elementen van onderdeel e – «publiekrechtelijke taak» en «bestuursorgaan» – naast elkaar betekenis.
In aansluiting op de richtlijn ziet onderdeel e op twee verschillende situaties waar bestuursorganen bij betrokken kunnen zijn. In de eerste plaats kan een verwerking noodzakelijk zijn met het oog op een publiekrechtelijke taak die het bestuursorgaan dat als verantwoordelijke voor de gegevensverwerking geldt, zelf verricht. Deze situatie vertegenwoordigt de meerderheid van de gevallen. Het bestuursorgaan dat gegevens verwerkt zal deze meestal met name gebruiken voor eigen doeleinden. Daarnaast laat de richtlijn echter uitdrukkelijk open dat ook gegevens gebruikt mogen worden ten behoeve van de publiekrechtelijke taak die door een ander bestuursorgaan wordt verricht. Ten behoeve van een dergelijke taak mogen beschikbare gegevens worden verstrekt, mits dat met het oog op die taak noodzakelijk is.
De in onderdeel e gehanteerde terminologie sluit niet uit dat het bestuursorgaan de verwerking van de gegevens uitbesteedt aan een particuliere instelling. Deze instelling zal echter niet als verantwoordelijke mogen worden aangemerkt. De bepaling biedt geen grondslag voor de verzameling of de vastlegging van persoonsgegevens door een instantie die geen bestuursorgaan is. Dergelijke verwerkingen zullen bijvoorbeeld door artikel 8, onder c of f, moeten worden gerechtvaardigd.
De gegevensverwerking moet wel noodzakelijk zijn voor de vervulling van de betrokken taak van het bestuursorgaan. Bij gebreke van gedetailleerde wettelijke regels voor deze taakuitoefening, dient bijzondere aandacht te worden besteed aan de vraag of wel sprake is van een rechtmatige taakuitoefening. Om deze reden spreekt onderdeel e – in navolging van het advies van de Registratiekamer – ook van een «goede vervulling» van de taak. Bij de beoordeling van de noodzaak van de betrokken verwerking zullen verder de beginselen van proportionaliteit en subsidiariteit een belangrijke rol spelen.
Onderdeel e bouwt in zekere zin voort op de norm van artikel 18, eerste en tweede lid, WPR. Uit deze bepalingen, die zijn gericht op de publieke en semi-publieke sector, vloeit reeds thans voort dat de gegevensverwerking noodzakelijk dient te zijn voor een goede vervulling van de taak van de houder.
In een aantal gevallen zal in de sfeer van de publieke sector de gegevensverwerking kunnen worden gebaseerd op artikel 8, onder c. Niet alle gegevensverwerkingen van de overheid zijn echter terug te voeren op een verplichting tot gegevensverwerking krachtens een wettelijk voorschrift. Een gegevensverwerking ter vervulling van een publiekrechtelijke taak kan immers eveneens geschieden zonder dat daaraan een wettelijk verplichting ten grondslag ligt. Op grond van onderdeel e is een gegevensverwerking gerechtvaardigd indien deze noodzakelijk is voor de vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan gegevens worden verstrekt. Het verschil tussen onderdelen c en e blijkt onder meer uit de omstandigheid dat de betrokkene enkel recht heeft zich tegen een verwerking te verzetten in geval de verwerking noodzakelijk is ter vervulling van een publiekrechtelijke taak (artikel 40, eerste lid). Een

wettelijke verplichting tot gegevensverwerking laat immers in de regel zo weinig beoordelingsruimte voor de verantwoordelijke over dat in dergelijke gevallen een recht van verzet van de betrokkene niet zinvol is.

Onderdeel f

Ingevolge dit onderdeel is een gegevensverwerking geoorloofd indien deze noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, doorslaggevend zijn. Onderdelen b tot en met e van artikel 8 zijn specifiek daar steeds een bepaald doel wordt genoemd waaraan moet worden getoetst. Onderdeel f is met de verwijzing naar een gerechtvaardigd belang van de verantwoordelijke, welk belang dan ook, veel algemener van aard en daarmee in wezen een soort restbepaling. In de praktijk blijkt dat een sluitende regeling van de gronden van verwerking van persoonsgegevens niet goed mogelijk is.
De vraag rijst op welke wijze van de daarin gegeven interpretatieruimte gebruik moet worden gemaakt. In de eerste plaats vereist onderdeel f dat er sprake is van een gerechtvaardigd belang van de verantwoordelijke of van een derde. Een gerechtvaardigd belang van de verantwoordelijke kan aanwezig worden geacht in het geval dat de betreffende verwerking voor laatstgenoemde noodzakelijk is om zijn reguliere bedrijfsactiviteiten te kunnen verrichten. De verantwoordelijke kan zijn beroep of bedrijf niet goed uitoefenen indien hem de mogelijkheid zou worden ontzegd de met het oog daarop noodzakelijke gegevens te verwerken. Zo dient een schadeverzekeraar ten behoeve van een schadeclaim naast de gegevens van zijn cliënt ook gegevens van de tegenpartij en eventuele getuigen te kunnen verwerken. Zonder een dergelijke verwerking zou een goede dienstverlening niet goed mogelijk zijn.
Een dergelijke interpretatie vindt rechtstreekse steun in de richtlijn: in overweging 30 komt tot uitdrukking dat persoonsgegevens in het kader van wettige activiteiten, zoals «dagelijks beheer van ondernemingen en andere organisaties», in beginsel kunnen worden gebruikt en aan derden verstrekt. Cruciaal is evenwel dat de toelaatbaarheid van de gegevensverwerking door diezelfde richtlijn begrensd wordt: de verwerking is uitsluitend toelaatbaar indien zij noodzakelijk is met het oog op belang van de verantwoordelijke of een derde én het belang van degene van wie de gegevens worden verwerkt niet prevaleert. De bepaling impliceert een motiveringsplicht voor de verantwoordelijke. Hij dient voor zichzelf verschillende vragen te beantwoorden, zoals:
– Is er werkelijk een belang dat verwerking van persoonsgegevens rechtvaardigt?
– Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan – afhankelijk van de ernst van de inbreuk – gegevensverwerking niet achterwege te blijven?
– Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg – zonder verwerking – worden bereikt?
– Is de verwerking in de mate die is beoogd evenredig aan het nagestreefde doel?

De noodzakelijkheidseis die in artikel 8 besloten ligt, veronderstelt dat de verantwoordelijke op dergelijke vragen een bevredigend antwoord heeft. Desgevraagd dienen deze antwoorden ook zichtbaar te worden gemaakt, zodat zij eventueel door de rechter kunnen worden getoetst.
Enige voorbeelden mogen de betekenis van dit onderdeel verduidelijken. In het algemeen deel van deze memorie is reeds het voorbeeld genoemd van de schadeverzekeraar die ten behoeve van de afwikkeling van een schadeclaim naast de gegevens van zijn cliënt ook gegevens van de

tegenpartij en eventuele getuigen moet kunnen verwerken. Ook in het geval iemand een levensverzekeringsovereenkomst wil sluiten te behoeve van een derde, zullen eveneens de gegevens van die derde door de verzekeraar daartoe verwerkt moeten worden. Zonder dat zou zijn dienstverlening niet goed mogelijk zijn. Ook ten aanzien van gegevensverwerkingen die weliswaar geen onderdeel uitmaken van de reguliere bedrijfsactiviteiten van de verantwoordelijke maar deze wel in wezenlijke zin ondersteunen, kan in de regel worden aangenomen dat de verantwoordelijke een gerechtvaardigd belang heeft. Als voorbeeld kan worden genoemd de gegevensverwerking in het bedrijf in het kader van fraudebestrijding en intern marktonderzoek. Een gegevensverwerking kan ook geschieden in het kader van activiteiten die weliswaar geen (direct) onderdeel uitmaken van de kernactiviteiten van de verantwoordelijke maar daar nauw mee verweven zijn. Een voorbeeld is wanneer een bedrijf zijn cliëntgegevens wil benutten voor het doen van een mailing om een nieuw produkt onder hun aandacht te brengen (direct marketing). Ook dan kan in beginsel een gerechtvaardigd belang van de verantwoordelijke worden aangenomen.
Daarnaast moet de gegevensverwerking noodzakelijk zijn ten behoeve van het gerechtvaardigd belang van de verantwoordelijke (of een derde). Kunnen hun belangen anderszins of met minder ingrijpende middelen worden gediend, dan is de voorgenomen gegevensverwerking niet toegestaan. Hier spelen wederom het proportionaliteits- en subsidiariteitsbeginsel een rol. Evenals bij de gronden b tot en met e dient de noodzaak in de uiteengezette zin in verhouding tot het doel te worden beoordeeld. Dat betekent dat, alle belangen in ogenschouw genomen, de voorgenomen gegevensverwerking als noodzakelijk voor het doel moet worden beschouwd.
De bepaling schrijft in aanvulling op de eerste afweging (noodzakelijk voor een gerechtvaardigd belang van de verantwoordelijke), waarbij mogelijk de belangen van de betrokkene als onderdeel van een veelheid van belangen reeds onder ogen zijn gezien, nog een tweede toets voor. Deze tweede toets vergt een nadere afweging, waarbij de belangen van de betrokkene een zelfstandig gewicht in de schaal leggen tegenover het belang van de verantwoordelijke. Met deze tweede toets wordt nog eens extra de nadruk gelegd op het proportionaliteitsvereiste. Deze extra toets is aan het slot van het voorschrift opgenomen door middel van de zinsnede «tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert». Dit betekent niet dat op voorhand de belangen van de betrokkene zwaarder moeten wegen, doch slechts dat een hernieuwde aangescherpte toets, waarbij de belangen van de betrokkene afzonderlijk moeten worden gewogen. Indien de betrokkene geen belang heeft bij de door de verantwoordelijke voorgestane gegevensverwerking, behoeft dit geenszins te betekenen dat daarmee de gegevensverwerking ongeoorloofd is. Verantwoordelijke en betrokkene kunnen tegengestelde belangen hebben bij een gegevensverwerking. Een bank heeft bij voorbeeld een geheel ander belang bij het verwerken van de beschikbare gegevens teneinde mogelijkheden tot compensatie van vorderingen na te gaan dan de daarbij betrokken cliënten zelf hebben. Alleen in het geval dat het belang van de betrokkene op bescherming van zijn persoonlijke levenssfeer doorslaggevend is dient de verantwoordelijke af te zien van de gegevensverwerking.
De verantwoordelijke dient de belangen af te wegen zoals deze aan hem bekend zijn. Indien de omstandigheden daartoe aanleiding geven zal van hem kunnen worden verwacht nader onderzoek te doen naar het gewicht van deze belangen. De afweging zal in dit stadium evenwel in de regel een meer algemeen karakter hebben. Kan een individuele betrokkene aanspraak maken op een andere uitkomst van deze afweging op gronden die de verantwoordelijke niet kende en niet behoefde te kennen, dan kan

de betrokkene deze nadere afweging in zijn geval op de door aangedragen gronden afdwingen via het recht van verzet als bedoeld in artikel 40.
Bij de in onderdeel f voorgeschreven afweging speelt een rol de mate van gevoeligheid van de gegevens die de verantwoordelijke wil verwerken en de maatregelen die de verantwoordelijke heeft genomen ten einde rekening te houden met de belangen van de betrokkene. De belangen van de betrokkene zullen in mindere mate gewicht in de schaal leggen naarmate in zijn belang meer waarborgen voor een zorgvuldig gebruik van de gegevens zijn genomen. Zo kan een bank er een gerechtvaardigd belang bij hebben de betalingsverkeergegevens van bepaalde cliënten – bij voorbeeld cliënten die regelmatig op hun rekening rood staan of hoge kredieten hebben opgenomen en aflossingsproblemen hebben – te analyseren, bij voorbeeld om deze personen te kunnen adviseren met het doel hun betaalgedrag efficiënter te doen zijn. Duidelijk is dat een dergelijke analyse gerechtvaardigd is nadat de desbetreffende cliënten zijn benaderd met het verzoek een dergelijke analyse te mogen doen en zij in de gelegenheid zijn gesteld daartegen bezwaar te maken. Het ongevraagd analyseren en adviseren van de cliënt op basis van een analyse van zijn persoonlijke gegevens, zal in het algemeen niet door de onderhavige bepaling kunnen worden gedragen. Het feit dat een verantwoordelijke in een gedragscode nadere voorschriften heeft opgenomen over het gebruik dat van de gegevens wordt gemaakt en de personen aan wie ze kunnen worden verstrekt, kan eveneens een rol spelen bij de beantwoording van de vraag in het kader van onderdeel f of de verantwoordelijke een juiste afweging van belangen heeft gemaakt.

Tot de relevante omstandigheden die eveneens meewegen bij een oordeel over de door de verantwoordelijke gemaakte afweging speelt tevens een rol of het gaat om de publieke dan wel de private sector. Binnen de publieke sector geldt immers de rechtstreeks werkende grondwetsbepaling die de persoonlijke levenssfeer beschermt, mede tegen de achtergrond van de daarmee corresponderende verdragsbepalingen. Ook in gevallen dat het onderdeel zou leiden tot een inbreuk op de persoonlijke levenssfeer, en de bepaling in dat geval als een legitimerende grondslag zou moeten worden aangemerkt als bedoeld in artikel 10, eerste lid, van de Grondwet, dan nog mag in het licht van artikel 8 EVRM, deze inbreuk niet verdergaan dan noodzakelijk is. De jurisprudentie van het EHRM heeft hieraan een uitgewerkte betekenis gegeven, zoals in het algemeen deel van deze memorie is uiteengezet.
De Grondwet en het EVRM beogen in eerste instantie slechts de vrijheidssfeer van de burger ten opzichte van de overheid te waarborgen. Gaat het om de private sector dan hebben de in het geding zijnde grondrechten slechts een afgeleide werking (de z.g. horizontale werking) namelijk voor zover zij uit een oogpunt van maatschappelijke zorgvuldigheid ook door burgers jegens elkaar in acht behoren te worden genomen. De werking heeft niet de volle omvang als in de publieke sector. Bij de interpretatie van het begrip «noodzakelijk» in onderdeel f speelt de vraag of het gaat om een publieke dan wel een private context daarom mede een rol. Waar dus het bestaande onderscheid in de materiële bepalingen van de WPR tussen private en publieke sector in de tekst van het wetsvoorstel wordt opgeheven, blijft dit onderscheid bij de interpretatie van het voor beide sectoren geldende algemene norm van onderdeel f, desalniettemin relevant.
In het algemeen deel van de toelichting bij dit artikel is al ingegaan op het belang van artikel 8, onder f. Wij wezen erop dat deze verwerkingsgrond ten opzichte van de WPR, in de private sector een aanscherping van mogelijkheden oplevert om gegevens te verwerken: niet meer de verwerkingen waartoe het belang van de verantwoordelijke dat redelijkerwijs aanleiding geeft (artikel 4 WPR), maar de noodzaak van de behartiging van diens gerechtvaardigd belang, dient voortaan de

grondslag voor de gegevensverwerking te zijn. Dit laatste criterium gold krachtens de WPR alleen voor de publieke sector.
Overeenkomstig de WPR kan ook het belang van een derde grond kan zijn voor de verwerking van gegevens. Als gevolg hiervan behoeft de verantwoordelijke niet dezelfde persoon te zijn als degene in wiens belang de gegevens worden verwerkt. De verantwoordelijke kan zich een belang van een derde aantrekken en ten behoeve van dat belang gegevens die hij reeds onder zich heeft, verwerken. Een koepelorganisatie kan bijvoorbeeld in het belang van de bij haar aangesloten organisaties een registratie aanhouden van geconstateerde fraudegevallen. Een vergelijking kan ook worden getrokken met artikel 13 WPR dat spreekt van het bedrijfsmatig verstrekken van gegevens aan derden. De verantwoordelijke kan gegevens verwerken voor een ander doel dan het oorspronkelijke waarvoor de gegevens werden vergaard, eventueel ten behoeve van een derde, voor zover het gaat om doeleinden die verenigbaar zijn met het oorspronkelijk doel. Dit brengt met zich mee dat de verwerking niet kan plaatsvinden voor een doel ofwel belang van een derde dat niet verenigbaar is met het doel waarvoor de gegevens door de verantwoordelijke zijn verzameld. Het is niet mogelijk dat de verantwoordelijke enkel uit faciliterende overwegingen gegevens ten behoeve van een derde verwerkt. Indien het doel waaraan de verantwoordelijke is gebonden bijvoorbeeld met zich brengt dat de gegevens moeten worden vernietigd kan hij deze niet meer bewaren enkel om de reden dat het verwerken van die gegevens het belang van de derde zou dienen.
Gaat het om verstrekking aan een derde dan zou een vergelijking kunnen worden getrokken met artikel 13 WPR dat eveneens uitgaat van het doel van een derde als grond voor een verstrekking.
Het bovenstaande brengt een verruiming van het beginsel van doelbinding met zich omdat immers niet alleen het doel van de verwerking maar ook andere doeleinden, mits verenigbaar met het oorspronkelijk doel, grond kunnen zijn voor een verstrekking aan derden. Onderdeel f laat in beginsel een dergelijke verwerking toe, tenzij het belang van de betrokkene zwaarder moet wegen. In de regel zal diens belang vergen dat hij vooraf in de gelegenheid wordt gesteld bezwaar te maken tegen een dergelijke voorgenomen verstrekking, tenzij een dergelijke bekendmaking van de zijde van het gemeentelijk energiebedrijf aan de betrokkenen een onevenredige inspanning zou vergen.
Bij gegevensverwerking noodzakelijk voor de behartiging van een gerechtvaardigd belang van een derde, dient de verantwoordelijke – alvorens tot verwerking over te gaan – op de hoogte te zijn van het belang dat de derde heeft bij de gegevensverwerking en welke hem ter beschikking staande gegevens in het licht van evenbedoelde belang van betekenis zijn (zie bij voorbeeld HR 10 december 1993, NJ 1994, 667). Ongeacht de verantwoordelijkheid van de derde dient de verantwoordelijke daarbij af te wegen of de verwerking noodzakelijk is met het oog op dat belang en of het belang van de betrokkene niet dient te prevaleren.

Artikel 9

Verenigbaar gebruik: algemene gezichtspunten

De eis van het verenigbaar gebruik geldt zowel binnen als buiten de organisatie van de verantwoordelijke. Waar in artikel 11, eerste lid, WPR voor het gebruik buiten de organisatie van de verantwoordelijke geldt dat een verstrekking aan een derde moet voortvloeien uit het doel van de registratie, is deze eis in dit wetsvoorstel vervallen. In dit opzicht is er sprake van een verruiming van de mogelijkheden: voor het interne en externe gebruik gelden dezelfde regels. Het verschil tussen beide wordt met de moderne informatiesystemen toch in toenemende mate diffuus. Binnen de organisatie van de verantwoordelijke, ongeacht of dit één of

meer ondernemingen zijn, het om één rechtspersoon dan wel meerdere rechtspersonen gaat, kunnen gegevens worden gebruikt voor andere doeleinden dan waarvoor zij zijn vergaard, zolang deze andere doeleinden verenigbaar zijn met het oorspronkelijk doel waarvoor zij worden verwerkt. Buiten de organisatie van de verantwoordelijke, tegenover derden, gelden dezelfde regels. Deze nieuwe structuur biedt meer flexibiliteit dan onder de WPR mogelijk was.
Als voorbeeld van onverenigbaar gebruik kan worden gewezen op gegevens die binnen eenzelfde concern naar aanleiding van uiteenlopende contracten zijn verkregen. Zeker wanneer het gaat om gevoelige gegevens klemt deze eis temeer. Indien bij voorbeeld een verzekeraar met een betrokkene zowel een ziektekostenverzekering als een ziektewetverzekering (loondervingsregeling) als een levensverzekering heeft gesloten, is het denkbaar dat in het kader van elk van deze overeenkomsten met toestemming van de betrokkene medische gegevens zijn verkregen die op gerechtvaardigde gronden bij de uitvoering van de verzekering worden verwerkt. Desondanks zal in de regel het bijeenvoegen van deze gegevens, bij voorbeeld wanneer de betrokkene een nieuwe verzekering aanvraagt, moeten worden aangemerkt als onverenigbaar gebruik. Deze mogelijkheid is er slechts indien de betrokkene daartoe uitdrukkelijk toestemming heeft gegeven. Deze eis impliceert dat deze toestemming niet als polisvoorwaarde kan worden opgenomen, doch dat de betrokkene op dit bijzonder facet van gegevensverwerking zijn afzonderlijk fiat geeft. Artikel 33 eist verder dat wanneer dat noodzakelijk is in verband met de verwerking te goeder trouw, betrokkene moet worden geïnformeerd of een weigering van de toestemming van het gebruik van de persoonsgegevens voor andere doeleinden tot gevolg heeft dat de beoogde verzekeringsovereenkomst niet tot stand komt.
Bij de beantwoording van de vraag of er sprake is van verenigbaar gebruik leggen uiteenlopende factoren gewicht in de schaal. Een aantal van deze factoren is ter nadere invulling van de verenigbaarheidseis, in het tweede lid opgesomd. Aldus wordt de verantwoordelijke een handvat geboden met behulp waarvan hij kan beoordelen of een bepaalde wijze van gebruik onverenigbaar is. Het gaat nadrukkelijk niet om een limitatieve opsomming. Het niet-limitatieve karakter is in het tweede lid tot uitdrukking gebracht door middel van de zinsnede «in elk geval». Evenmin kan worden gesteld dat een van de factoren op zichzelf van doorslaggevende betekenis is. Elk van de genoemde factoren dienen – mogelijk in samenhang met andere factoren die in het concrete geval als relevant moeten worden beschouwd – in onderling verband worden beoordeeld en gewogen ter beantwoording van de vraag of sprake is van verenigbaar gebruik.
In de eerste plaats is van belang om te kijken naar de verwantschap tussen het doel waarvoor de verantwoordelijke de gegevens overweegt te gebruiken enerzijds en het doel waarvoor de gegevens zijn verkregen anderzijds. Dit criterium is te vinden in onderdeel a. De bepaling inzake verenigbaar gebruik geeft uitdrukking aan het doelbindingsprincipe. Om die reden ligt het voor de hand om eerst te bezien welke verwantschap er bestaat tussen het oorspronkelijke doel en het doel waarvoor de verantwoordelijke de gegevens op dat moment zou willen gebruiken. Is die verwantschap nauwer dan is vanzelfsprekend eerder sprake van verenigbaar gebruik dan wanneer slechts van een verder verwijderd verband sprake is.
Vervolgens is van belang de aard van de betreffende gegevens (onderdeel b). Artikel 16 betreft de gegevens die uit hun aard gevoelig zijn. Daarnaast kunnen gegevens gevoelig zijn door de context waarin zij worden gebruikt, bij voorbeeld de gegevens omtrent iemands kredietwaardigheid of welstand. Hoe gevoeliger het gegeven, hoe minder snel mag worden aangenomen dat er sprake is van verenigbaar gebruik indien bij enige verwerking wordt afgeweken van het oorspronkelijk doel.

Voorts is van belang in welke mate de betrokkene de gevolgen ondervindt van een doelwijziging (onderdeel c). Worden de gegevens gebruikt als basis voor mogelijke beslissingen met betrekking tot hem, dan is er eerder sprake van onverenigbaar gebruik dan wanneer de gegevens worden gebruikt voor wetenschappelijk onderzoek of voor de toezending van bepaalde boodschappen. Bij deze beslissingen gaat het zowel om beslissingen in de private sector, bij voorbeeld in het kader van het acceptatiebeleid van verzekeraars, of in de publieke sector, bij voorbeeld de beslissing om iemand te onderwerpen aan de uitoefening van bepaalde toezichthoudende bevoegdheden. Daar waar echter geen beslissingen worden genomen jegens betrokkenen, is het onverenigbaar gebruik minder snel aanwezig.
Het duidelijkst is dit het geval bij wetenschappelijk onderzoek. In beginsel wordt de betrokkene dan op geen enkele wijze meer geconfronteerd met de verwerking van de hem betreffende gegevens. Dit is slechts anders indien iemand die hem kent, als onderzoeker kennis neemt van gegevens die niet identificeerbaar zijn, of wanneer bij longitudinaal onderzoek de betrokkene in latere fase weer wordt benaderd met nadere vragen. In de WPR is dan ook voor het wetenschappelijk onderzoek een aparte bepaling opgenomen, waarbij bij het externe gebruik een andere invulling is gegeven aan het beginsel dat een verstrekking aan een derde moet voortvloeien uit het doel van de registratie. Verstrekking voor wetenschappelijk onderzoek is blijkens 11, tweede lid, WPR toegestaan, tenzij op de persoonlijke levenssfeer een onevenredige inbreuk wordt gemaakt. Dit is bij voorbeeld het geval wanneer personen door onderzoekers worden benaderd nadat zij zijn geselecteerd als slachtoffer van een zedenmisdrijf. Minder duidelijk is dit bij verstrekkingen voor direct marketing of fondsenwerving voor liefdadige doeleinden. Het gebruik van persoonsgegevens voor deze doeleinden heeft geen invloed op iemands mogelijkheden tot maatschappelijke ontplooiing, noch leidt dit ertoe dat iemand het voorwerp van bijzondere aandacht van de kant van overheidsorganen. Ieder is vrij de aan hem geadresseerde informatie al dan niet gelezen weg te werpen zonder dat dit enige gevolgen voor hem heeft. Om die reden is ook voor deze vorm van extern gebruik in de WPR in artikel 14 een soepeler bepaling opgenomen dan het voortvloeien uit het doel: in beginsel is verstrekking toegestaan. Ook hier geldt echter thans – door de verwijzing naar artikel 13 WPR – dat in ieder geval de persoonlijke levenssfeer niet onevenredig mag worden geschaad. Dit is bijvoorbeeld in beginsel het geval indien de betrokkene ongevraagd wordt benaderd op grond van mogelijke persoonlijke voorkeuren die door anderen in kaart zijn gebracht. Wordt iemand geconfronteerd met een profiel van zijn persoon dat zonder zijn toestemming van hem is vervaardigd en voor commerciële doeleinden wordt aangewend, bij voorbeeld om hem te benaderen, dan is het niet onredelijk wanneer hij dit als een inbreuk op de persoonlijke levenssfeer ervaart.
Van belang in laatstgenoemd geval is vooral dat de gegevens buiten de betrokkene om zijn verkregen en deze gegevens bovendien zijn verwerkt tot een specifiek voor die persoon geldend profiel zonder deze persoon daarbij op enigerlei wijze te betrekken. Onder die omstandigheden zal veel eerder van onverenigbaarheid sprake zijn. Zijn daarentegen de gegevens van de betrokkene zélf verkregen en worden er bovendien met het oog op het belang van de betrokkene passende waarborgen geboden, is de kans groter dat aan de voorwaarde van verenigbaar gebruik is voldaan. De hier bedoelde criteria zijn eveneens in het tweede lid neergelegd. Verwezen zij naar de onderdelen d en e. Welke waarborgen passend zijn zal per concreet geval moeten worden beoordeeld. Het kan zijn dat de betrokkene over het voorgenomen gebruik wordt geïnformeerd, dan wel – een stap verder – in de gelegenheid wordt gesteld om zijn zienswijze hieromtrent te geven. De meest vergaande variant zou zijn indien aan de betrokkene voor het betreffende gebruik om toestemming wordt gevraagd.

De in het tweede lid opgenomen factoren zullen per geval verschillend worden toegepast. Een enkel voorbeeld moge de uitwerking van deze criteria verder verduidelijken. De gemeentelijke basisadministratie bevat persoonsgegevens voor velerlei uiteenlopende doeleinden. Het gaat evenwel om gegevens die personen identificeren en hun adres vastleggen. Daar de gegevens weinig informatie omtrent de betrokkenen bevatten, is het gebruik voor de uiteenlopende doeleinden gerechtvaardigd. In beginsel zijn de gegevens bestemd voor de overheid. Wanneer daarentegen een ziekenfonds op basis van de gegevens van de declaraties van een specialist een selectie maakt van patiënten die aan een bepaalde kwaal lijden en deze lijst ter beschikking stelt aan een fabrikant van hulpmiddelen die het leven met deze kwaal vergemakkelijkt, is er sprake van onverenigbaar gebruik. Aangenomen mag worden dat veel mensen niet op prijs stellen door onbekenden te worden benaderd met aanbiedingen die aan hun handicap tegemoet komt. Een dergelijk gebruik is onverenigbaar. Het gaat hier om een gevoelig gegeven, ook in de zin van het wetsvoorstel. Een selectie van personen op basis van dit criterium is niet toegestaan.
Uit deze samenhang moge blijken dat wanneer dezelfde fabrikant van medische hulpmiddelen zijn waren aanbiedt aan burgers op basis van persoonsgegevens uit de gemeentelijke basisadministratie, dit geen inbreuk is op de persoonlijke levenssfeer, terwijl een aanbieding aan dezelfde persoon, doch op basis van selectie op een criterium dat een gevoelig gegeven, bevat, welk als een dergelijke inbreuk wordt ervaren. Niet de aanbieding van handelsreclame als zodanig is wel of niet toegestaan. Beslissend is in casu het criterium op grond waarvan iemand is geselecteerd.
Hetzelfde geldt voor bij voorbeeld een creditcardmaatschappij. Deze zal op basis van de afrekeningen die hij krijgt, een vrij nauwkeurig profiel kunnen maken van het bestedingenpatroon van zijn cliënten. Een zorgvuldig geselecteerde lijst van personen met een bepaalde levenswijze, kan onder omstandigheden een belangrijke commerciële waarde vertegenwoordigen voor handelaren in produkten die inspelen op een dergelijke levenswijze. Een dergelijke profilering van personen moet, ook wanneer het gaat om de naar verhouding lichtere inbreuk op de persoonlijke levenssfeer die is verbonden met het aanbieden van reclame, als een vorm van onverenigbaar gebruik worden beschouwd.
Tot slot zij er op gewezen dat indien er geen sprake is van verenigbaar gebruik, de verwerking in uitzonderlijke omstandigheden toch rechtmatig kan zijn uit hoofde van artikel 43. Op grond van deze bepaling kan conform artikel 13 van de richtlijn de eis van verenigbaar gebruik worden doorbroken voor zover dat noodzakelijk is in het belang van een van de aldaar opgesomde doeleinden. Het gaat hier evenwel om uitzonderingen: artikel 43 dient restrictief te worden geïnterpreteerd.
Het derde lid van artikel 9 bevat daarnaast nog een aparte voorziening ten behoeve van persoonsgegevens die niet voor historische, statistische of wetenschappelijke doeleinden zijn verzameld (of verder worden verwerkt). Verdere verwerking van deze gegevens voor historische, statistische of wetenschappelijke doeleinden wordt op grond van artikel 6, eerste lid, onderdeel b, van de richtlijn, niet als onverenigbaar beschouwd mits de Lid-Staten in passende waarborgen voorzien. Als passende waarborg is in het derde lid opgenomen een verplichting van de verantwoordelijke in te kunnen staan voor een verder gebruik van de gegevens binnen deze strikte doelbinding. Hij zal daartoe de nodige maatregelen moeten treffen. In overweging 29 bij de richtlijn is bepaald dat deze maatregelen met name moeten voorkomen dat de gegevens worden gebruikt voor het nemen van maatregelen of besluiten die tegen een bepaald persoon gericht zijn. Gedacht kan worden aan een «functionele scheiding» tussen toepassing en onderzoek. De maatregelen kunnen juridisch van aard zijn: een nadere uitwerking van het gebruik dat van de gegevens mag worden

gemaakt in bij voorbeeld het aanmeldingsformulier, in een gedragscode of contractueel worden overeengekomen. Ook zijn (andere) organisatorische of technische maatregelen mogelijk. In dat laatste geval dient de verantwoordelijke deze – in geval hij de verwerking moet melden op grond van artikel 27 – te beschrijven bij de aanmelding (artikel 27, eerste lid, onder f). Een overeenkomstig voorschrift is opgenomen ten aanzien van het bewaren van gegevens (artikel 10, tweede lid). Voor gevoelige gegevens zijn in artikel 23, tweede lid, aanvullende eisen opgenomen.
Het derde lid is niet van toepassing indien het resultaat van de verwerking niet op personen herleidbare informatie betreft. De statistische informatie mag in dat geval voor allerlei (andere) doeleinden worden gebruikt, dus bijvoorbeeld ook voor marketing-doeleinden (niet zijnde direct marketing).

Koppeling en verenigbaar gebruik

Een vorm van gebruik is het koppelen van persoonsgegevens. Zowel de juridische als de sociaal-wetenschappelijke evaluatie bepleiten bijzondere regels te stellen voor situaties waarbij bijzondere gevaren voor de persoonlijke levenssfeer ontstaan. Wij hebben afgezien van een aparte bepaling over koppeling. In de praktijk is het geen eenduidig begrip. De algemene regels over het verenigbaar gebruik zijn op gegevensverwerkingen van toepassing die als koppeling worden aangemerkt.
De eis van verenigbaar gebruik brengt met zich mee dat persoonsgegevens kunnen worden gekoppeld wanneer ten minste aan de eis is voldaan dat de doeleinden waartoe de gegevens oorspronkelijk zijn verzameld, met elkaar verenigbaar zijn. In technische zin wordt daaronder soms ook de on-line consultatie verstaan. Dan gaat het om raadpleging van een databank met het oog op de mogelijke aanvulling van de gegevens omtrent personen die reeds bij degeen die consulteert bekend zijn. Dit kan nodig zijn om de de gegevens up to date te houden, terwijl het oogmerk ontbreekt om als gevolg van deze consultatie een nieuwe groep van personen naar een bepaald criterium in beeld te brengen. Een dergelijke technische voorziening kan echter ook worden gebruikt voor de vergelijking van twee verschillende bestanden met het oogmerk om te zien welke personen in beide voorkomen. Deze laatste vorm behoeft vanuit het gezichtspunt van het verenigbaar gebruik bijzondere aandacht.
De bijzondere aandacht voor koppeling ligt ook ten grondslag aan artikel 24 over identificerende nummers. Deze dienen in de praktijk immers in hoofdzaak als koppelingsinstrument. Deze bepaling geeft uitvoering aan artikel 8, zevende lid, van de richtlijn dat gaat over gevoelige gegevens. Elke vorm van verwerking behoeft een rechtvaardiging ingevolge artikel 8. Gelet op de gevoeligheid van deze verwerking zullen de factoren die aandacht behoeven bij de beoordeling of sprake is van verenigbaar gebruik, extra gewicht in de schaal leggen.
De te koppelen bestanden kunnen gegevensverwerkingen betreffen met eenzelfde doelstelling, doch onder beheer van verschillende verantwoordelijken, dan wel gegevensverwerkingen van eenzelfde verantwoordelijke, doch met elkaar onverenigbare doelstellingen. Zeer uiteenlopende casusposities kunnen zich voordoen. In het algemeen zal gelet op de toepasselijkheid van de eis van verenigbaar gebruik vooral gezocht moeten worden naar zodanige vormen van verwerking dat de mogelijk vast te stellen gegevens niet buiten de kring de personen bekend worden dan ten behoeve van wie de koppeling heeft plaatsgevonden. Zo is denkbaar dat twee bestanden van twee verschillende verantwoordelijken tegen elkaar moeten worden afgedraaid om te zien of er dubbelen in zitten, zonder dat één van de verantwoordelijke daarmee komt te beschikken over alle gegevens van de ander. Technisch kan de vergelijking van de gegevens als het ware in een «black box» plaatsvinden, waarbij mogelijke treffers aan één van beide verantwoordelijken worden meegedeeld.

Een voorbeeld is de vergelijking van het gedetineerdenbestand en het bestand van de ontvangers van een sociale uitkering. Wanneer geen aanspraak bestaat op een uitkering in geval van detentie, kunnen beide bestanden worden vergeleken met als resultaat dat eventuele treffers worden bekend gemaakt aan het desbetreffende uitvoeringsorgaan van de sociale zekerheid. Het is daartoe niet nodig dat penitentiaire inrichtingen kennis nemen van het bestand van uitkeringsgerechtigden of de uitvoeringsorganen van de sociale zekerheid kennis nemen van de gehele gedetineerdenadministratie. Dit dient dan door technische en organisatorische maatregelen te worden voorkomen. De verstrekking van treffers aan het desbetreffende uitvoeringsorgaan vindt in dat geval zijn rechtvaardiging in de opdracht de criteria voor de toekenning van een uitkering toe te passen. In dit geval vertoont het doel van de koppeling een zodanig nauwe verwantschap met het oorspronkelijke doel waarvoor het uitvoeringsorgaan de gegevens heeft verkregen dat – mede gelet op de voorzieningen die zijn getroffen om de verspreiding van de gegevens te beperken tot het noodzakelijke minimum – sprake is van verenigbaar gebruik. Anders ligt de situatie wanneer gekoppeld wordt voor een doel dat relatief ver verwijderd ligt van het doel waarvoor de gegevens zijn vergaard. In dat geval zal – los van de koppelingen die hun grondslag kunnen vinden in artikel 43 – veel eerder sprake zijn van onverenigbaar gebruik.
De vraag rijst hoe de mogelijkheden tot koppeling zich verhouden tot het regime onder de WPR. Er is onder de WPR in de private sector geen algemene mogelijkheid om uit een registratie gegevens te verstrekken in afwijking van het doel, ook niet in individuele gevallen. Artikel 11, eerste lid, kende een strikte doelbinding: een verstrekking moet voortvloeien uit het doel van de registratie. Dat heeft tot gevolg dat de ruimere norm van het verenigbaar gebruik ingevolge artikel 6, eerste lid, slechts geldt voor het gebruik binnen de organisatie van de houder. Slechts in bepaalde nauw omschreven situaties kan daarvan worden afgeweken. Voor de overheid biedt artikel 18, derde lid, WPR de bevoegdheid om een inbreuk te maken op de doelbinding. Dit artikel kent het element «desgevraagd». In de jurisprudentie van de Registratiekamer is dit uitgelegd als een beperking van de bevoegdheid tot verstrekking van gegevens van een individuele persoon of een beperkte groep van personen. Dit heeft tot gevolg dat voor koppeling van persoonsregistraties met uiteenlopende doelen voor de overheid onder de WPR een afzonderlijke machtiging van de wetgever nodig is.
De ontwikkelingen in de informatietechnologie leiden tot verruimde mogelijkheden tot koppeling en van de maatschappelijke acceptatie ervan. Er is daarom van afgezien strikte bepalingen op dit punt te handhaven of voor te stellen. Ook wordt het onderscheid tussen de private en de publieke sector opgeheven. Daar waar koppeling tot vergaande consequenties dreigt te leiden is er de mogelijkheid om de norm van het verenigbaar gebruik op een op de desbetreffende sector toegespitste wijze invulling te geven via een jurisprudentiële concretisering of een nadere uitwerking in bij voorbeeld gedragscodes.

Geheimhoudingsplicht

Het vierde lid bevat een nadere precisering van de norm van de artikelen 8 en 9 aangebracht. Bepaald is dat de verwerking van persoonsgegevens achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat. Met deze bepaling wordt buiten twijfel gesteld dat een ambts- of beroepsgeheim dan wel een wettelijke verplichting tot geheimhouding niet kan worden terzijde geschoven door het bepaalde in artikel 8.
De bepaling is ontleend aan het huidige artikel 11, derde lid, WPR met dien verstande dat haar bereik ruimer is: ze betreft iedere vorm van

verwerking van persoonsgegevens. Het bestaande beschermingsniveau van de WPR wordt aldus verruimd tot iedere vorm van gegevensverwerking. Voor deze verruiming is – in navolging van het advies van de Registratiekamer – gekozen omdat niet uitgesloten kan worden geacht dat ook andere handelingen met persoonsgegevens dan het enkele verstrekken aan derden, een inbreuk kunnen opleveren met de geheimhoudingsverplichting. Indien het gaat om een omgeving waar de beveiliging van gegevens niet verzekerd kan worden, zouden ook de vastlegging en bewaring daaronder kunnen vallen.
De bepaling dient in samenhang te worden bezien met artikel 61, vijfde lid. Op een geheimhoudingsverplichting kan geen beroep worden gedaan indien de Registratiekamer inlichtingen verlangt in verband met de betrokkenheid bij de verwerking van persoonsgegevens van degene op wie de geheimhoudingsverplichting rust.

Artikel 10

Eerste lid

Deze bepaling geeft uitvoering aan artikel 6, eerste lid, onder e, van de richtlijn. De eerste volzin vindt zijn uitwerking in artikel 10, eerste lid. Overeenkomstig het advies van de Registratiekamer en in de lijn met hetgeen is opgemerkt t.a.v. de begripsomschrijving van «persoonsgegeven» in artikel 1, is het woord «herleidbaar» uit het voorschrift geschrapt.
De WPR kent geen afzonderlijke regels voor de bewaring van gegevens. Het redelijk belang dat de houder dient te hebben bij het doel van de registratie (artikel 4, eerste lid), het vereiste dat de gegevens in overeenstemming dienen te zijn met het doel van de registratie (artikel 5, eerste lid) en – ten aanzien van de persoonsregistraties in de publieke sector – het voorschrift dat de persoonsregistratie noodzakelijk dient te zijn voor de goede vervulling van de taak van de houder (artikel 18, eerste lid) impliceren echter dat gegevens uit een registratie moeten worden verwijderd wanneer deze voorwaarden niet langer gelden.
In het Besluit genormeerde vrijstelling waren ten aanzien van specifieke persoonsregistraties bewaartermijnen opgenomen. Registraties die na afloop van deze bewaartermijn werden verwijderd behoefden niet te worden aangemeld bij de Registratiekamer. Een voorbeeld daarvan is artikel 5, tweede lid, van het besluit waarin is bepaald dat persoonsgegevens uit standaardpersoneelsadministraties dienen te worden verwijderd uiterlijk twee jaren nadat het dienstverband of de werkzaamheden van de betrokkene ten behoeve van de verantwoordelijke zijn beëindigd. Ook is soms in bijzondere wetgeving de algemene termijn gedurende gegevens kunnen worden bewaard, gefixeerd. Zo is in artikel 7:454, derde lid, BW de termijn gedurende welke medische gegevens in een dossier mogen worden bewaard in de regel vastgesteld op tien jaren. Het onderhavige artikel beoogt op dit punt geen wijzigingen aan te brengen. Dit brengt met zich dat de verantwoordelijke zich dient af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven. Zijn er voldoende redenen dan kan hij bepalen welke termijnen gelden om die gegevens te bewaren. Zijn die termijnen verlopen dan zal hij de gegevens niet meer mogen verwerken, tenzij voor een ander, daarmee verenigbaar doel, bij voorbeeld statische archivering. In voorkomende gevallen kunnen in de bijzondere wetgeving nadere regels worden gesteld. Voorts kunnen in de algemene maatregel van bestuur als bedoeld in artikel 29 – gelet op het tweede lid, onder e van dit artikel – criteria of termijnen worden geformuleerd.
In specifieke omstandigheden kan het doeleinde met zich brengen dat persoonsgegevens voor onbepaalde tijd mogen worden bewaard. In dit verband kan worden gewezen op de archiefbescheiden als bedoeld in de

Archiefwet 1995 die naar een archiefbewaarplaats zijn overgebracht. Voor deze bescheiden geldt onder meer als doeleinde: behoud van (een deel van) het Nederlandse culturele erfgoed. Daarmee is de termijn gedurende welke de daarin opgenomen persoonsgegevens mogen worden bewaard, in beginsel onbepaald.

Tweede lid

Het tweede lid is een uitwerking van artikel 6, eerste lid, onder e, tweede volzin, van de richtlijn. Het gaat hier om persoonsgegevens die niet voor historische, statistische of wetenschappelijke doeleinden zijn verzameld (of verder worden verwerkt). Deze gegevens mogen desalniettemin voor historische, statistische of wetenschappelijke doeleinden langer worden bewaard mits de Lid-Staten voorzien in passende waarborgen. In de lijn van artikel 9, derde lid, is als passende waarborg opgenomen een verplichting van de verantwoordelijke in te kunnen staan dat de gegevens enkel binnen deze strikte doelbinding worden gebruikt. Hij zal daartoe de nodige maatregelen moeten treffen. Verwezen wordt naar de toelichting bij artikel 9, derde lid. Voor gevoelige gegevens zijn in artikel 23, tweede lid, aanvullende eisen opgenomen.

Artikel 11

Het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, is bepalend voor de hoeveelheid en de soort gegevens die onderwerp van verwerking vormen. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn (eerste lid). Tevens dienen persoonsgegevens juist en nauwkeurig te zijn (tweede lid).
Het artikel legt op degene die de gegevens verwerkt een continue verplichting tot toetsing. Elke keer dat gegevens bij voorbeeld worden verwerkt voor een ander – met het oorspronkelijk doel verenigbaar – doel dient immers de toets die dit artikel voorschrijft, plaats te vinden. Ook is het mogelijk dat de (oorspronkelijke) doelbinding in de loop der tijden op een andere wijze wordt geïnterpreteerd hetgeen gevolgen kan hebben voor de gegevens die ten behoeve van dat doel mogen worden verwerkt.

Eerste lid

Het eerste lid is een uitwerking van artikel 6, eerste lid, onderdeel c, van de richtlijn. De gegevens dienen, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig te zijn. In dit lid is de norm van artikel 5, eerste lid, van de WPR geïncorporeerd.
Indien de verantwoordelijke een zo beperkt aantal gegevens verwerkt dat in redelijkheid niet kan worden gezegd dat hij daarmee, gelet op de doeleinde waarvoor hij de gegevens wenst te verwerken, een juist beeld van de betrokkene heeft, overtreedt hij het voorschrift dat de gegevens met het oog op het doel waarvoor ze worden verwerkt, toereikend dienen te zijn. Als voorbeeld kan worden genoemd de registratie van het gegeven dat betrokkene niet betaald heeft voor een bepaald produkt zonder daarbij te vermelden dat dit niet betalen te wijten is aan het feit dat die betrokkene niet tevreden is met dit produkt en om die reden de betaling heeft opgeschort. Eveneens kan in dit kader worden gedacht aan het verzuimen van het aanbrengen van de herstelcodes in het BKR.
Daar staat tegenover dat de gegevens die worden verwerkt evenmin met het oog op het doel waarvoor ze worden verwerkt bovenmatig mogen zijn. De winkelier die ten behoeve van de bestrijding van winkeldiefstal een registratie opzet van personen die hij heeft betrapt op winkeldiefstal zal in de regel niet behoeven te registreren welke goederen door de

betrokkene uit zijn winkel zijn ontvreemd, wel bij voorbeeld de waarde daarvan.
Tot slot dienen de gegevens met het oog op de doeleinde waarvoor ze worden verwerkt ter zake dienend te zijn. De boven reeds aangehaalde winkelier mag bij voorbeeld geen gegevens omtrent het (legale) koopgedrag van de betrokken persoon in zijn registratie opslaan.

Tweede lid

Het tweede lid is een uitwerking van artikel 6, eerste lid, onderdeel d, van de richtlijn. Het voorschrift gaat meer uit van een inspanningsverplichting voor de verantwoordelijke dan het eerstgenoemde: de verantwoordelijke moet de nodige maatregelen treffen opdat de gegevens juist en nauwkeurig zijn. Op hem wordt geen absolute verplichting gelegd. Een garantie voor de juistheid van gegevens kan van hem niet worden gevergd. De juistheid van de gegevens wordt mede bepaald door de context waarin ze worden gebruikt (zie ook de toelichting op het begrip «verantwoordelijke» in artikel 1, onder d). Een bank die voor de uitvoering van een betalingsopdracht gegevens in moet voeren in een berichtenveld is gehouden de gegevens in te voeren zoals die door de opdrachtgever worden aangereikt en heeft niet de verplichting de gegevens nader te verifieren. Dit geldt ook voor de verantwoordelijke die verplicht is de gegevens op te nemen zoals die uit een notariële akte blijken.
Met «nodige» maatregelen wordt uitgedrukt dat alle maatregelen moeten worden getroffen die in redelijkheid kunnen worden gevergd. De redelijkheid stelt daarbij, afhankelijk van bij voorbeeld de soort gegevens die onderwerp van verwerking zijn, de stand van techniek en de kosten die met de maatregelen gepaard gaan, grenzen aan de te nemen maatregelen. Dit voorschrift sluit aan bij artikel 5, tweede lid, van de WPR.

Artikel 12

Eerste lid

Het eerste lid neemt de norm over van artikel 16 van de richtlijn over de vertrouwelijkheid van de gegevensverwerking. Het uitgangspunt is dat de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking. Deze verantwoordelijkheid kan hij slechts dragen wanneer zijn ondergeschikten of degenen die in opdracht van de verantwoordelijke gegevens verwerken, zich naar zijn aanwijzingen richten.
Ieder die handelt onder het gezag van de verantwoordelijke dienen te handelen overeenkomstig de door de verantwoordelijke gegeven aanwijzingen. Dit gezag kan zijn grond vinden in een arbeidscontract, doch ook in een aanbestedingscontract of elke rechtsverhouding waarin de zeggenschap van de verantwoordelijke stilzwijgend of uitdrukkelijk ligt besloten.

Tweede lid

Het tweede lid vormt een precisering van de door artikel 16 van de richtlijn beoogde vertrouwelijkheid. De bepaling legt een geheimhoudingsplicht op aan de bewerker, alsmede degenen die onder het gezag van de verantwoordelijke of de bewerker werkzaam zijn. In beginsel kan slechts een uitdrukkelijke wettelijke verplichting op de geheimhoudingsplicht een inbreuk maken. Zo is bij voorbeeld artikel 161 van het Wetboek van Strafvordering een bevoegdheid tot het doen van aangifte van een strafbaar feit. Deze bepaling zet de onderhavige geheimhoudingsbepaling niet opzij. Daarentegen bevat artikel 162 van het Wetboek van Strafvordering een wettelijke verplichting voor ambtenaren tot het doen van aangifte in bepaalde gevallen. Een dergelijke verplichting

geldt, evenals een wettelijke verplichting aan ambtenaren om inlichtingen te verstrekken uit openbare registers die bij wet zijn ingesteld, als een verplichting als bedoeld in de onderhavige bepaling.
Daarnaast kan blijkens het tweede lid de geheimhouding worden doorbroken voor zover uit de taak van de betreffende persoon de noodzaak tot mededeling voortvloeit. Of een noodzaak tot mededeling aanwezig is, wordt bepaald door de verantwoordelijke onder wiens gezag of in wiens opdracht de persoon werkzaam is. Uiteraard is deze bevoegdheid van de verantwoordelijke evenmin onbegrensd. De verantwoordelijke is immers op zijn beurt gehouden aan regels inzake doelbinding en verenigbaar gebruik.
De richtlijn laat, zoals gebruikelijk in het communautaire recht, de sanctionering van de norm over aan de lid-staten. Blijkens de jurisprudentie van het Europese Hof van Justitie op artikel 189 van het EG-Verdrag eist het gemeenschapsrecht wel een daadwerkelijke sanctionering. De belangen van zowel de verantwoordelijke als van de betrokkene zijn hierbij in het geding. Een uitdrukkelijke, strikt geformuleerde geheimhoudingsbepaling is een passende nationale implementatie van de communautaire norm. Deze is neergelegd in het tweede lid. Bij de formulering is aansluiting gezocht bij de standaard-geheimhoudingsbepaling (zie punt 163 van de Aanwijzingen voor de regelgeving). Het gaat om een aanvullende plicht. Geldt reeds bij voorbeeld uit hoofde van medisch beroepsgeheim of ambtsgeheim een dergelijke plicht, dan is de onderhavige bepaling niet van toepassing.
De geheimhoudingsbepaling is een verplichting uit hoofde van een wettelijk voorschrift als bedoeld in artikel 272 van het Wetboek van Strafrecht. Opzettelijke niet-naleving kan worden bestraft met gevangenisstraf van vier jaren of geldboete van vijfentwintigduizend gulden. Van een dergelijke opzet is in ieder geval sprake indien wordt gehandeld in strijd met een uitdrukkelijke aanwijzing van de verantwoordelijke of een waarschuwing van enige toezichthouder. Een en ander geldt ook ten aanzien van strijd met een aanwijzing of een terzake bekend standpunt van de Registratiekamer.
Daar de bepaling niet uitsluitend strekt tot bescherming van de belangen van de betrokkene, is het karakter van het klachtdelict dat eigen is aan artikel 272, hieraan ontnomen. Aansluiting is gezocht bij de gedachte van artikel 30, tweede lid, van de Wet politieregisters: het gaat om het algemene belang van een behoorlijke naleving van de onderhavig wetgeving. Zou in voorkomend geval het belang van de betrokkene strijdig zijn met een strafvervolging, dan kan dit slechts gewicht in de schaal leggen bij de afweging van de opportuniteit van strafrechtelijk optreden.

Artikel 13

De bepaling geeft uitvoering aan artikel 17 van de richtlijn en sluit aan bij de bestaande bepaling van artikel 8 WPR. Het beveiligingsvoorschrift richt zich tegen «verlies of enige vorm van onrechtmatige verwerking van gegevens». Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking. Zie ook paragraaf 10.3 over openbare registers wat betreft de vormen van verstrekking en openbare bekendmaking die onverenigbaar zijn met het doel van de register.
In het begrip «passende» ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Dit is in eerste aanleg een vraag van professionele ethiek van personen belast met de informatiebeveiliging. De normen van deze ethiek worden in deze bepaling van een juridisch sluitstuk voorzien, in die zin dat daaraan een wettelijke

verplichting voor de verantwoordelijke is verbonden. Het is niet aan de wetgever om nadere details te geven over de aard van de beveiliging. Dergelijke details zouden sterk tijdgebonden zijn en daarmee afbreuk doen aan het nagestreefde niveau van beveiliging.
Het begrip «passend» duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate bij voorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is geen verplichting om steeds de allerzwaarste beveiliging te nemen. Daarom duidt ook het feit dat inbreuken zijn gemaakt op het beveiligingsniveau niet noodzakelijkerwijs op nalatigheid in de beveiliging. Er moet sprake zijn van een adequate beveiliging. Het voorschrift gaat daarmee verder dan artikel 138a, eerste lid, onderdeel a, van het Wetboek van Strafrecht, waar wordt gesproken van «enige beveiliging».
Technische en organisatorische maatregelen dienen cumulatief te worden getroffen. Software is een belangrijk instrument tot beveiliging. Dit wetsvoorstel geeft de normen die mede met behulp van software dienen te worden gehandhaafd. Klassieke technische beveiligingsmaatregelen omvatten mede de fysieke afscherming van de randapparatuur die toegang geeft tot de te beveiligen gegevens. Daarnaast zijn er de modernere informatietechnologische maatregelen zoals beveiliging met een «password» en door middel van encryptie. Grotere bedrijven zullen een eigen beveiligingsafdeling hebben. Kleinere bedrijven zullen beveiligingsexpertise van buitenaf inhuren. Wat betreft encryptie zijn de initiatieven vermeldenswaard van de Europese Commissie om te komen tot een min of meer uniform systeem van vertrouwenstussenpersonen (trusted third parties) binnen de Europese Unie.

Artikel 14

Voor de verschillen tussen de WPR en het wetsvoorstel wat betreft het bewerkerschap, zij verwezen naar de toelichting op artikel 1, onder e. De tweede volzin van artikel 8 WPR, is in het onderhavig wetsvoorstel uitgewerkt in een aparte bepaling. De strekking van de bepaling is te voorkomen dat bij eventuele tekortkomingen in de gegevensverwerking, verantwoordelijke en bewerker zich wat betreft hun verantwoordelijkheden achter elkaar zouden kunnen verschuilen. De verplichtingen moeten over en weer duidelijk zijn neergelegd. Op de verantwoordelijke rust een zorgplicht daarvoor zorg te dragen. Niet alleen dient hij civielrechtelijk de bewerker voldoende te hebben duidelijk gemaakt hoe met de persoonsgegevens wordt omgegaan, tevens dient hij toe te zien op de feitelijke naleving van de aldus gecreëerde verplichtingen.
Het tweede en derde lid maken duidelijk dat het om juridisch bindende voorschriften moet gaan: bindend in de zin dat de bewerker jegens de verantwoordelijke datgene waartoe de verantwoordelijke vanuit zijn verantwoordelijkheid verplicht is, ook als zijn eigen verplichting op zich neemt. Onderdeel a verwijst in het voetspoor van het advies van de Registratiekamer naar artikel 12, eerste lid. Het bepaalt dat de verantwoordelijke ervoor zorg draagt dat de bewerker handelt overeenkomstig die bepaling. Daardoor is de wettelijke verplichting tevens een verbintenis jegens de verantwoordelijke.
De overeenkomst tussen de verantwoordelijke en de bewerker moet naar zijn aard betrekking hebben op de gegevensverwerking. Het contract mag niet betrekking hebben op een vorm van dienstverlening waar de gegevensverwerking slechts een uitvloeisel van is. Het tweede en derde lid kunnen tot consequentie hebben dat lopende contracten en andere rechtsverhoudingen als in dit artikel bedoeld, herziening behoeven.
Het vierde lid geeft uitvoering aan artikel 17, derde lid, tweede liggende

streepje van de richtlijn, voor zover daarinis bepaald dat wanneer de bewerker is gevestigd in een andere lid-staat van de Europese Unie,het recht van het land van vestiging van toepassing is. Deze bepaling is noodzakelijk in het licht van de interne markt, ook op het gebied van bewerkerscontracten, zonder handelsbelemmeringen.

Het vijfde lid stelt het bewijs veilig waaruit van de verplichtingen van de bewerker blijkt. Het kan niet gaan om mondelinge afspraken. De ratio is dat de betrokkene als een soort impliciete derde belanghebbende, in geval jegens hem onrechtmatig wordt gehandeld, over de nodige bewijsstukken kan beschikken wanneer deze overeenkomstig de regels van het procesrecht een rol gaan spelen. Klassiek zou daartoe een schriftelijke neerslag van de afspraken, van belang kunnen zijn. In de toekomstige informatiemaatschappij zijn ook andere, gelijkwaardige vormen van gegevensopslag denkbaar, bij voorbeeld door tussenkomst van personen die zich als een soort «elektronische notaris» op de markt aanbieden wat betreft de zekerstelling van gewisselde gegevens en alles wat daarmee samenhangt.

Artikel 15

Artikel 6, eerste lid, van de richtlijn bevat een aantal vereisten betreffende de kwaliteit van persoonsgegevens. Deze vereisten zijn als algemene beginselen geformuleerd en richten zich niet tot een bepaalde actor. In hoofdstuk 2 van dit wetsvoorstel worden deze vereisten nader uitgewerkt waarbij artikel 6 als algemene norm geldt: persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Deze algemene norm vindt vervolgens zijn uitwerking in de overige artikelen van dit wetsvoorstel. Een ieder die persoonsgegevens verwerkt heeft deze beginselen – ongeacht in welke hoedanigheid hij ze verwerkt – in acht te nemen. Desalniettemin rust op de verantwoordelijke een extra verplichting: op grond van het tweede lid van dat artikel dient hij namelijk zorg te dragen voor de naleving van deze vereisten. Hij dient de nodige maatregelen te treffen c.q. garanties te bedingen dat degene die de gegevens verwerkt, zich houdt aan deze algemene beginselen. In dit kader dient ook artikel 14, tweede lid, van dit wetsvoorstel te worden bezien: de verplichting van de verantwoordelijke een overeenkomst aan te gaan met de bewerker. In deze overeenkomst kunnen de nodige garanties worden bedongen of voorwaarden worden gesteld. Dit laat onverlet de verantwoordelijkheid van een ieder die gegevens verwerkt de algemene beginselen in acht te nemen. Is de verantwoordelijke op de hoogte van een schending van deze beginselen en laat hij na de nodige maatregelen te treffen dan is hij hierop aanspreekbaar.

PARAGRAAF 2 DE VERWERKING VAN BIJZONDERE GEGEVENS

Artikel 16

In deze bepaling is de grondgedachte van artikel 8 van de richtlijn geïmplementeerd, namelijk dat de verwerking van specifiek in de richtlijn opgesomde gevoelige persoonsgegevens door de lidstaten moet worden verboden. Van dit verbod kan alleen ontheffing worden verleend indien de verwerking zijn grondslag vindt in een van de overige bepalingen van paragraaf 2. De belangrijkste algemene garantie – verwoord in het hierna te bespreken artikel 23, eerste lid, onder e – is dat verwerking van dergelijke gegevens niet is toegestaan dan voor zover dat bij wet is bepaald. In het overgrote deel van de gevallen zal een verwerking op de onderhavige wetsvoorstel kunnen worden gebaseerd. Het is echter niet uitgesloten dat in specifieke situaties een basis gecreëerd zal worden in een bijzondere wet. Voor gevoelige gegevens, zoals opgesomd in artikel 8 van de richtlijn, geldt op grond van artikel 8, vierde lid, als hoofdregel dat

een verwerking slechts kan worden toegestaan in bijzondere wetgeving als de verwerking door een algemeen zwaarwegend belang wordt gerechtvaardigd. De richtlijn geldt immers ook voor andere wetten voor zover zij worden bestreken door het communautaire recht. Deze voorwaarde is uitdrukkelijk in artikel 23 tot uitdrukking gebracht. Voor een nadere uitleg zij verwezen naar de toelichting op dat artikel.
Artikel 16 is conform de richtlijn geformuleerd als een verbod. Dit impliceert dat als hoofdregel geldt dat verwerking van gevoelige gegevens niet is toegestaan. De daarop volgende bepalingen (artikel 17 tot en met 23) zijn in dezelfde sleutel geplaatst en geformuleerd als een ontheffing van het algemene verwerkingsverbod. Langs deze weg wordt ook tot uitdrukking gebracht dat artikel 17 e.v. niet zonder meer legitimeren tot gegevensverwerking: zij doorbreken slechts een verbod. Vervolgens zal aan de hand van de algemene beginselen van gegevensverwerking – zoals vastgelegd in artikel 6 tot en met 15 van het wetsvoorstel – moeten worden vastgesteld of de gegevensverwerking in het concrete geval rechtmatig is.
De Registratiekamer heeft er terecht op gewezen dat artikel 16 in een enkel opzicht een verhoging van het beschermingsniveau oplevert in vergelijking tot het huidige regime. Zo heeft artikel 1 BGG uitsluitend betrekking op het «opnemen» van gevoelige gegevens in een persoonsregistratie, terwijl artikel 16 – conform de richtlijn – in algemene zin ziet op het «verwerken» daarvan. Aldus is het bijzondere regime inzake gevoelige gegevens van toepassing op alle stadia van het proces van gegevensverwerking. Het is de vraag in hoeverre dit ook in de praktijk een aanscherping zal betekenen. Onder het regime van de WPR werkt het gevoelige karakter van de gegevens door in de wijze waarop de algemene wettelijke regels worden toegepast. Als gevolg daarvan kan per saldo hetzelfde resultaat worden bereikt. Niettemin is niet uitgesloten dat de uitbreiding van het regime inzake gevoelige gegevens tot alle verwerkingen, in bepaalde gevallen tot meer bescherming zal leiden.
Conform het huidige artikel 1 BGG wordt in artikel 16 gesproken over persoonsgegevens «betreffende» een aantal met name genoemde categorieën. Hiermee wordt beoogd aan te sluiten bij het thans geldende recht. Zoals de Registratiekamer terecht in zijn advies opmerkt, wordt daarbij uitgegaan van een onderscheid tussen «direct» en «indirect» gevoelige gegevens. Afgezien van gegevens die als zodanig betrekking hebben op een gevoelig kenmerk – aangeduid als «direct» gevoelige gegevens – worden tot de gevoelige gegevens ook gerekend de gegevens die weliswaar als zodanig daarop geen betrekking hebben, maar waaruit wel de aanwezigheid van een gevoelig kenmerk rechtstreeks kan worden afgeleid. Een eerder genoemd voorbeeld van het laatste is de administratie van een kerkgenootschap waarin alle namen en adressen van de leden zijn opgenomen. Weliswaar hebben deze namen en adressen op zichzelf beschouwd geen betrekking op een gevoelig kenmerk, doch uit de opneming van deze gegevens in de administratie van het kerkgenootschap vloeit dwingend voort dat het gaat om gegevens betreffende de godsdienstige overtuiging van betrokkenen. Noodzakelijk is wel dat er een rechtstreeks verband is. Gegevens die hooguit een indicatie geven dat het om een gevoelig kenmerk zou kunnen gaan, vallen – zoals de Registratiekamer terecht stelt – buiten de reikwijdte van de bijzondere regeling voor gevoelige gegevens. Voor een nadere uiteenzetting zij verwezen naar de nota van toelichting van het BGG.
In artikel 16 is zoveel mogelijk aangesloten bij de terminologie die ook wordt gehanteerd in de richtlijn. Wat betreft de categorieën van persoonsgegevens die als gevoelig worden aangemerkt, zijn er enkele verschillen tussen enerzijds de richtlijn en de WBP en anderzijds het BGG en de WPR. In de bepaling wordt bijvoorbeeld gesproken over persoonsgegevens betreffende iemands gezondheid in plaats van de formulering die thans in artikel 7 WPR en het BGG wordt gebruikt. Daarin wordt het begrip

«persoonsgegevens van medische en psychologische aard» gebruikt. De richtlijnterminologie is op dit punt enerzijds ruimer, anderzijds beperkter dan het BGG. De richtlijn is ruimer daar waar «gegevens omtrent gezondheid» meer omvat dan «gegevens van medische aard». Het enkele gegeven dat iemand ziek is, is – conform de richtlijn – een gezondheidsgegeven in de zin van het wetsvoorstel, doch is geen medisch persoonsgegeven: zij omvat geen nadere informatie over de aard van de ziekte. Anderzijds omvatten gezondheidsgegevens niet zonder meer psychologische gegevens. Weliswaar zullen psychologische gegevens vaak tevens iemands lichamelijke of geestelijke gezondheid raken, doch dit behoeft niet altijd het geval te zijn. De formulering van de richtlijn en de WBP is aldus beperkter. Hetzelfde geldt voor het begrip «seksuele leven» dat in de plaats komt van de thans gebruikte zinsnede «seksualiteit of intiem levensgedrag». Ook hier zijn de richtlijn en de WBP beperkter aangezien niet alle vormen van intiem levensgedrag het seksuele leven betreffen. Overigens mag hieruit niet zonder meer worden afgeleid dat er ook sprake zal zijn van een vermindering van bescherming ten opzichte van de WPR. Via het op artikel 7 van de richtlijn gebaseerde artikel 8, in het bijzonder kan gewezen worden op de in onderdeel f opgenomen noodzakelijkheidstoets, blijft de thans op grond van de WPR gebaseerde bescherming van psychologische gegevens en persoonsgegevens inzake intiem levensgedrag, in belangrijke mate intact. Het is meer zo dat voor de categorieën van gevoelige persoonsgegevens die wel onder de reikwijdte van de richtlijn vallen, als gevolg van artikel 16 e.v. een hoger beschermingsniveau wordt gerealiseerd dan in de huidige situatie het geval is.
Voor het overige is er de voorkeur aan gegeven dezelfde begrippen te blijven gebruiken als in artikel 1 van de Grondwet en de Algemene wet gelijke behandeling. De begrippen ras, godsdienst, levensovertuiging en politieke gezindheid hebben in het Nederlandse recht inmiddels een gevestigde traditie. Het is onwenselijk om daarvan af te wijken. Dit is mogelijk omdat met de terminologie in de richtlijn geen andere resultaten worden beoogd. Met name is van belang om op te merken dat het begrip «ras» naar Nederlands recht ruim wordt uitgelegd en ook het in de richtlijn gebruikte begrip «etnische afkomst» omvat.
Wat betreft de persoonsgegevens van strafrechtelijke of tuchtrechtelijke aard geldt ingevolge artikel 8, vijfde lid, een afzonderlijke regime. Niettemin is er – mede gelet op artikel 7 WPR en het huidige BGG – geen reden om voor deze gegevens een ander uitgangspunt te kiezen dan hetgeen in artikel 16 is verwoord. De gegevens in verband met strafbaar of hinderlijk gedrag worden derhalve in dit artikel met andere gevoelige gegevens op één lijn gesteld. In deze gevallen betreft het personen die anders worden behandeld dan anderen omdat zij in verband worden gebracht met verwijtbaar gedrag.

Artikel 17

Deze bepaling is een voortzetting van artikel 2 BGG. Zij is aangepast aan artikel 8 van de richtlijn. Artikel 8, tweede lid onder d, bevat voorschriften die grenzen stellen aan de verwerking van persoonsgegevens door kerkgenootschappen en andere genootschappen op geestelijke grondslag. Een dergelijke verwerking mag zich slechts uitstrekken tot personen die lid zijn van het desbetreffende genootschap, alsmede tot degenen met wie het genootschap in verband met haar doelstelling regelmatige contacten onderhoudt.
De mate waarin gesproken kan worden van lidmaatschap zal per genootschap verschillen. Dit wordt in belangrijke mate bepaald door het statuut van het betrokken genootschap, bedoeld in artikel 2:2, tweede lid, BW en moet mede worden begrepen tegen de achtergrond van de aard van de relatie tussen het betrokken genootschap en de betrokkene. De vrijheid van kerkgenootschappen en andere genootschappen op geeste-

lijke grondslag om zelf in hun statuut de werkwijze en de organisatie te regelen moet worden gezien in het licht van de in artikel 6, eerste lid, van de Grondwet gewaarborgde vrijheid van godsdienst en levensovertuiging. Om deze vrijheid te respecteren is er voor gekozen de term «behoren tot», die ook reeds gebruikt is in het BGG, te hanteren. Afhankelijk van hetgeen in de relatie tussen een kerkgenootschap of een ander genootschap op geestelijke grondslag met haar leden gebruikelijk is, wordt met deze neutrale term gedoeld op doopleden, geboorteleden en dergelijke.
Daarnaast blijft krachtens artikel 17 – uiteraard binnen de grenzen van de algemene beginselen van gegevensverwerking – de bevoegdheid gehandhaafd om ook persoonsgegevens van gezinsleden te verwerken, voor zover het gaat om genootschappen of onderdelen daarvan als bedoeld in onderdeel a. Deze bepaling vormt een voortzetting van artikel 2, tweede lid, BGG. De richtlijn laat die mogelijkheid open, zij het dat daarvoor stringente voorwaarden gelden. De richtlijn vormt op dit punt een aanscherping van het BGG. Zo is krachtens artikel 8, tweede lid, onder d, van de richtlijn alleen verwerking toegestaan van gegevens van personen met wie het genootschap «regelmatige contacten» onderhoudt. De hoedanigheid van gezinslid is op zichzelf dus niet voldoende. Uit feiten en omstandigheden zal moeten blijken dat een gezinslid van degene die tot het genootschap of de instelling behoort, met dat genootschap ook een feitelijke relatie onderhoudt. Deze relatie hoeft uiteraard niet zo intensief te zijn als met actieve leden het geval is; het contact kan bijvoorbeeld hierin bestaan dat vertegenwoordigers van het genootschap regelmatig, bijvoorbeeld een keer per jaar, in het kader van de pastorale zorg op bezoek gaan bij het gezin van degene die tot het genootschap behoort. Noodzakelijk is dan wel dat de hiermee verband houdende gegevensverwerking niet gebeurt tegen de uitdrukkelijke wens van het betrokken gezinslid. Om die reden wordt als aanvullende voorwaarde gesteld dat verwerking alleen is toegestaan als het gezinslid daartegen geen schriftelijk bezwaar heeft gemaakt.
Voorts geldt als algemene voorwaarde dat het genootschap geen gegevens aan derden mag verstrekken zonder toestemming van de betrokkene, degene die tot het genootschap behoort of een gezinslid hiervan. Deze voorwaarde vloeit eveneens voort uit artikel 8, tweede lid onder d, van de richtlijn. De betrokkene is vrijwillig toegetreden tot een kerkgenootschap of een genootschap op geestelijke grondslag. Om die reden dient er van te worden uitgegaan dat zijn toestemming zich slechts uitstrekt tot verwerking van gegevens door dat genootschap en niet tot verwerking van gegevens door anderen. In dat licht bezien ligt het voor de hand om voor verstrekking van gegevens aan derden steeds toestemming van de betrokkene te vragen.
Overigens is er niet voor gekozen om gebruik te maken van de door artikel 8, tweede lid, onder d, van de richtlijn geboden mogelijkheid om de bestaande mogelijkheid om persoonsgegevens van gezinsleden van de betrokkene te verwerken uit te breiden en de bevoegdheid daartoe ook toe te kennen aan andere instellingen op godsdienstige of levensbeschouwelijke grondslag. Tot dusverre is niet gebleken van een behoefte daartoe. Uit een oogpunt van bescherming van persoonsgegevens verdient het de voorkeur om de bestaande beperking tot de in artikel 17, eerste lid, onderdeel a, genoemde genootschappen te handhaven. Artikel 17, tweede lid, dient in dit verband te worden beschouwd als een precisering in de zin van artikel 5 van de richtlijn.
Het onderhavige artikel bevat verder een ontheffing voor de verwerking van gegevens door instellingen op godsdienstige of levensbeschouwelijke grondslag. Hierbij kan worden gedacht aan de kerkelijke gezindte van bijvoorbeeld (bestuurs-)leden en personeelsleden van instellingen op confessionele grondslag in de zorgsector. Onder deze bepaling valt ook de verwerking van gegevens omtrent de godsdienstige overtuiging van personen door bejaardentehuizen, onderwijsinstellingen en ziekenhuizen

met een godsdienstige of levensbeschouwelijke grondslag, voor zover dit noodzakelijk is voor de verwezenlijking van deze grondslag. Een dergelijke verwerking kan bijvoorbeeld noodzakelijk zijn in het kader van een benoemings- en toelatingsbeleid van de instelling dan wel om een proportionele vertegenwoordiging van bepaalde stromingen of richtingen binnen de instelling te behouden of te bewerkstelligen.
Deze bepaling geldt eveneens als implementatie van artikel 8, tweede lid onder d. In dit artikel gaat het om non-profitinstellingen, die ter uitvoering van hun maatschappelijke activiteiten gegevens verwerken over personen met wie zij regelmatige contacten onderhouden. De bepaling voorziet in de door de richtlijn geëiste garanties door als voorwaarde te stellen dat verwerking van gegevens alleen is toegestaan voor zover deze gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag noodzakelijk is. Met deze bepaling wordt tevens aangesloten bij de artikelen 5, tweede lid, onderdelen a en c, en 7, tweede lid van de Algemene wet gelijke behandeling. De bepaling brengt met zich dat het de instelling alleen is toegestaan om gegevens met betrekking tot godsdienst of levensovertuiging van personen te verwerken wanneer deze gegevens overeenkomen met de grondslag van de instelling. Een op de katholieke godsdienst georiënteerde school zal bijvoorbeeld gezien haar doelstellingen in beginsel enkel de katholieke geloofsovertuiging van haar leerlingen mogen verwerken, tenzij in verband met de grondslag een verdergaande verwerking kan worden gerechtvaardigd. De grondslag en de doelstellingen van de school brengt immers niet noodzakelijkerwijs met zich dat tevens gegevens omtrent andere geloofsovertuigingen van de leerlingen moeten worden verwerkt.
Ten slotte is een bepaling opgenomen voor de verwerking van gegevens voor de geestelijke verzorging. Hier is, in tegenstelling tot hetgeen bepaald is in het eerste lid onder a en b, het doel van de verwerking bepalend. Gedacht kan daarbij worden aan de geestelijke verzorging in of ten behoeve van het leger, gevangenissen, ziekenhuizen of bejaardenoorden. Verwerking van gegevens betreffende godsdienst of levensovertuiging door deze instellingen is slechts toegestaan indien dit noodzakelijk is voor de geestelijke verzorging. Als aanvullende garantie is – evenals in het BGG – bepaald dat verwerking niet langer is toegestaan nadat de betrokkene op enig moment schriftelijk bezwaar heeft gemaakt.

Artikel 18

Verwerking van persoonsgegevens betreffende iemands ras dient slechts in zeer uitzonderlijke gevallen te worden toegestaan. In het verlengde van het huidige BGG wordt hiertoe in beginsel slechts de moeglijkheid gecreëerd indien het betreft de verwerking van gegevens omtrent ras voor identificatiedoeleinden dan wel in het kader van een voorkeursbeleid ten aanzien van bepaalde minderheidsgroeperingen. In beginsel is er alleen in die gevallen een zwaarwegend algemeen belang in de zin van artikel 8, vierde lid, van de richtlijn, dat verwerking van dergelijke gegevens kan rechtvaardigen.
In de toelichting bij artikel 16 is reeds ingegaan op de keuze voor het begrip «ras». Dit begrip heeft hier dezelfde betekenis als in artikel 1 van de Grondwet en moet mede in het licht worden gezien van het Internationaal Verdrag inzake de uitbanning van alle vormen van rassendiscriminatie[1].
Het begrip moet ruim worden opgevat en omvat ook huidskleur, afkomst en nationale of etnische afstamming. Daarmee worden de begrippen uit de richtlijn, waarin wordt gesproken over «raciale of etnische afkomst» afgedekt.
Het eerste lid voorziet in een ontheffing van het verbod om gegevens betreffende iemands ras te verwerken met het oog op de identificatie van de betrokken persoon. Een voorbeeld is de met foto's voorziene identiteitspasjes die door een werkgever aan zijn werknemers worden

[1] Trb. 1967, 48.

verstrekt. Omdat een kopie van dergelijke pasjes in de regel door de werkgever wordt bewaard in een kaartenbak die volgens meerdere criteria toegankelijk is of door de werkgever geautomatiseerd is opgeslagen, is doorgaans sprake van een verwerking van persoonsgegevens in de zin van de richtlijn. Aangezien van de foto op het pasje het ras van de werknemer kan worden afgeleid, valt de hier bedoelde verwerking tevens onder de reikwijdte van artikel 8 van de richtlijn. Een dergelijk pasje kan verstrekt worden met het oog op de identificatie van de betrokken persoon bij het betreden van het gebouw van de werkgever. Het belang van de werkgever kan met zich brengen dat invoering van een pasjes-systeem noodzakelijk is. Dit zal zich bijvoorbeeld kunnen voordoen bij grote werkgevers die veel werknemers in dienst hebben en waarbij identificatie bij het betreden van het terrein van de werkgever slechts deugdelijk kan plaatsvinden aan de hand van een van een foto voorzien identiteitsbewijs. Omdat het gaat om een gevoelig gegeven, stelt het eerste lid wel een harde eis. Verwerking van een rasgegeven is – afgezien van de grenzen die inherent zijn aan de elders in het wetsvoorstel geregelde algemene beginselen van gegevensverwerking – alleen dan geoorloofd als het met het oog op die identificatie onvermijdelijk is. Dit is een aanscherping van het in artikel 23, eerste lid, onder e opgenomen noodzakelijkheidscriterium; zij kan worden beschouwd als een passende waarborg in de zin van artikel 8, vierde lid, van de richtlijn.
In het tweede en derde lid zijn voorschriften gegeven voor het verwerken van rasgegevens in het kader van het voeren van een voorkeursbeleid voor bepaalde minderheidsgroeperingen. Het voorkeursbeleid als bedoeld in dit voorschrift moet voldoen aan de vereisten in artikel 2 van de Algemene wet gelijke behandeling. In deze wet is het verbod op het maken van onderscheid neergelegd. Het onderhavige artikel maakt het echter mogelijk om aan onder andere leden van etnische of culturele minderheidsgroeperingen een voorkeursbehandeling te geven indien daarmee wordt beoogd feitelijke ongelijkheden op te heffen of te verminderen. Het onderscheid moet dan in een redelijke verhouding staan tot dat doel. De grond van dit onderscheid is gelegen in de algemene achterstandspositie van deze groepen in het maatschappelijk leven. Dit is een zwaarwegend algemeen belang in de zin van artikel 8, vierde lid, van de richtlijn. Onder deze verwerkingsgrond valt ook de verwerking door scholen van gegevens omtrent herkomst en nationaliteit ter uitvoering van de zgn. «gewichtenregeling» in de Formatiebesluiten WBO. Een vergelijkbare regeling is neergelegd op grond van de ISOVSO en de WVO. Dergelijke regelingen zijn gericht op de verstrekking van extra financiële middelen ter bestrijding van onderwijsachterstanden van o.a. allochtone leerlingen. Hetzelfde geldt voor de in sommige onderwijssectoren bestaande faciliteitenregelingen welke gericht zijn op culturele minderheidsgroeperingen en anderstalige leerlingen.
In diezelfde bepaling wordt gesteld dat er echter wel passende waarborgen getroffen moeten zijn en verwerking van rasgegevens is daarom alleen geoorloofd als aan bepaalde voorwaarden is voldaan. De eerste voorwaarde is dat verwerking alleen is toegestaan voor zover deze noodzakelijk is voor het doel van de verwerking: in dit geval de verwezenlijking van het voorkeursbeleid. Deze voorwaarde vloeit eigenlijk al min of meer voort uit artikel 2 van de Algemene wet gelijke behandeling en aan deze voorwaarde dient steeds te worden getoetst. Zo is van belang dat het voorkeursbeleid uit zijn aard een tijdelijk karakter heeft: het beleid is slechts gerechtvaardigd zolang er nog sprake is van een bepaalde achterstandspositie van de desbetreffende minderheidsgroepering. Indien de positie van deze groepering het voeren van een voorkeursbeleid niet meer rechtvaardigt, zal het duidelijk zijn dat eveneens de grond aan de verwerking van rasgegevens is vervallen. Tevens kan zich het geval voordoen dat ten tijde van het toepassen van een voorkeursbeleid de maatschappelijke achterstand van deze groepering zodanig is veranderd

dat er aanleiding is het voorkeursbeleid aan te passen. Het proportionaliteitsbeginsel brengt dan met zich dat, indien in het kader van dit beleid gegevens omtrent ras worden verwerkt, deze verwerking eveneens moet worden heroverwogen.
In de tweede plaats moet de verwerking beperkt blijven tot gegevens omtrent iemands geboorteland, het geboorteland van diens ouders of van diens grootouders. Deze beperking is in overeenstemming met de Wet bevordering evenredige arbeidsdeelname allochtonen (WBEAA). Zij geldt ook thans al op grond van het BGG. Andere gegevens dan de hiervoor genoemde kunnen in het kader van een dergelijk voorkeursbeleid niet worden verwerkt. Zelfs de toestemming van de betrokkene kan dit verbod niet ongedaan maken. Artikel 18, tweede lid, is – mede gelet op de in deze bepaling gehanteerde terminologie – uitputtend bedoeld zodat voor de in artikel 23, eerste lid, onder a opgenomen toestemmingsgrond geen plaats meer is.
Als derde en laatste voorwaarde geldt dat verwerking van gegevens omtrent ras in het kader van voorkeursbeleid niet is toegestaan, indien de betrokkene daartegen schriftelijk bezwaar maakt. Het bezwaar hoeft niet te worden gemotiveerd en kan ten allen tijde worden ingediend. Na een dergelijk bezwaar zal de verantwoordelijke de verwerking terstond moeten beëindigen, ook al zouden deze ter zake dienend zijn met het oog op het doel waarvoor de gegevens worden verwerkt.
Buiten de reikwijdte van de regeling vallen de gegevens uit de verwerking waarvan niet zonder meer een gevoelig karakter kan worden afgeleid. Deze gegevens kunnen worden aangemerkt als indirect gevoelige gegevens. Er is in dergelijke gevallen sprake van hooguit een indicatie dat het gegeven een gevoelig karakter kan hebben. Indien een school bij voorbeeld met het oog op de identificatie van de leerlingen van hen allen de geboorteplaats in de administratie opneemt, vloeit uit deze verwerking, indien het gaat om de geboorteplaats in het buitenland, niet rechtstreeks een gevoelig gegeven voort. De verwerking heeft niet plaats gevonden met het doel om de mogelijk andere etnische herkomst van de leerlingen te registreren. Dit laat de mogelijkheid open dat dergelijke gegevens, mogelijk door vergelijking met andere gegevens, alsnog worden gebruikt om gegevens omtrent ras te herleiden. Onder omstandigheden zal dit toelaatbaar zijn, bij voorbeeld in geval van wetenschappelijk of statistisch onderzoek in het kader van het allochtonenbeleid. We komen hierop in de toelichting op artikel 23 terug.

Artikel 19

Deze bepaling bevat voorschriften die grenzen stellen aan de verwerking van persoonsgegevens door instellingen op politiek terrein. Zij is nagenoeg gelijk aan artikel 5 BGG. Het eerste lid, onder a, is een implementatie van artikel 8, eerste lid, onder d, van de richtlijn. Daarbij valt in de.eerste plaats te denken aan politieke partijen en de wetenschappelijke bureaus en vormingsorganisaties die daarmee verbonden zijn. Volgens de richtlijn mag een dergelijke instelling slechts gegevens verwerken van personen die lid zijn van deze instelling, of van personen waarmee de instelling in verband met haar doelstelling regelmatige contacten onderhoudt. De kring van personen die in het eerste lid onder a, wordt omschreven, wordt geacht aan deze voorwaarde te voldoen. Werknemers en «andere tot de instelling behorende personen» moeten worden gerekend tot degenen met wie de instelling regelmatige contacten onderhoudt.
Concreet zal het bij de toepassing van deze bepaling gaan om de ledenadministraties van politieke partijen, de administraties die worden aangehouden van de personen die in dienst zijn van een politieke partij en de administraties van andere personen die gerekend kunnen worden tot een instelling op politieke grondslag. Onder het voorschrift vallen ook de

verwerkingen van gegevens omtrent personen die betrokken zijn bij wetenschappelijke bureaus van politieke partijen, ledenregistraties van vormingsorganisaties van politieke partijen en registraties van bijvoorbeeld personen die nauw bij de organisatie van de partij zijn betrokken of zich als belangstellende bij de partij hebben kenbaar gemaakt.
De bepaling sluit aan bij artikel 5, tweede lid, onder b van de Algemene wet gelijke behandeling. Van belang is dat de verwerking van gegevens beperkt moet blijven tot hetgeen noodzakelijk is voor de verwezenlijking van de grondslag van de instelling. Indien niet meer aan deze voorwaarde wordt voldaan, moet de verwerking terstond worden beëindigd, tenzij de gegevens nodig blijven voor de afhandeling van een geschil. Artikel 23, eerste lid, biedt, in het verlengde van artikel 8, tweede lid, onder e van de richtlijn, hiertoe de ruimte. Voorts geldt krachtens het tweede lid dat de desbetreffende persoonsgegevens niet aan derden verstrekt mogen worden zonder toestemming van de betrokkene.
Voor verwerkingen van gegevens omtrent iemands van politieke gezindheid in verband met benoemingen in bepaalde openbare functies kan een beroep worden gedaan op het bepaalde onder b van dit artikel. Deze bepaling is gebaseerd op artikel 8, vierde lid, van de richtlijn. Het kan daarbij gaan om benoemingen bij bestuursorganen of adviesorganen. Dergelijke gegevens spelen bijvoorbeeld een belangrijke rol bij burgermeestersbenoemingen. Het is evident dat bij bepaalde openbare functies gegevens omtrent politieke gezindheid relevant kunnen zijn in het kader van de beoordeling van iemands geschiktheid. Verwerking van die gegevens dient een zwaarwegend algemeen belang. Wel geldt uiteraard als voorwaarde dat er voor de desbetreffende functie ook daadwerkelijk eisen met betrekking tot politieke gezindheid mogen worden gesteld. Alleen dan is verwerking van daarop betrekking hebbende gegevens toegestaan. Een en ander is tot uitdrukking gebracht in het eerste lid onder b. Zie voorts artikel 5, vierde lid van de Algemene wet gelijke behandeling. Voorts blijven – zoals hiervoor al in algemene zin opgemerkt – de algemene beginselen van gegevensverwerking in dit wetsvoorstel onverkort van toepassing.

Artikel 20

Anders dan in de WPR wordt in de richtlijn het aangesloten zijn bij een vakbond als gevoelig gegeven aangemerkt. In artikel 20 van de WBP wordt dit in navolging van de richtlijn ook zo aangemerkt. Evenals artikel 17 en 19 vormt het een artikel een implementatie van artikel 8, tweede lid, onder d.
Wat de gevoeligheid van het gegeven betreft is het lidmaatschap van een vakbond tot op zekere hoogte vergelijkbaar met het lidmaatschap van een politieke partij en in de richtlijn worden deze gegevens dan ook op één lijn geplaatst. Om die reden is zo veel mogelijk aangesloten bij de formulering van artikel 19. Evenals in artikel 19, eerste lid, onder a, is de eis gesteld dat het verbod om dergelijke gegevens te verwerken alleen dan niet van toepassing is als dit gelet op de doelstelling van de desbetreffende instelling noodzakelijk is. Tevens is in het tweede lid bepaald dat persoonsgegevens betreffende het lidmaatschap van een vakbond niet aan derden mogen worden verstrekt.
Anderzijds zijn er ook verschillen. Anders dan bij een politieke partij of een kerkgenootschap kan niet zonder meer gesproken worden over de «grondslag» van een vakbond. Weliswaar komt het vaak voor dat een vakbond gelieerd is aan een politieke, godsdienstige of levensbeschouwelijke stroming, maar een noodzakelijke voorwaarde is dit geenszins. Bovendien verschilt de relatie die de vakbond onderhoudt met de verwante stroming sterk van geval tot geval. Soms zijn de banden geformaliseerd in statuten of andere officiële stukken, in andere gevallen echter zijn er slechts contacten van feitelijke aard. In afwijking van artikel

19 (en ook artikel 17 eerste lid, onder b) wordt daarom niet bepaald dat de gegevensverwerking noodzakelijk moet zijn voor de verwezenlijking van de «grondslag» van de vakbond of vakcentrale. Het noodzakelijkheidsvereiste is hier louter gekoppeld aan de doelstelling van de desbetreffende organisatie.
In artikel 8, eerste lid, van de richtlijn wordt gesproken over «gegevens waaruit het aangesloten zijn bij een vakvereniging blijkt». In artikel 20 is dit beschreven als «persoonsgegevens betreffende iemands lidmaatschap van een vakbond». Gelet op tekst van de richtlijn gaat het daarbij niet alleen om gegevens die direct betrekking hebben op het lidmaatschap zèlf, maar ook om gegevens waaruit kan worden afgeleid dat iemand lid is van een vakbond. Als voorbeeld kan worden genoemd de administratie van een vakbond waarin alle namen en adressen van de leden zijn opgenomen. Strikt genomen verschaffen deze gegevens op zichzelf geen informatie omtrent het lidmaatschap van een vakbond, maar uit het feit dat de namen en adressen hierin zijn opgenomen kan lidmaatschap geconcludeerd worden. Overigens geldt dat thans ook al voor andere gevoelige gegevens op grond van het BGG.
In artikel 8, tweede lid, onder d van de richtlijn wordt in algemene zin gesproken over «een stichting, een vereniging of enige andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is». Voor Nederland geldt dat, wat betreft het vakbondsgebied, dit gepreciseerd kan worden. De hier bedoelde gegevens moeten verwerkt kunnen worden door de vakbond waarvan de betrokkene lid is, alsmede de organisatie waarvan de bond mogelijk deel uitmaakt. In Nederland is het gebruikelijk dat een vakbond is opgenomen in een vakcentrale. Om die reden wordt ook dat begrip in het onderhavige artikel gehanteerd. Overigens geldt evenals bij de bepaling inzake politieke gezindheid dat gegevensverwerking buiten het geval bedoeld in de onderhavige bepaling ook mogelijk is op grond van artikel 23, eerste lid. Dit betekent dat verwerking van vakbondsgegevens bijvoorbeeld ook mogelijk is indien betrokkene daarvoor uitdrukkelijk toestemming geeft. Verwezen zij naar de toelichting op die bepaling.

Artikel 21

Dit artikel vormt de gedeeltelijke implementatie van artikel 8, derde lid, van de richtlijn. Het verwerken van medische gegevens wordt ook elders geregeld. Bijzonder van belang zijn de artikelen 7:446 e.v. BW, waarin bepalingen voorkomen omtrent de omgang van persoonsgegevens in het kader van de geneeskundige behandelingsovereenkomst. Voorts kan gewezen op de relevante artikelen uit de Wet bijzondere opneming in psychiatrische ziekenhuizen (Wet BOPZ). De bepalingen in het BW en de Wet BOPZ zijn in overeenstemming met de richtlijn. Wat de verhouding tussen deze bepalingen en het onderhavige wetsvoorstel betreft, wordt geen wijziging beoogd ten opzichte van de huidige situatie. Het BW en de Wet BOPZ vormen derhalve geen lex specialis ten opzichte van het thans voorgestelde artikel 21 WBP. De diverse bepalingen vullen elkaar wederzijds aan. In bepaalde gevallen zullen zowel de WBP als het BW of de Wet BOPZ van toepassing zijn. Voor een uiteenzetting over de verhouding tussen de WBP en de bijzondere wetgeving wordt verwezen naar par. 5 van het algemeen deel van de toelichting.
Voorts heeft de Registratiekamer er terecht op gewezen dat het onderhavige artikel steeds in samenhang moet worden bezien met het medische beroepsgeheim. Het kan zich voordoen dat in een geval waarin het verbod om medische gegevens te verwerken op grond van artikel 21 niet van toepassing is, het medische beroepsgeheim niettemin aan de gegevensverwerking in de weg kan staan. In dit verband zij verwezen naar artikel 9, derde lid, dat – als onderdeel van de algemene beginselen van

het wetsvoorstel – onverkort van toepassing is op de verwerking van gezondheidsgegevens.
In het artikel wordt de aanduiding «persoonsgegevens omtrent iemands gezondheid» gebruikt. Deze aanduiding verschilt – zoals reeds bij artikel 16 is toegelicht – in een aantal opzichten van «persoonsgegevens van medische of psychologische aard», waarmee in het BGG medische gegevens worden aangeduid. Psychologische gegevens vallen daar niet zonder meer onder. Het begrip «gezondheid» moet niettemin ruim worden opgevat; het omvat niet alleen de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts worden verwerkt, maar alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen. Niet alleen indien een bedrijfsarts vaststelt dat een werknemer lijdt aan een psychosomatisch probleem is er sprake van een «gegeven betreffende iemands gezondheid», dit is ook het geval indien een chef van een werknemer constateert dat de werknemer lichamelijk gehandicapt is. Ondanks het feit dat een dergelijk gegeven voor een ieder kenbaar is, mag een werkgever dit gegeven – afgezien van de situatie die valt onder het eerste lid, onder e – niet verwerken, tenzij hij daarvoor de uitdrukkelijke toestemming van de betrokkene heeft verkregen. Voorts is ook het enkele gegeven dat iemand ziek is een gegeven omtrent gezondheid, hoewel dat gegeven op zichzelf nog niets zegt over de aard van de aandoening.
Naast de implementatie van 8 van de richtlijn vormt artikel 21 een gedeeltelijke voortzetting van artikel 5 BGG. Anders dan laatstgenoemde bepaling vormt artikel 21 evenwel geen ontheffing voor verwerking van persoonsgegevens betreffende het seksuele leven. Voor zover dergelijke gegevens niet tevens de gezondheid van personen betreffen, achten wij de noodzaak van een afzonderlijke ontheffingsbasis voor verwerking van deze categorie gegevens in dit artikel niet noodzakelijk. Zoals de Registratiekamer terecht opmerkt zal ontheffing inzake verwerking van gegevens betreffende het seksuele leven dus alleen op de voet van artikel 23 kunnen plaatsvinden.
In artikel 21 wordt de verwerking van gegevens omtrent gezondheid niet uitputtend geregeld. Specifieke regelgeving kan daaraan nadere invulling geven. Ontheffing van het verbod om gezondheidsgegevens te verwerken anders dan in de gevallen als bedoeld in het eerste lid kan ook geschieden op grond van artikel 23, eerste lid, mits aan één of meer van de daarin opgenomen criteria is voldaan. Indien de verwerking geen zwaarwegend algemeen belang dient in de zin van laatstgenoemd artikel, is in de regel de uitdrukkelijke toestemming van de betrokkene vereist. In de contractuele sfeer zal dit laatste het geval zijn, mits voldaan is aan de stringente voorwaarden die artikel 1, onderdeel h, in verband met artikel 23, eerste lid, onderdeel a, aan de toestemming worden gesteld. Aangezien bij overeenkomsten niet altijd aan dergelijke vergaande toestemmingsvoorwaarden kan worden voldaan, bestaat de noodzaak om in het onderhavige artikel een aantal afzonderlijke voorzieningen te treffen.

Eerste lid

Onderdeel a

Deze bepaling heeft in het verlengde van artikel 5 BGG betrekking op de verwerking van gegevens door «hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening». Dit betekent dat op grond van dit onderdeel – binnen de grenzen van de algemene beginselen van gegevensverwerking – niet alleen gegevens omtrent gezondheid mogen worden verwerkt door ziekenhuizen en andere medische instellingen, maar ook door instanties op het terrein van de maatschappelijke dienstverlening voor zover dat voor de in onderdeel a aangegeven doelstellingen noodzakelijk zijn. Te denken valt aan

bejaardenoorden en instanties voor jeugdhulpverlening. Voorts staat onderdeel a toe dat individuele hulpverleners voor zover zij niet bij voornoemde instellingen werkzaam zijn, maar bijvoorbeeld een zelfstandige praktijk uitoefenen, gezondheidsgegevens verwerken.
In de richtlijn wordt een lange opsomming gegeven van activiteiten binnen de gezondheidszorg waarbij verwerking van gegevens omtrent gezondheid in beginsel mogelijk is. In artikel 21, onder a van het eerste lid is voor een eenvoudiger vorm gekozen, namelijk dat het verbod op gegevensverwerking niet van toepassing is wanneer een goede behandeling van de betrokkene dit noodzakelijk maakt of wanneer het voor het beheer van de desbetreffende instelling of voorziening noodzakelijk is. Daarmee worden alle activiteiten die in artikel 8, derde lid, van de richtlijn genoemd gedekt. Tevens wordt daarmee aangesloten bij de diverse functies van gegevensverwerking die, afgezien van wetenschappelijk onderzoek, meestal binnen de gezondheidszorg worden onderscheiden. Het begrip «beheer» dient in onderdeel a beperkt te worden uitgelegd. In de eerste plaats kan het gaan om het waarborgen van de kwaliteit van de verleende zorg. Naast de verwerking van gegevens omtrent gezondheid voor de behandeling sec kan het onder omstandigheden noodzakelijk zijn dat dergelijke gegevens worden verwerkt ten behoeve van de intercollegiale toetsing door hulpverleners onderling. Deze toetsing valt onder de noemer «kwaliteitsbeheer». Daarnaast moeten verwerkingen die rechtstreeks verband houden met de betaling van rekeningen voor medische behandeling tot het «beheer» in de zin van het eerste lid worden gerekend. Dit laatste geldt zowel voor een instelling als bijvoorbeeld een ziekenhuis als een beroepspraktijk van een individuele hulpverlener. Voor andere beheersdoeleinden kan in beginsel worden volstaan met het gebruik van gegevens omtrent personen die niet geidentificeerd of identificeerbaar zijn. Verwerking van gegevens omtrent gezondheid is dan niet noodzakelijk en derhalve op grond van artikel 21, eerste lid, niet toegestaan.
Afgezien van de veel voorkomende gegevensverwerking binnen de gezondheidszorg is in het eerste lid een aantal specifieke situaties geregeld waarin van het verbod om gezondheidsgegevens te verwerken is afgeweken. In onderdeel b van het eerste lid is een uitdrukkelijke ontheffingsgrondslag opgenomen voor bepaalde verwerkingen door verzekeringsinstellingen. Hoewel de relatie tussen verzekerden en verzekeringsinstellingen doorgaans vorm krijgen in de contractuele sfeer, kan in veel gevallen – mede gelet op de strenge eisen die in het onderhavige wetsvoorstel op dit punt worden gesteld – niet steeds van een op een gegevensverwerking gerichte, uitdrukkelijke toestemming van de betrokkene worden uitgegaan. De Registratiekamer heeft daar terecht op gewezen. Derhalve zal dan ook in veel gevallen de verwerking van gegevens omtrent gezondheid door verzekeringsinstellingen niet of althans niet automatisch op artikel 23, eerste lid, onderdeel a, gebaseerd kunnen worden. Ten einde hoe dan ook elke twijfel uit te sluiten verdient het de voorkeur om in artikel 21 een expliciete ontheffingsgrondslag voor bedoelde verwerkingen te creëren.

Onderdeel b

Bij verwerking van gegevens omtrent gezondheid door verzekeraars dient onderscheid te worden gemaakt tussen verschillende situaties. Om te beginnen is er uiteraard het geval waarin iemand een aanvraag invult voor het verkrijgen van een bepaalde verzekering en in dat kader gegevens omtrent gezondheid verstrekt. Deze gegevens zijn nodig ter beoordeling van het door de verzekeraar te verzekeren risico. Een ontheffing van het verbod om de aldus vergaarde gegevens voor dat doel te verwerken vindt zijn grondslag in de eerste categorie van onderdeel b. Om evenwel te voorkomen dat verzekeraars buiten de betrokkene om

gegevens met het oog op dit doel uit andere bron verzamelt en verwerkt, dient de aspirant-verzekerde voorafgaand aan de afsluiting van de overeenkomst de gelegenheid te worden geboden om tegen een zodanige verwerking bezwaar te maken. Uit artikel 33, derde lid, van het wetsvoorstel volgt dat indien de verzekeraar van de geschetste mogelijkheid gebruik zou willen maken, de verzekerde op het aanvraagformulier moet worden gewezen op de mogelijkheid van bezwaar. Een actieve handeling van verzekeraarszijde is in dit geval nodig om een behoorlijke en zorgvuldige verwerking te waarborgen. Vervolgens moet betrokkene op het aanvraagformulier van een eventueel bezwaar zijnerzijds mededeling kunnen doen. Aldus is ook – conform artikel 8, vierde lid, van de richtlijn – sprake van een passende waarborg. Het aantekenen van bezwaar kan uiteraard tot gevolg hebben dat de verzekeraar afziet van het sluiten van de overeenkomst indien naar zijn opvatting onvoldoende gegevens beschikbaar zijn om het risico adequaat te beoordelen.
Vervolgens kunnen zich bij de uitvoering van de verzekeringsovereenkomst diverse situaties voordoen waarin verzekeraars gezondheidsgegevens verwerken. Naar aanleiding van het advies van de Registratiekamer geven wij er de voorkeur aan deze gevallen onder te brengen onder de algemene norm dat de verwerking van gegevens omtrent gezondheid geoorloofd is voor zover zulks met het oog op dat doel noodzakelijk is. De norm is opgenomen als tweede categorie van onderdeel b. Deze norm zal toepassing moeten vinden tijdens de gehele periode die volgt op de totstandkoming van de overeenkomst. De Registratiekamer heeft er voorts terecht op gewezen dat – zoals hiervoor al is vermeld – naast deze algemene norm de algemene beginselen zoals vastgelegd in artikel 6 e.v. van toepassing blijven. De toepassing van artikel 21 zal steeds in samenhang met deze beginselen moeten worden bezien.
Onder omstandigheden kan de uitvoering van de overeenkomst meebrengen dat verzekeraars gezondheidsgegevens van derden – dat wil zeggen anderen dan de verzekerde – dienen te verwerken. Een dergelijke verwerking kan zijn rechtvaardiging vinden in het algemene, in het verzekeringsrecht geldende beginsel dat een verzekerde verplicht is al het mogelijke te doen om schade te voorkomen of te verminderen. Dit beginsel is neergelegd in artikel 283 van het Wetboek van Koophandel. Op grond van dit beginsel is de verzekerde onder omstandigheden gehouden gegevens over een derde aan de verzekeraar te verstrekken die ertoe kunnen bijdragen om een door of namens die derde ingediende claim op adequate wijze te kunnen afhandelen. Wel geldt uiteraard ook hier dat niet meer gegevens worden verwerkt dan noodzakelijk is voor de uitvoering van de overeenkomst.
Voorts is de verzekeraar in dit geval niet bevoegd om de betreffende gegevens langs andere weg te verkrijgen dan via de verzekerde op wie de schadebeperkingsplicht rust.
Ook met betrekking tot de in onderdeel b geregelde gevallen geldt dat artikel 21 geen onbeperkte legitimatie voor gegevensverwerking vormt. De bepaling is in eerste instantie gericht op doorbreking van het verwerkingsverbod van artikel 16. Indien een verwerking in deze termen valt, dient vervolgens aan de hand van de algemene beginselen van gegevensverwerking zoals geregeld in artikel 6 e.v., te worden beoordeeld of de betreffende gegevensverwerking rechtmatig is. Voorts sluit artikel 21 niet uit dat in bijzondere wetgeving of zelfregulering een nadere precisering wordt gegeven van de algemene norm die in de WBP voor verzekeringsrelaties wordt gesteld.

Onderdeel c

In dit onderdeel wordt voor scholen op beperkte schaal een uitzondering

gecreëerd om gegevens omtrent gezondheid te verwerken. In de huidige situatie betreft dit conform artikel 5, tweede lid, BGG alleen scholen waarop de Interimwet op het speciaal onderwijs en het voortgezet speciaal onderwijs (ISOVSO) – binnenkort te vervangen door de Wet op de expertisecentra en de Wet op het primaire onderwijs – van toepassing is. Het betreft hier onderwijs aan leerlingen die vanwege fysieke of psychische oorzaken leerproblemen hebben en uit dien hoofde speciale begeleiding behoeven. Om aan deze doelstelling te kunnen voldoen moeten de scholen gezondheidsgegevens kunnen vastleggen. Na de inwerkingtreding van het BGG is het overheidsbeleid er op gericht om leerlingen die vanwege psychische of fysieke oorzaken met een leerachterstand kampen niet of althans niet zonder meer op een ISOVSO-school te plaatsen, maar door middel van speciale begeleiding in het reguliere (basis)onderwijs te houden. Als gevolg van deze beleids-wijziging dient de mogelijkheid om gezondheidsgegevens te verwerken te worden verruimd tot alle scholen in het primaire onderwijs. Voorts bestaan er in het onderwijs faciliteiten- en bekostigingsregelingen voor gehandicapte leerlingen die onder omstandigheden eveneens nopen tot verwerking van gegevens inzake gezondheid. Deze regelingen strekken zich ook uit tot het voortgezet onderwijs.
De te onderscheiden gevallen vinden allen hun basis in onderdeel c: de speciale begeleiding van leerlingen en het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand worden in dit onderdeel als geoorloofde verwerkingsdoelen naast elkaar genoemd. De noodzakelijkheidseis brengt met zich dat alleen gezondheidsgegevens mogen worden verwerkt van leerlingen die in verband met hun gezond-heidstoestand voor de hier bedoelde speciale begeleiding of bijzondere voorziening in aanmerking komen. Verwerking van gezondheidsgegevens van andere leerlingen is niet toegestaan. Voorts mag verwerking alleen plaatsvinden voor zover dat voor dat doel noodzakelijk is. Dit stelt niet alleen grenzen aan de aard en omvang van de gegevens die mogen worden verwerkt, maar ook aan de kring van personen die binnen een school van deze gegevens kennis mogen nemen. In dat verband zal worden aangesloten bij de werkwijze die thans op grond van artikel 33 ISOVSO wordt gevolgd. Deze houdt in dat de verwerking van gezondheidsgegevens in beginsel is voorbehouden aan de leden van een Commissie van onderzoek, die krachtens de zojuist genoemde bepaling onder meer is belast met de beoordeling in hoeverre leerlingen voor speciale begeleiding in aanmerking komen. Van deze commissie maken behalve de directeur van de school diverse deskundigen deel uit, zoals bijvoorbeeld een arts en een psycholoog of pedagoog.

Onderdeel d

Dit onderdeel bepaalt dat het verbod om gezondheidsgegevens te verwerken niet van toepassing indien de verwerking geschiedt door de Minister van Justitie voor zover dat noodzakelijk is in verband met de tenuitvoerlegging van vrijheidsstraffen of vrijheidsbenemende maatre-gelen. In het gevangeniswezen is in tal van situaties verwerking van gegevens omtrent gezondheid noodzakelijk. Afgezien van verwerking ten behoeve van een adequate medische behandeling en verzorging – welke onder omstandigheden ook hun grondslag kunnen vinden in onderdeel a – kunnen gezondheidsgegevens van belang zijn voor de bejegening van de gedetineerde door het gevangenispersoneel alsook voor de verstrekking van een eventueel dieet. Voorts kunnen gegevens omtrent gezondheid relevant zijn voor de wijze waarop gedetineerden moeten worden vervoerd. Ook bij het nemen van beperkende maatregelen – bijvoorbeeld het onder dwang toepassen van een geneeskundige handeling – ter afwending van ernstig gevaar voor de gezondheid of de veiligheid van de gedetineerde of van anderen, is het noodzakelijk

gezondheidsgegevens te verwerken. Al deze verwerkingen vinden doorgaans plaats binnen penitentiaire inrichtingen, TBS-inrichtingen en justitiële jeugdinrichtingen onder de verantwoordelijkheid van de Minister van Justitie. Voorts valt te denken aan gegevensverwerking in het kader van de tenuitvoerlegging van de vreemdelingenbewaring.

Onderdeel e

Dit onderdeel omvat de verwerking van gegevens omtrent gezondheid in de sfeer van de sociale zekerheid. Er bestaat hier een nauwe samenhang met wetswijzigingen die kort geleden op het terrein van de sociale zekerheid tot stand zijn gekomen. Een onderdeel hiervan betreft de grotere verantwoordelijkheid van de werkgever in het geval van ziekte en arbeidsongeschiktheid van zijn werknemers. Tot voor kort lag deze nagenoeg volledig in handen van overheidsinstellingen. In dat kader had de werknemer een aantal in de wet vastgelegde controle-, informatie- en medewerkingsverplichtingen. Recente wijzigingen van de Ziektewet hebben in deze situatie belangrijke veranderingen teweeg gebracht. Op 1 januari 1994 is de Wet terugdringing ziekteverzuim (Stb. 1993, 750) in werking getreden. Op grond van deze wet zijn werkgevers in de meeste gevallen verplicht gedurende de eerste zes weken van arbeidsongeschiktheid 70% van het loon door te betalen. Vanaf 1 maart 1996 is deze periode uitgebreid tot een jaar als gevolg van de Wet uitbreiding loondoorbetalingsplicht bij ziekte (Stb. 1996, 134). Voor een beperkt aantal categorieën van werknemers blijft de Ziektewet gewoon van toepassing en blijft het betreffende bestuursorgaan de bevoegde instantie.
De recente wetswijzigingen hebben de vraag doen rijzen op welke wijze de persoonlijke levenssfeer van de werknemer jegens de werkgever moet worden gewaarborgd. De relatie tussen werkgever en werknemer behoeft in dit opzicht bijzondere aandacht. Voorkomen moet worden dat – gelet op de afhankelijkheidssituatie waarin de werknemer zich doorgaans ten opzichte van de werkgever bevindt – gezondheidsgegevens worden verwerkt op een wijze die de persoonlijke levenssfeer van de werknemer aantast. Als algemene richtsnoer is daarom allereerst geformuleerd dat de werknemer niet meer gegevens behoeft te verschaffen aan zijn werkgever dan deze nodig heeft om vast te stellen of de werknemer recht op de loondoorbetaling heeft. Deze brengt bijvoorbeeld met zich dat in het geval de werknemer zich ziek meldt, hij zijn werkgever de aard en de oorzaak van de ziekte niet behoeft mede te delen. Voor de loondoorbetalingsverplichting is de laatste vraag niet van belang en de werknemer moet daarom met het oog op de bescherming van zijn persoonlijke levenssfeer een antwoord op die vraag zonder gevolgen schuldig kunnen blijven.
Voorts zal de bedrijfsarts die de werkgever ondersteunt bij de reïntegratie en begeleiding van de zieke werknemer de gegevens omtrent de aard van de ziekte die hij in deze hoedanigheid verkrijgt, niet aan de werkgever mogen doorgeven. Een belangrijke ontwikkeling in de recente wetgeving is tenslotte dat de betrokken bestuursorganen en werkgevers bevoegd zijn om de uitvoering van regelingen inzake arbeidsongeschiktheid uit te besteden aan derden.
Met de geschetste ontwikkelingen is bij de formulering van onderdeel e rekening gehouden. In dit onderdeel wordt een tweetal categorieën van situaties geregeld. In de eerste plaats betreft het verwerkingen die noodzakelijk zijn met het oog op de uitvoering van regelingen die samenhangen met de gezondheidstoestand van de werknemer of de uitkeringsgerechtigde. Daarbij gaat het onder meer om uitkeringen in verband met arbeidsongeschiktheid. Om te kunnen bepalen of en gedurende welke periode iemand in aanmerking komt voor een uitkering kan het nodig zijn dat degene die de uitkering verstrekt, zich op de hoogte stelt van gegevens die betrekking hebben op de gezondheid van de betrokkene. Daarnaast bestaan er in de sociale zekerheidswetgeving

materiële voorzieningen of verstrekkingen die samenhangen met de gezondheidstoestand waarin de betrokkene zich bevindt, zoals bijvoorbeeld het aanbrengen van specifieke voorzieningen in woningen in verband met een lichamelijke handicap. Om precies te kunnen beoordelen welke voorziening in een specifiek geval noodzakelijk is, is eveneens een medische beoordeling noodzakelijk. Al deze regelingen zijn ondergebracht onder de algemene noemer van «aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene».
De tweede categorie van onderdeel e omvat de gegevensverwerking die noodzakelijk is met het oog op de reïntegratie of begeleiding van de werknemer of de uitkeringsgerechtigde. Deze laatste formulering bevat twee elementen. Allereerst kan het gaan om begeleiding van werknemers teneinde te voorkomen dat ten gevolge van het werk schade aan de gezondheid optreedt. Om met het gezondheidsbelang van de individuele werknemer – dat geregeld is in de Arbeidsomstandighedenwet – rekening te kunnen houden, dienen in voorkomende gevallen gegevens omtrent gezondheid te worden verwerkt. Daarnaast kan het gaan om het terugbrengen van werknemers in het arbeidsproces indien eenmaal arbeidsongeschiktheid is opgetreden, bijvoorbeeld door het treffen van een op een handicap afgestemde werkvoorziening. Ook met het oog op dat doel – aangeduid als «reïntegratie»- kan verwerking van gezondheidsgegevens nodig zijn.
Benadrukt dient te worden dat ook in dit onderdeel de verwerking van gegevens begrensd wordt door de noodzakelijkheidseis. Deze eis brengt met zich dat in bepaalde situaties slechts een beperkt aantal gezondheidsgegevens verwerkt mogen worden. Een duidelijk voorbeeld hiervan betreft de recente, zojuist besproken arbeidsongeschiktheidswetgeving. In dit kader betekent dit dat gegevens over de medische achtergronden van de arbeidsongeschiktheid niet door de werkgever mogen worden verwerkt. Werkgevers mogen enkel gegevens verwerken omtrent het feit dat en de mate waarin iemand arbeidsongeschikt is, alsmede de periode van arbeidsongeschiktheid. Het vierde lid opent de mogelijkheid om de nadere invulling van de noodzakelijkheidseis te verankeren in een algemene maatregel van bestuur.

Tweede lid

Een belangrijke waarborg is dat de persoonsgegevens in situaties als bedoeld in het eerste lid alleen mogen worden verwerkt door personen die uit hoofde van hun beroep of krachtens overeenkomst tot geheimhouding zijn verplicht. Voor een deel de van onder artikel 21 vallende situaties vloeit deze voorwaarde voort uit artikel 8, derde lid, van de richtlijn. Daarin wordt bepaald dat gezondheidsgegevens in de in dat lid geregelde gevallen alleen mogen worden verwerkt door personen die onderworpen zijn aan het krachtens nationale wetgeving geldende beroepsgeheim dan wel personen voor wie een gelijkwaardige geheimhoudingsplicht geldt. Het begrip «gelijkwaardige geheimhoudingsplicht» is in het tweede lid gepreciseerd. In de eerste plaats is conform artikel 2:5 Awb rekening gehouden met situaties waarin de geheimhoudingsplicht ook uit ambt of wettelijk voorschrift kan voortvloeien. Daarnaast kan ingevolge de bepaling sprake zijn van een verplichting die in privaatrechtelijke zin is overeengekomen. Voor kleine zelfstandigen met eigen personeel geldt ingevolge de tweede volzin een zelfstandige geheimhoudingsplicht. De omvang ervan wordt bepaald door de verplichtingen die ingevolge de wet op een werkgever rusten.

Voor de gevallen die niet vallen onder artikel 8, derde lid, maar onder artikel 8, vierde lid, van de richtlijn geldt dezelfde verplichting. In die situaties geldt de geheimhoudingsplicht als een «passende waarborg» in de zin van laatstgenoemde bepaling. De in dit lid opgenomen verplichting

sluit weer niet uit dat in bijzondere wetgeving een verdere aanscherping plaatsvindt. Denkbaar is dat voor specifieke situaties wordt voorgeschreven dat slechts een aan het beroepsgeheim gebonden arts bevoegd is tot gegevensverwerking.

Derde lid

Het derde lid betreft de specifieke situatie waarin in het belang van een goede geneeskundige behandeling en verzorging van patiënten in aanvulling op gezondheidsgegevens in strikte zin andere gevoelige persoonsgegevens moeten worden verwerkt. Gegevens als godsdienst of levensovertuiging kunnen in bijzondere gevallen van essentiële betekenis zijn bij de onderkenning van bijvoorbeeld bepaalde psychiatrische ziektebeelden en kunnen directe invloed hebben op het behandelingsplan van een patiënt. Ook het gegeven ras kan soms een belangrijke determinant zijn bij de diagnosestelling. Voorts kunnen ook gegevens omtrent het seksuele leven in een bepaalde context als medisch relevante gegevens worden aangemerkt. Als uit de verwerking van een gegeven rechtstreeks en dwingend voortvloeit dat het gegeven als gevolg van bijkomende omstandigheden een medisch karakter heeft, kan het noodzakelijk zijn deze gegevens met het oog op een goede geneeskundige behandeling vast te leggen. Dit geldt evenzeer voor gegevens die op zichzelf al als een gevoelig gegeven kunnen worden beschouwd, zoals etnische afkomst. Stelt bijvoorbeeld een arts tijdens een medische behandeling van een persoon vast dat zijn psychische problemen in een grote mate worden benvloed door zijn etnische afkomst, dan zal dit gegeven mede bij de behandeling van die persoon mede in aanmerking moeten worden genomen. Er dient dan wel een duidelijk verband te bestaan tussen de etniciteit en de psychische problemen. Is dat verband er niet dan kunnen dergelijke gegevens niet voor dat doel worden verwerkt.
Het derde lid biedt een opheffing van het verbod voor de verwerking van andere gevoelige persoonsgegevens als bedoeld in artikel 16 in de hierboven bedoelde specifieke situatie. De bepaling blijft strikt beperkt tot de verwerking door hulpverleners, instellingen of voorzieningen van gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene noodzakelijk is. Daartoe wordt in de bepaling verwezen naar het eerste lid, onder a. De bedoelde mogelijkheid bestond ook reeds onder het regime van het bestaande Besluit gevoelige gegevens. In de toelichting bij dit besluit werden de bedoelde gegevens omtrent ras, godsdienst of levensovertuiging, seksuele leven etc. als medische gegevens in ruime zin aangemerkt. Thans verdient het de voorkeur voor het gebruik van dergelijke gegevens in een medische context een uitdrukkelijke wettelijke basis te creëren.

Vierde lid

Een bijzondere bepaling betreft het vierde lid inzake erfelijkheidsgegevens. Een essentieel verschil tussen deze en andere gegevens is dat zij niet uitsluitend betrekking hebben op de gezondheidstoestand van de individuele persoon van wie zij in eerste instantie afkomstig zijn, maar ook op diens familieleden. Erfelijkheidsgegevens hebben per definitie tevens betrekking op anderen. De bepaling bevat geen allesomvattende regeling, doch regelt alleen een specifiek aspect van het gebruik van erfelijkheidsgegevens. Het schrijft voor dat de verwerking van persoonsgegevens betreffende erfelijke eigenschappen in beginsel alleen dan is toegestaan voor zover de verwerking plaatsvindt met betrekking tot de betrokkene bij wie de betreffende gegevens zijn verkregen. Specifieke wetgeving, zoals bijvoorbeeld de Wet medische keuringen, geven hieraan nadere invulling

in die zin dat zij – in het voetspoor van artikel 12 van het Verdrag inzake mensenrechten en geneeskunde van de Raad van Europa – de voorwaarden regelen waaronder bij betrokkenen erfelijke gegevens kunnen worden vergaard.
De bepaling heeft vooral tot doel de gelijkheid van iedere burger tot op zekere hoogte te waarborgen, en geeft daarmee invulling aan het fundamentele recht als omschreven in artikel 1 van de Grondwet (non-discriminatie). Voor zover genetische gegevens een rol spelen bij de behandeling van burgers in het maatschappelijk leven, dient deze omtrent hemzelf, verplicht of vrijwillig, te zijn verkregen. Een burger kan niet anders worden behandeld omdat omtrent hem gegevens kunnen worden herleid uit genetische gegevens van anderen in dezelfde genetische lijn. Het gelijkheidsbeginsel werkt daarom ook door ten aanzien van bij voorbeeld opgeslagen DNA-gegevens. Deze kunnen op grond van deze bepaling alleen worden gebruikt met betrekking tot de betrokkene zelf en niet tot anderen in dezelfde genetische lijn (zie ook het Reglement DNA-profielregistratie Gerechtelijk Laboratorium, Stcrt 1994, 96, van 25 mei 1994). Een en ander impliceert dat de bepaling niet alleen betrekking heeft op het gebruik van erfelijkheidsgegevens in de gezondheidszorg, maar ook op gebruik van die gegevens op andere terreinen van het maatschappelijk leven. Een voorbeeld is het onderzoek van erfelijk materiaal voor de vaststelling van de identiteit van personen in verband met een strafbaar feit waarbij DNA-sporen zijn veiliggesteld.
De bepaling heeft ook consequenties in het kader van de totstandkoming en uitvoering van bepaalde overeenkomsten, zoals bijvoorbeeld de verzekeringsovereenkomst. Erfelijkheidsgegevens die een aspirant-verzekerde met het oog op het afsluiten van een levensverzekering omtrent hemzelf aan de verzekeraar heeft verstrekt, mogen uitsluitend en alleen met betrekking tot die persoon worden gebruikt en niet met betrekking tot een ander in dezelfde genetische lijn. Het verbiedende karakter van de bepaling – zoals eerder toegelicht – brengt met zich dat zulks ook niet is toegestaan op een van de gronden van artikel 23, eerste lid. Dit betekent onder meer dat verwerking van erfelijkheidsgegevens met betrekking tot anderen dan degene omtrent wie de gegevens oorspronkelijk zijn verkregen ook niet is toegestaan met uitdrukkelijke toestemming van de betrokkene of enig familielid waarop de gegevens eveneens betrekking hebben. Artikel 8, tweede lid, onder a, van de richtlijn maakt een dergelijk voorschrift uitdrukkelijk mogelijk. Een en ander heeft tot gevolg dat indien iemand zich meldt als aspirant-verzekerde waarvan in theorie via erfelijkheidsgegevens van familieleden bekend zou kunnen zijn dat zich met het oog de toekomstige gezondheidstoestand een bijzondere situatie voordoet, de betrokkene niettemin op gelijke voet met elke andere aspirant-verzekerde behandeld behoort te worden.
Als gevolg van het vierde lid blijft het gebruik van genetische gegevens beperkt tot de betrokkene zelf die deze heeft verstrekt. Daarmee staan zij op één lijn met de verstrekking van andere gegevens van medische aard die de betrokkene bij het aanvragen van een verzekering verstrekt. De essentie van de regeling is aldus dat het bijzondere uitstralingseffect dat inherent is aan erfelijkheidsgegevens wordt geredresseerd. Daarmee wordt de keuze gemaakt het risico voor mogelijke erfelijke tekortkomingen bij een persoon niet buiten hem om voor zijn rekening te brengen, doch vanouds te laten bij de samenleving. Daardoor wordt voorkomen dat bij de voortschrijdende ontwikkeling van de genetica een tweedeling van mensen ontstaat: zij die genetisch wel en zij die niet een risico vormen. Waar vroeger het gebrek aan wetenschappelijke kennis feitelijk een dergelijke ongelijkheid tussen mensen voorkwam, is het in de toekomst nodig normatief, via het recht, een dergelijke ongelijkheid te voorkomen. De vanouds bestaande situatie dat de betrokkene zelf gegevens verstrekt opdat de verzekeraar het risico dat hij met het accepteren van de betrokkene loopt, te kunnen inschatten, blijft onverlet. Een en ander laat

ook onverlet dat de verwerking van erfelijkheidsgegevens op grond van de WBP – afgezien van artikel 21 – aan dezelfde regels zal zijn gebonden als andere gegevensverwerkingen.
Het verbod van het vierde lid vindt alleen geen toepassing indien een zwaarwegend geneeskundig belang prevaleert. De situatie kan zich voordoen dat in het kader van een geneeskundig onderzoek uit erfelijkheidsgegevens blijkt dat behandeling van anderen dan degene bij wie het onderzoek is gedaan, wellicht noodzakelijk is. In dat geval moet het in het belang van de desbetreffende personen zelf, in beginsel mogelijk zijn om deze daaromtrent te benaderen. In hoeverre zulks in het concreet geval aangewezen is zal afhangen van de omstandigheden en zal door de hulpverlener binnen de regels van zijn professie zorgvuldig moeten worden afgewogen. Het ligt voor de hand dat hiertoe gedragsregels worden geformuleerd.
Daarnaast geldt het verbod niet indien een verwerking als hiervoor bedoeld, noodzakelijk is ten behoeve van wetenschappelijk onderzoek of statistiek. Een dergelijke uitzondering is noodzakelijk om het wetenschappelijk onderzoek waarbij erfelijkheidsgegevens niet kunnen worden gemist, niet te belemmeren. Een afzonderlijke bepaling is hier nodig omdat het vierde lid een verbiedende bepaling is die – zoals in het algemeen deel van deze memorie reeds is toegelicht – de toepassing van artikel 23, tweede lid, uitsluit. Voor de hier bedoelde onderzoeken dienen echter wel voorwaarden te worden gesteld die gelijk zijn aan de voorwaarden die voortvloeien uit toepassing van artikel 23. Om die reden zijn in de laatste volzin artikel 23, eerste lid, onderdeel b en tweede lid van overeenkomstige toepassing verklaard. Dit impliceert dat verwerking van gegevens omtrent erfelijke eigenschappen als bedoeld in het vierde lid alleen is toegestaan met uitdrukkelijke toestemming van de betrokkene, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost. Voorts geldt dat bij de uitvoering van het onderzoek moet zijn voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Deze laatste voorwaarde komt overeen met hetgeen in algemenere zin krachtens het huidige artikel 11, tweede lid, WPR wordt bepaald.
Indien inderdaad een zwaarwegend geneeskundig belang of het belang van wetenschappelijk onderzoek en statistiek noopt tot afwijking van de hoofdregel van het vierde lid, zal de verwerking van de desbetreffende gegevens uiteraard wel aan de overige door de WBP gestelde voorwaarden dienen te voldoen. Ook hier geldt derhalve dat het vierde lid slechts een verbod opheft en derhalve geen algemene machtiging vormt voor het gebruik van de betreffende gegevens. Is aan de voorwaarde van het vierde lid voldaan, dan zal om de rechtmatigheid van de gegevensverwerking te kunnen vaststellen vervolgens een toetsing dienen plaats te vinden aan de bepalingen van paragraaf 1 van het onderhavige hoofdstuk (art. 6 e.v.). Daarnaast is het mogelijk dat in aanvulling hierop bepalingen uit andere wetten van toepassing zijn. Zo is voor zover het gaat om wetenschappelijk onderzoek met erfelijkheidsgegevens verkregen binnen de sfeer van de gezondheidszorg, artikel 7:458 BW van toepassing. De betreffende bepaling is te beschouwen als een precisering van de WBP. Zie ook paragraaf 5 van het algemeen deel van de toelichting.

Vijfde lid

Het laatste lid van artikel 21 bepaalt dat omtrent de toepassing van de onderdelen b en e bij algemene maatregel van bestuur nadere regels kunnen worden gesteld. De mogelijkheid hiertoe wordt geopend om te kunnen komen tot een precisering van de in het wetsvoorstel neergelegde noodzakelijkheidseis met het oog op de verwerking van gezondheidsgegevens in de sociale zekerheid. De bepaling is vanwege de breedte van het terrein facultatief geformuleerd. Niettemin zijn wij voornemens voor

een beperkt deel van het terrein van de geboden mogelijkheid gebruik te maken, namelijk wat betreft de uitkomsten van het recente parlementaire debat over het gebruik van medische gegevens in het kader van de uitvoering van de arbeidsongeschiktheidswetgeving. Verwezen zij naar de toelichting op onderdeel. In de algemene maatregel van bestuur zullen in elk geval als uitvloeisel van deze discussie nadere regels worden gesteld, alsmede ten aanzien van verwerking van gezondheidsgegevens door verzekeraars, die het financiële risico van werkgevers in verband met ziekte en arbeidsongeschiktheid van hun werknemers verzekeren. Om deze reden wordt in het vijfde lid ook verwezen naar onderdeel b. Conform de huidige beleidslijn zal voor deze verzekeraars gelden dat zij slechts een beperkt aantal persoonsgegevens betreffende iemands gezondheid mogen verwerken. Indien een verzekeraar meer gezondheidsgegevens nodig heeft, dan zal hij voor de verwerking daarvan uitdrukkelijke toestemming dienen te verkrijgen van de betrokken werknemer. De gegevensverwerking op basis van uitdrukkelijke toestemming van de betrokkenen is geregeld in artikel 23.

Artikel 22

De bepaling geeft uitvoering aan artikel 8, vijfde lid, van de richtlijn in die zin dat zij beoogt de passende en specifieke waarborgen te geven voor de verwerking van gegevens inzake overtredingen, strafrechtelijke veroordelingen of veiligheidsmaatregelen.
Het begrip «strafrechtelijke gegevens» heeft betrekking zowel op veroordelingen als op min of meer gegronde verdenkingen. Veroordelingen betreffen gegevens waarbij de rechter, al dan niet onherroepelijk, strafrechtelijk gedrag heeft vastgesteld. Bij verdenkingen gaat het om concrete aanwijzingen jegens een bepaalde persoon. Het begrip strafrechtelijk gegevens omvat mede gegevens omtrent de toepassing van het formele strafrecht, bijvoorbeeld het gegeven dat iemand is gearresteerd of dat tegen hem proces-verbaal is opgemaakt wegens een bepaald vergrijp. De bepaling heeft geen betrekking op de verwerking van persoonsgegevens gericht op de vaststelling van mogelijk strafbaar gedrag, bij voorbeeld door het volgen van trends. Daarop is het algemene regime van paragraaf 1 van hoofdstuk 2 van toepassing.
De bepaling regelt de verwerking van gegevens over personen die wegens gebleken of vermoede onregelmatigheden niet op gelijke voet als anderen aan het maatschappelijk verkeer kunnen deelnemen of op wie de aandacht is gericht in verband met mogelijk verwijtbaar gedrag. De verwerking van dergelijke gegevens dient aan bijzondere waarborgen te worden onderworpen. Niet alleen de persoonlijke levenssfeer, maar ook het gelijkheidsbeginsel is hier in het geding. De presumptio innocentiae (het vermoeden van onschuld) brengt met zich mee dat iemand niet duurzaam de verdenking mag worden tegengehouden van een strafbaar feit, wanneer niet in rechte zijn schuld is vastgesteld. Vervolgens brengt de resocialisatiegedachte met zich mee dat iemand niet na een veroordeling en het ondergaan van de straf, duurzaam van deelname aan de samenleving kan worden uitgesloten. Het resocialisatiebelang dient te worden afgewogen tegen het belang van de samenleving om zich te beveiligen tegen criminaliteit.
Dit wetsvoorstel geeft hier een concretisering van de fundamentele rechten en vrijheden, ook van andere dan het recht op bescherming van de persoonlijke levenssfeer, zoals al eerder in meer abstracte vorm aan de orde kwam in artikel 8, onder f, voor zover het gaat om strafrechtelijke gegevens.
Indien het gaat om het waarborgen van een zorgvuldig omgang met strafrechtelijke persoonsgegevens is er een belangrijk onderscheid tussen veroordelingen en verdenkingen. Bij strafrechtelijke veroordelingen heeft de betrokkene zich kunnen uitlaten over het hem telastgelegde en

vervolgens heeft de rechter de feiten vastgesteld. Dit geldt ook voor veroordelingen waartegen nog beroep mogelijk is. Het gaat om «harde» gegevens. De vastlegging van een strafrechtelijke veroordeling vergt een apart regime in verband met de ingrijpende gevolgen die het bekend zijn daarvan voor het maatschappelijk functioneren kunnen hebben. Dit klemt evenwel te meer voor de verwerking van gegevens die betrekking hebben op een verdenking. De betrokkene heeft zich dan immers veelal nog niet over de gegevens kunnen uitlaten. Het kan gaan om summiere aanwijzingen waarvan achteraf kan blijken dat zij van iedere grond zijn ontbloot. Deze worden veelal aangeduid als «zachte» gegevens.
Indien de rechter heeft vastgesteld dat de verdenking ten onrechte op de betrokkene was gericht, dan wel de gedraging van de betrokkene niet is te kwalificeren als een strafbaar feit, dan is een bijzondere rechtvaardiging nodig om de gegevens op rechtmatige wijze te blijven bewaren. Ingevolge artikel 8 van het wetsvoorstel mogen particulieren gegevens verwerken voor zover dit noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene prevaleert. Indien de betrokkene terzake wordt ontslagen van rechtsvervolging of wordt vrijgesproken geldt daarom voor de verantwoordelijke een extra bewijslast. Wanneer bij voorbeeld gegevens worden bijgehouden over iemand teneinde vast te stellen of hij er een gewoonte van maakt om goederen te kopen zonder te betalen en zich daarmee schuldig maakt aan flessetrekkerij (artikel 326a van het Wetboek van Strafrecht), zullen ook na een vrijspraak, de verschillende gevallen van niet-betalen echter kunnen worden geregistreerd. Dergelijke gevallen zullen immers in de toekomst in samenhang met nieuwe gevallen mogelijk alsnog van belang zijn voor een hernieuwde vervolging.
De richtlijn noemt nog de categorie «veiligheidsmaatregelen». Hiermee wordt gedoeld op rechterlijke uitspraken, ongeacht of deze afkomstig zijn van de strafrechter, de civiele of de administratieve rechter, waarbij op enigerlei wijze aan de betrokkene voorschriften zijn gegeven met betrekking tot zijn gedrag. In de regel zal het gaan om z.g. straatverboden: iemand mag niet een bepaalde straat of een bepaald gebouw binnentreden. Aanzeggingen van de eigenaar van bij voorbeeld een winkelbedrijf dat iemand niet meer de desbetreffende winkel mag betreden, vallen dus niet onder het bijzondere regime van deze bepaling. De verwerking daarvan valt weer onder het algemene regime van persoonsgegevens.

Uit een oogpunt van criminaliteitsbestrijding kan de vastlegging van strafrechtelijk gegevens niet worden voorbehouden aan de overheidsorganen die zijn belast met het toezicht. Ook private (rechts)personen hebben een gerechtvaardigde beveiligingsbehoefte in welk verband onder omstandigheden de verwerking van persoonsgegevens noodzakelijk is. Een aangescherpte regeling is nodig gelet op het reeds aangeduide gevoelige karakter van deze gegevens.

Eerste lid

De bepaling ziet op de organen van Justitie en de bijzondere opsporingsdiensten. Het slaat niet op de reguliere politie. De algemene normen zijn wat betreft de uitvoering van haar specifieke taak nader uitgewerkt in sectorale wetgeving: de Wet politieregisters. Dit wetsvoorstel wijkt niet af van de keuze die met de WPR is gemaakt, om bijzondere opsporingsdiensten, gelet op hun diversiteit van taken en het gezag waaronder zij ressorteren, onder het algemene regime van gegevensbescherming te brengen. Bij het wetsvoorstel tot wijziging van de Wet politieregisters (kamerstukken II 1996/97, ...) wordt evenwel voorgesteld om nader bij algemene maatregel van bestuur te bepalen bijzondere opsporings-

diensten voor een deel hun registraties met betrekking tot zware criminaliteit onder de Wet politieregisters te brengen.
Verder bevat dit lid een spiegelbepaling ten opzichte van de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag en de Wet politieregisters, opdat de krachtens die wetten door derden ontvangen gegevens ook daadwerkelijk kunnen worden verwerkt voor de doeleinden waarvoor deze zijn verkregen. Wat betreft de eerste wet gaat het vaak om veroordelingen die tijdens een openbare zitting zijn uitgesproken en op enig moment voor ieder kenbaar zijn. Toch is de verdere verwerking van deze gegevens slechts onder de beperkende voorwaarden van deze bepaling toegestaan. Artikel 36 van de eerste en artikel 30 van de tweede wet bevatten op elkaar lijkende geheimhoudingsbepalingen, ingevolge welke de aldus ontvangen gegevens niet mogen worden gebruikt voor andere doeleinden dan waarvoor zij zijn verkregen. Dit kan met zich meebrengen dat deze apart als zodanig moeten worden gemarkeerd, bij voorbeeld wanneer niet uit het verband waarbinnen zij worden gebruikt al van een dergelijk beperkt regime blijkt.

Tweede lid

Deze bepaling bevat een zelfstandig, beperkt gebruiksregime: de verantwoordelijke mag de gegevens gebruiken ter bescherming van zichzelf. Deze bescherming kan daarin bestaan dat de betrokkene binnen de organisatie van de verantwoordelijke beperktere ontplooiingsmogelijkheden heeft, wordt uitgesloten van toekomstige contracten of dat het contract met hem wordt beëindigd. Uit artikel 16 vloeit voort dat de gegevens dus niet kunnen worden verstrekt aan anderen dan volgens het bijzondere regime van het vierde lid. Zonder een dergelijke beperking moet immers worden gevreesd dat bij de afweging van het beveiligingsbelang van de samenleving tegen het resocialisatiebelang van de betrokkene, het eerste bijna altijd zwaarder zal wegen. De wettelijke bepalingen die een dergelijke afweging beogen te bewerkstelligen, zouden daarmee hun doel missen. Een voorbeeld is het systeem van de verklaring omtrent het gedrag.
Ingevolge onderdeel a mogen strafrechtelijk gegevens worden gebruikt met het oog op een beslissing omtrent betrokkene of een maatregel met betrekking tot hem naar aanleiding van een verzoek. Het hoeft daarbij niet noodzakelijkerwijs te gaan om gegevens betreffende strafrechtelijk gedrag waarvan de verantwoordelijke slachtoffer is. Denkbaar is dat een koepelorganisatie van een branche, optredend met het oog op dienstverlener aan zijn leden, gegevens verwerkt afkomstig van het ene bedrijf die relevant kunnen zijn voor de beoordeling van de vraag of een contract met de betrokkene zal worden aangegaan door een ander bedrijf. Wanneer de verantwoordelijke deze rechtmatig van een dergelijke koepelorganisatie heeft verkregen, kan hij deze gebruiken. Daarnaast kunnen bepaalde organisaties ter beveiliging van zichzelf aanspraak maken op verstrekking van gegevens uit de justitiële documentatie of uit de politieregisters.
Onderdeel b ziet vooral op gegevens die hun oorsprong vinden binnen de organisatie van de verantwoordelijke zelf. De bepaling machtigt een verantwoordelijke om ten behoeve van zichzelf gegevens vast te leggen en te gebruiken wanneer hij het slachtoffer is geweest van een strafbaar feit of mogelijk slachtoffer dreigt te worden. Daarnaast machtigt dit onderdeel de verantwoordelijke om gegevens vast te leggen wanneer door personeel in de uitoefening van zijn dienst strafbare feiten heeft gepleegd of dreigt te plegen, hetzij tegen de verantwoordelijke zelf hetzij tegen derden. Het gaat dan om personeel dat arbeid verricht in dienst van de verantwoordelijke (krachtens arbeidscontract of als ambtenaar), dan wel krachtens een andere overeenkomst.

Derde lid

Deze bepaling stelt zeker dat gegevens in de arbeidsrechtelijke sfeer slechts worden verwerkt na betrokkenheid van de ondernemingsraad. De bepaling impliceert een opdracht tot zelfregulering, gebruikmakend van de omstandigheid dat er vanuit een ander perspectief een organisatorisch kader beschikbaar is waarin de verantwoordelijke en de betrokkenen in onderling overleg binnen de algemene kaders van dit wetsvoorstel rechtsvormend kunnen werken. Het beperkt zich tot de gegevensverwerking binnen een bedrijf.

Vierde lid

Deze bepaling geeft een bijzondere regeling ter bescherming van de belangen van derden die het slachtoffer zouden kunnen worden van criminaliteit. In beginsel is daarvoor, zoals vermeld, het instrument beschikbaar van de verklaring omtrent het gedrag zoals deze is geregeld in de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag. In bijzondere gevallen bevatten deze wet en de Wet politieregisters aparte procedures om belangen van derden te beschermen tegen personen met criminele achtergronden. Dan gaat het om de verstrekking van informatie door de overheid, die daarbij put uit een landelijk dekkende registratie. In zeer bijzondere gevallen wordt een veiligheidsonderzoek als bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten uitgevoerd door de Binnenlandse Veiligheidsdienst. Ondanks deze voorzieningen kan het toch nodig zijn ook tussen particulieren onderling uit een oogpunt van beveiliging van elkaar gegevens uit te wisselen.
Blijkens onderdeel a kan de verstrekking van strafrechtelijke gegevens aan derden plaatsvinden door een verantwoordelijke die valt onder de werking van de Wet particuliere beveiligingsorganisaties en recherchebureaus[1]. Deze particuliere organisaties kunnen met een vergunning en onder toezicht van de overheid taken verrichten die verband houden met criminaliteitsbestrijding. In de vergunningsvoorwaarden kunnen op grond van artikel 4, zesde lid, onder b, in verband met artikel 6, onder i, van die wet nadere voorschriften worden gegeven over onderwerpen die de kwaliteit van deze organisaties raken. Deze voorschriften kunnen mede betrekking hebben op de bescherming van persoonsgegevens.
Onderdeel b opent de mogelijkheid dat binnen een concern deze gegevens worden verwerkt. Daarnaast blijkt in de praktijk behoefte te bestaan om ook anderszins strafrechtelijke gegevens tussen bedrijven onderling uit te wisselen via een landelijk dekkend of nagenoeg dekkend systeem. Het gaat dan vooral om uitwisseling binnen een bepaalde branche. Een voorbeeld is het Bureau Kredietregistratie (BKR) dat is opgezet ten behoeve van de kredietverlening door banken. De bestaande praktijk is zo divers dat het bezwaarlijk is daarvoor algemene inhoudelijke normen vast te stellen met een zodanig beschermend karakter dat wordt voldaan aan de eis van de richtlijn dat het moet gaan om «passende en specifieke waarborgen». Daarom is gekozen voor een deels procedurele benadering.
Onderdeel c herhaalt de algemene norm van de richtlijn, zodat deze in het kader van zelfregulering invulling kan krijgen. Deze norm zelf voldoet uiteraard niet aan haar eigen eis: zij is onvoldoende specifiek en alleen al daarom niet passend. De daarin besloten liggende eis tot afweging van belangen behoeft nadere concretisering. Een voorstel daartoe kan worden gedaan door de verantwoordelijke. Het zou echter onjuist zijn dat hij zelf, als belanghebbende bij de afweging, daarin het laatste woord zou hebben. Gaat het om registratie op brancheniveau dan valt ook de werking van de markt weg. Een aanvullende waarborg is nodig om het belang van de betrokkenen een gezicht te geven. De aard van de

[1] Kamerstukken II 1994/95, 23 478, nr. 7.

gegevens staat echter aan hun deelname bij de totstandkoming van de zelfregulering in de weg. Daarom is gekozen voor het publiekrechtelijke sluitstuk van de procedure van artikel 31 inzake het voorbereidende onderzoek door de Registratiekamer. Het rapport van de Registratiekamer over «zwarte lijsten» van mei 1995 die binnen bepaalde branches worden gehanteerd, geeft een indicatie van de grenzen die daarbij in acht moeten worden genomen. Een spiegelbepaling is opgenomen in artikel 31, eerste lid, onder c.

Vijfde lid

Het is mogelijk dat strafrechtelijke gegevens tevens betrekking hebben op bij voorbeeld gegevens omtrent het seksuele leven. Denkbaar is dat in de ondernemingsraad afspraken worden gemaakt over de bestrijding van seksuele intimidatie op de werkvloer. Voor zover daarbij gegevens met een strafrechtelijke relevantie moeten worden vastgelegd, laat deze bepaling dat toe.

Zesde lid

Het zesde lid ziet op een rechterlijk verbod jegens een bepaalde persoon. Dit verbod is civielrechtelijk of vindt zijn grondslag in een bijzondere voorwaarde bij een voorwaardelijke strafrechtelijke veroordeling zoals bijvoorbeeld een straatverbod. Ook kan het gaan om een verbod krachtens het administratieve recht. Zo bestaan er zwarte lijsten waarop een burgemeester personen opgenomen heeft die wegens drankmisbruik geen cafés meer mogen betreden[1]. Wanneer een dergelijke aanzegging niet nagekomen wordt, bestaat de mogelijkheid aangifte van huis- of lokaalvredebreuk in de zin van de artikelen 138 of 139 van het Wetboek van Strafrecht te doen. Dergelijke verboden of aanzeggingen moeten kunnen worden gedocumenteerd. Zij worden dus in de regel gedaan naar aanleiding van onrechtmatig of hinderlijk gedrag en zijn in die zin verwant aan gegevens van strafrechtelijke aard. Iemands mogelijkheden om op gelijke voet als anderen deel te nemen aan het maatschappelijk verkeer, worden daardoor immers, zij het in de regel door eigen schuld, beperkt. De bepaling laat onverlet dat op een andere wettelijke grondslag ook voor andere doeleinden deze gegevens worden verwerkt. Zo laat artikel 23 bijvoorbeeld toe dat deze gegevens ook voor statistische doeleinden worden verwerkt. Zonder een dergelijke uitdrukkelijke wettelijke grondslag geldt evenwel het algemene verbod van artikel 16. Evenzeer blijft de eis van kracht van een toereikende rechtvaardigingsgrondslag als bedoeld in afdeling I van dit hoofdstuk.

Artikel 23

Deze bepaling bevat voorschriften voor de gevallen dat het verwerken van gevoelige gegevens niet in de daaraan voorafgaande eerdere artikelen is geregeld. Dit artikel kan daarmee worden beschouwd als een algemene restbepaling waarin voor het verwerken van de betrokken gegevens een ontheffing van het verwerkingsverbod van artikel 16 kan gelden. Het artikel heeft dezelfde functie als het huidige artikel 8 BGG. In het artikel worden onderdelen van artikel 8, tweede en vierde lid, van de richtlijn geïmplementeerd.

Eerste lid

In onderdeel a wordt artikel 8, tweede lid, onder a van de richtlijn geimplementeerd. Anders dan in artikel 8 van het Besluit gevoelige gegevens wordt geen schriftelijke toestemming vereist. Daarentegen is met het begrip «uitdrukkelijke» wel een aanscherping beoogd ten opzichte

[1] Vgl. ARRS 16-9-1982, AB 1983, 38.

van de toestemmingseis die elders wel in de richtlijn wordt gesteld. In geval de verantwoordelijke de uitdrukkelijke toestemming van de betrokkene dient te verkrijgen, dient de betrokkene expliciet zijn wil omtrent de verwerking te hebben geuit. Een stilzwijgende of impliciete toestemming is onvoldoende: de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking. Voor een nadere uiteenzetting zij verwezen naar de toelichting op het in artikel 1 gehanteerde toestemmingsbegrip.
Onderdeel b is de implementatie van artikel 8, tweede lid, onder e, van de richtlijn. Er geldt een ontheffing voor de verwerking van gevoelige gegevens indien de gegevens door de betrokkene openbaar zijn gemaakt. Evenals bij onderdeel a ligt de rechtvaardigingsgrond voor de ontheffing besloten in het handelen of het gedrag van de betrokkene zélf. Anders dan bij onderdeel a is er echter geen sprake van op de gegevensverwerking gerichte toestemming, maar van een spontane gedraging van de betrokkene en waar niet door enig andere persoon met het oog op een eventuele gegevensverwerking om is gevraagd. Dat de gegevens openbaar zijn, moet derhalve volgen uit gedrag van de betrokkene waaruit de intentie om openbaar te maken uitdrukkelijk blijkt. Het laatste blijkt onder meer uit het feit – de Registratiekamer heeft hier terecht op gewezen – dat de richtlijn bepaalt dat de gegevens «duidelijk» door de betrokkene openbaar moeten zijn gemaakt. Dit is bijvoorbeeld duidelijk het geval in de situatie waarin een persoon die verkiesbaar is voor de volksvertegenwoordiging, zich met bepaalde politieke opvattingen in de publiciteit profileert. Het betreft hier een gegeven omtrent politieke gezindheid dat in beginsel door anderen mag worden verwerkt. Dat er sprake moet zijn van een intentie bij de betrokkene, blijkt ook uit de formulering van de bepaling: de gegevens moeten door de betrokkene openbaar zijn gemaakt.
Anders ligt daarom de situatie waarin een bepaald gegeven openbaar is, maar de uitdrukkelijke wens tot openbaarmaking niet door de betrokkene is geuit. Dit doet zich bijvoorbeeld voor bij personen met een handicap. Dit gezondheidsgegeven is in veel gevallen voor een ieder zichtbaar, maar niet uit vrije wil aan de kant van de betrokkene. Dit gegeven mag derhalve niet op grond onderdeel b worden verwerkt, tenzij de betrokkene zich als zodanig – bijvoorbeeld als belangenbehartiger voor gehandicapten – in de openbaarheid profileert.
Het is hierbij niet relevant of de openbaarmaking vrijwillig of krachtens wettelijk voorschrift heeft plaatsgevonden. Een voorbeeld van vrijwillige openbaarmaking betreft het telefoonboek. Ieder is immers vrij de vermelding daarin te voorkomen. In de vermelding kunnen op verzoek van de betrokkene ook gevoelige gegevens voorkomen. Een voorbeeld van een verplichte openbaarmaking is de registratie van rechtspersonen bij de Kamers van Koophandel waarbij een natuurlijk persoon als bestuurder staat vermeld. Dit gegeven heeft de betrokkene krachtens wettelijk voorschrift zelf openbaar gemaakt. Dit kan ook impliciet door in te stemmen met de benoeming tot bestuurder. Wanneer het bij voorbeeld gaat om het bestuur van een politieke partij of een vereniging van patiënten die lijden aan een bepaalde ziekte, kan het daarbij gaan om een gevoelig gegeven. Overigens heft deze openbaarmaking slechts het verbod tot verwerking van gevoelige gegevens op. Daarmee is nog geenszins vastgesteld dat er ook een rechtvaardiging tot gegevensverwerking aanwezig is als bedoeld in artikel 8. Persoonsgegevens, ook al zijn deze openbaar, mogen slechts worden verwerkt binnen de grenzen van dit wetsvoorstel.
In onderdeel c wordt de laatste zinsnede van artikel 8, tweede lid, onder e geïmplementeerd. Verwerking van gevoelige persoonsgegevens kan toelaatbaar zijn indien dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte. De formulering van

de bepaling is gelijk aan die van de richtlijn. Particulieren kunnen onder omstandigheden hun rechten in een rechterlijke procedure niet effectueren zonder dat zij beschikken over bepaalde gegevens van hun wederpartij. Een voorbeeld daarvan is te vinden in CRvB 15 februari 1995, NJCM-Bull. 1995, p. 421 e.v. Uit deze uitspraak kan worden afgeleid dat een werkgever niet zonder meer kan worden verplicht tot betaling van een geldsom (in casu een malus op grond van de AAW) indien hij niet op de hoogte is van de gegevens die in het concrete geval aan het opleggen van de verplichting ten grondslag hebben gelegen. In casu betrof het medische gegevens van de werknemer die arbeidsongeschikt is geworden. Het begrip «noodzakelijk» in onderdeel c betekent dat de betreffende gegevens niet zonder meer mogen worden verwerkt: er zal een afweging moeten plaatsvinden tussen het recht van de betrokkene om zijn gezondheidsgegevens geheim te houden en het recht van de wederpartij op een eerlijk proces. Dit ligt in lijn met de zojuist genoemde uitspraak van de Centrale Raad van Beroep.
Onderdeel d brengt mee dat het verwerken van een gevoelig gegeven geoorloofd kan zijn indien daarmee wordt gehandeld overeenkomstig een volkenrechtelijke verplichting en deze verplichting tot het verwerken van zulke gegevens noodzaakt. In een dergelijk geval is het verwerken van de gegevens als zodanig niet formeel wettelijk geregeld, maar is het voldoende duidelijk dat de wel in de volkenrechtelijke regeling – bijvoorbeeld een verdrag – geregelde verplichting enkel kan worden uitgevoerd indien daartoe bepaalde gegevens kunnen worden verwerkt. Uiteraard geldt nadrukkelijk dat het verbod om gevoelige gegevens te verwerken alleen niet van toepassing is indien sprake is van een «zwaarwegend algemeen belang». De verwerking op deze grond kan immers slechts worden gebaseerd op artikel 8, vierde lid, van de richtlijn op grond waarvan bedoelde eis geldt. Voorts dient deze bepaling in het geval dat landen buiten de Unie zijn betrokken, in samenhang te worden gezien met artikel 76 e.v.
De onderhavige verwerkingsgrond wordt thans op gelijke wijze geregeld in artikel 8, onderdeel a, BGG. In afwijking van het BGG is niet opgenomen dat gevoelige gegevens ook kunnen worden verwerkt op grond van een formeelwettelijke verplichting. Een dergelijke verwerkingsgrond is – mede gelet op artikel 10 Grondwet en 8 EVRM – onvoldoende specifiek. Mede gezien het voorschrift van artikel 16 inhoudende dat een verwerking van een gevoelig gegeven bij wet moet zijn bepaald, dient een concretere rechtsgrondslag te bestaan. Zoals in de toelichting op laatstgenoemd artikel reeds is vermeld kan in deze grondslag zowel in de WBP als in een bijzondere wet worden voorzien.
Ten slotte is er in onderdeel e een algemene ontheffing tot verwerking van gevoelige gegevens gecreëerd. Voor zover een ontheffing niet kan worden gebaseerd op een van de hiervoor besproken bepalingen kan een verwerking ingevolge onderdeel e zijn grondslag vinden in hetzij een bijzondere wet, hetzij een beschikking van de Registratiekamer. Een en ander ligt in het verlengde van artikel 8, vierde lid, van de richtlijn. In beide gevallen dient aan twee voorwaarden te zijn voldaan: de verwerking dient noodzakelijk te zijn met het oog op een zwaarwegend algemeen belang en er dienen in het belang van de persoonlijke levenssfeer passende waarborgen te worden gecreëerd. Beide voorwaarden vloeien eveneens voort uit de genoemde bepaling van de richtlijn.
De Registratiekamer vraagt zich af of opneming van het criterium inzake het zwaarwegend algemeen belang als norm gericht tot de formele wetgever nodig is. Het is – zoals de Registratiekamer stelt – inderdaad juist dat de voorwaarde vooral bedoeld is als opdracht aan de bijzondere wetgever wanneer het voornemen bestaat een verwerking van gevoelige gegevens bij een bijzondere wet mogelijk te maken. Niettemin achten wij het wenselijk om indien artikel 23 WBP conform het huidige Besluit gevoelige gegevens (BGG) regelt dat verwerking van gevoelige gegevens

slechts mogelijk is voor zover dit bij wet is bepaald, dan in samenhang daarmee ook uitdrukkelijk te bepalen aan welke materiële norm de formele wetgever daarbij heeft te voldoen. Het verdient uit een oogpunt van kenbaarheid van het recht de voorkeur bij bedoelde basisnorm niet uitsluitend terug te hoeven vallen op de EG-richtlijn, maar deze ook uitdrukkelijk op te nemen in de Nederlandse wetgeving. Uit de context van de bepaling is voorts voldoende duidelijk dat het gaat om een door de formele wetgever te verrichten abstracte toetsing. Indien de wetgever van oordeel is dat een bepaalde verwerking noodzakelijk is met het oog op een algemeen zwaarwegend algemeen belang en voor een zodanige verwerking een uitdrukkelijke wettelijke basis creëert, behoeft bij de toepassing van de regeling niet steeds opnieuw in concreto aan de betreffende norm te worden getoetst.
Zoals gezegd wordt met artikel 23 de waarborg van artikel 1 BGG gecontinueerd. Op grond van laatstgenoemd artikel mogen gevoelige persoonsgegevens alleen in een persoonsregistratie worden opgenomen voor zover dit bij de wet is bepaald dan wel in het BGG is toegestaan. Aangezien dit besluit thans in het wetsvoorstel wordt geïncorporeerd, kan in de toekomst gelden dat de verwerking van gevoelige gegevens alleen bij wet (de WBP of een andere wet) kan worden toegestaan.
De zinsnede «bij wet bepaald» brengt met zich dat de verwerking van een gevoelig gegeven alleen mogelijk is indien bij formele wet daarin is voorzien. Dit betekent dat een zodanige verwerking in de WBP of in een formele wet uitdrukkelijk moet zijn geregeld. Is een regeling op het niveau van de formele wet niet voorhanden, dan is de verwerking niet toegestaan. De bedreiging die gevoelige gegevens kunnen inhouden voor de persoonlijke levenssfeer van de betrokkene rechtvaardigt een oordeel van de formele wetgever over de noodzaak van het verwerken van deze gegevens. Het is derhalve niet mogelijk dat een algemene maatregel van bestuur, ongeacht of deze op de wet steunt of niet, een zelfstandige basis biedt aan het verwerken van gevoelige gegevens. Wel is het toegestaan om binnen het door de formele wetgever aangegeven kader bij algemene maatregel van bestuur of ministeriële regeling regels te stellen omtrent uitvoeringsaspecten die samenhangen met een dergelijke verwerking. Het onderhavige delegatieverbod heeft daar geen betrekking op. Overigens wordt met deze benadering geen wezenlijke wijziging beoogd ten opzichte van de huidige situatie. In de toelichting op artikel 1 BGG wordt aan de zinsnede «bij de wet bepaald» een vergelijkbare interpretatie gegeven.
Indien de ontheffing niet op de WBP of een andere wet is gebaseerd, kan de verwerking ten slotte nog haar grondslag vinden in een ontheffing de Registratiekamer. Deze beslissing wordt op grond van onderdeel e bij beschikking vastgesteld. Met het oog op een adequate uitvoering van de ontheffingsbevoegdheid is in onderdeel e tevens uitdrukkelijk vastgelegd dat de Registratiekamer bij de verlening van de ontheffing beperkingen en voorschriften kan opleggen. Op grond van artikel 4:13 Awb dient de Registratiekamer de beschikking te geven binnen een redelijke termijn na ontvangst van de aanvraag. Deze termijn is in elk geval verstreken indien binnen acht weken geen beschikking is gegeven, dan wel geen kennisgeving is gedaan waarbij een redelijke termijn wordt genoemd waarbinnen de beschikking wel tegemoet kan worden gezien. Afhankelijk van het spoedeisend karakter van de betreffende verwerking kan het vereiste van een «redelijke» termijn met zich brengen dat binnen een kortere termijn dan acht weken wordt beslist. In zeer uitzonderlijke gevallen kan deze termijn slechts enkele dagen betreffen. De procedure van artikel 23, eerste lid, onderdeel e, staat los van het feit dat in specifieke gevallen, waarin zich met het oog op de bescherming van de persoonlijke levenssfeer bijzondere risico's voordoen, een uitgebreider onderzoek van de Registratiekamer nodig zal zijn, alvorens de desbetreffende verwerking zal kunnen plaatsvinden. Dit wordt nader geregeld in artikel 31 en 32.

Tweede lid

De richtlijn bevat geen afzonderlijke bepalingen voor de verwerking van gevoelige en strafrechtelijke gegevens in het kader van wetenschappelijk onderzoek en statistiek. Dit laat onverlet dat bij de totstandkoming van de richtlijn is erkend dat wetenschappelijk en statistisch onderzoek voor de samenleving van grote betekenis is. Wanneer aan nader vast te stellen voorwaarden is voldaan, wordt daarmee een zwaarwegend algemeen belang gediend. In beginsel dient daarom de verwerking van dergelijke gegevens, ook wanneer het om bijzondere gegevens in zin van deze bepaling betreft, voor dat doel te worden toegestaan. Artikel 8, vierde lid, van de richtlijn vormt hiervoor de basis. De onderhavige artikel vormt – in het verlengde van het huidige artikel 8, eerste lid, onder e, BGG – hiervoor de grondslag.
Artikel 7:458 BW bevat reeds een regeling voor het gebruik van gegevens die zijn vergaard in het kader van een geneeskundige behandelings-overeenkomst voor wetenschappelijk onderzoek. Aan deze bepaling wordt geen afbreuk gedaan: als lex specialis behoudt deze onverkort zijn gelding. Daaraan is weliswaar ten dele ontleend, doch deze naar verhouding strikte regeling is niet geheel overgenomen. Het bijzondere karakter van de verhouding arts tot patiënt is de basis voor een regeling die niet zonder meer kan worden worden getransplanteerd naar een regeling van andere bijzondere gegevens. De hier voorgestelde regeling is in overeenstemming met de richtlijn, doch niet zo strikt als die van het BW.
Voor de verwerking van bijzondere gegevens voor wetenschappelijke of statistische doeleinden staan twee wegen open. In de eerste plaats is verwerking mogelijk op grond van uitdrukkelijke toestemming van de betrokkene. Deze optie – die is gebaseerd op artikel 8, tweede lid, onder a, van de richtlijn en artikel 23, eerste lid, onder a, van dit wetsvoorstel – heeft de voorkeur.
Indien de uitdrukkelijke toestemming voor het gebruik van gegevens voor wetenschappelijke doeleinden niet kan worden verkregen, dient een ontheffing van het verwerkingsverbod te worden gebaseerd op artikel 8, vierde lid, van de richtlijn. De onderdelen a tot en met d in hun onderlinge samenhang gezien, stellen cumulatief nadere voorwaarden om invulling te geven aan de eis dat het moet gaan om een «zwaarwegend algemeen belang» terwijl «passende waarborgen» aanwezig zijn, als bedoeld in de richtlijn.
Onderdeel a vergt dat het onderzoek een algemeen belang moet dienen. Deze eis komt overeen met artikel 7:458 BW. Waar de bepaling in het BW als lex specialis zijn gelding behoudt voor de daar bedoelde gegevens, is dit onderdeel van de regeling van de BW in dit wetsvoorstel overgenomen voor bijzondere gegevens in het algemeen.
Onderdeel b is ontleend aan het bestaande voorschrift in het Besluit gevoelige gegevens. Het noodzakelijkheidscriterium brengt met zich dat de gegevens slechts voor zover en zo lang ze noodzakelijk zijn in het kader van bedoeld onderzoek, mogen worden verwerkt. Indien het belang van de gegevens met betrekking tot het onderzoek niet meer aanwezig is, dienen ze te worden verwijderd, dan wel op een zodanige wijze te worden verwerkt dat ze niet meer tot individuele personen zijn te herleiden.
Onderdeel c beperkt de toepassing van het tweede lid tot de gevallen waarin het vragen van toestemming niet kan worden gevergd. bij de formulering is aansluiting gezocht bij artikel 34, vierde lid.
Onderdeel d ten slotte is wederom ontleend aan artikel 7:458 BW. Hierin wordt bepaald dat gebruik van dergelijke gegevens alleen is toegestaan indien bij de uitvoering van het onderzoek of de statistiek is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Daarmee wordt aangesloten bij artikel 8, vierde lid, van de richtlijn dat de nationale wetgever verplicht tot het

creëren van «passende waarborgen». Welke waarborgen met het oog op de bescherming van de persoonlijke levenssfeer moeten worden getroffen, zal afhangen van het concrete geval. Te denken valt aan voorschriften met betrekking tot de toegang tot de gegevens, geheimhouding en de presentatie van de uitkomsten van het onderzoek. Slechts bij historisch onderzoek zullen persoonsgegevens ook in de uitkomsten openbaar kunnen worden gemaakt. Toetsingsmaatstaf is steeds dat de persoonlijke levenssfeer van de betrokkene niet onevenredig mag worden geschaad.
Indien aan deze aanvullende voorwaarden is voldaan, is de verwerking van bijzondere gegevens zonder uitdrukkelijke toestemming in beginsel toelaatbaar en is – anders dan de situaties die vallen onder artikel 23, eerste lid, onder e – geen instemming van de Registratiekamer nodig. Wel zal – zoals hiervoor al in algemene zin vermeld – voldaan moeten zijn aan de elders in het wetsvoorstel geregelde algemene beginselen van gegevensverwerking.
Voor statistische en wetenschappelijke doeleinden kunnen ook bijzondere gegevens worden ontleend aan registraties die op zichzelf geen direct gevoelige gegevens bevatten. Zie de toelichting op artikel 18. Zo is denkbaar dat via statistisch onderzoek de integratie van allochtonen in de Nederlandse samenleving wordt gemeten, door gebruikmakend van de geboorteplaats- en nationaliteitsgegevens van de gemeentelijke basisadministratie (GBA) of het vreemdelingeadminsitratiesysteem (VAS), vergelijkingen met andere bestanden te maken. Deze gegevens krijgen dan door het gebruik dat daarvan wordt gemaakt en het doel van hun verwerking een bijzonder karakter en komen daarmee onder de onderhavige bepaling te vallen.

Derde lid

Artikel 8, zesde lid, van de richtlijn schrijft voor dat afwijkingen van het verbod van om gevoelige gegevens te verwerken bij de Europese Commissie dienen te worden gemeld. In het geval de afwijking is gebaseerd op de wet wordt de melding verricht door de minister die het aangaat, d.w.z. de minister die voor de betreffende wet als eerste ondertekenaar optreedt. Vindt de afwijking haar grondslag in een beslissing van de Registratiekamer, dan draagt deze voor de melding zorg. Deze constructie is een logisch gevolg van artikel 23, eerste lid, onderdeel e, dat als hoofdregel formuleert dat een ontheffing van het verbod om gevoelige gegevens te verwerken hetzij op een formele wet, hetzij op een beslissing van de Registratiekamer moet zijn gebaseerd.

Artikel 24

In artikel 8, zevende lid, van de richtlijn wordt bepaald dat de lidstaten de voorwaarden vaststellen waaronder een nationaal identificatienummer of enig ander identificatiemiddel van algemene aard voor verwerkingsdoeleinden mag worden gebruikt. Deze bepaling verplicht de lidstaten tot het stellen van regels voor het gebruik van persoonsnummers van algemene aard. Thans zijn dergelijke regels allereerst te vinden in de bijzondere wetgeving. Voor het gebruik van het sofi-nummer zijn bijvoorbeeld regels opgenomen in de Algemene wet Rijksbelastingen en de Organisatiewet Sociale Verzekeringen. Verder zijn omtrent het gebruik van het A-nummer voorschriften te vinden in de Wet gemeentelijke basisadministratie persoonsgegevens. Deze regels behoeven als gevolg van de richtlijn niet te worden gewijzigd.
In aanvulling op dergelijke regels is op dit moment in artikel 6a WPR een algemene regeling voor het gebruik van persoonsnummers opgenomen. De bepaling is ontstaan vanuit de gedachte dat een persoonsidentificerend nummer een persoonsgegeven is: het is een gegeven

waarmee een individuele natuurlijke persoon kan worden geïdentificeerd. Uit een oogpunt van bescherming van de persoonlijke levenssfeer werd het noodzakelijk geacht om aan het gebruik van dergelijke nummers beperkingen te stellen. Vast staat immers dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Voor aanvullende regels bestond te meer reden daar het sofi-nummer sinds de inwerkingtreding van de Wet op de identificatieplicht onder omstandigheden ook ter kennis van particulieren kan komen.
Het thans voorgestelde artikel 24 vormt een voortzetting van artikel 6a WPR, zij het dat een enkele vereenvoudiging is aangebracht. De bepaling spreekt over een wettelijk voorgeschreven nummer. Dat kunnen verschillende soorten nummers zijn. Op grond van de Wet gemeentelijke basisadministratie persoonsgegevens wordt het administratienummer (A-nummer) verplicht in de GBA opgenomen en voor de uitvoering van genoemde wet gebruikt. Voorts wordt bijvoorbeeld in het kader van de kentekenregistratie een persoonsidentificerend nummer aan elke geregistreerde toegekend. Ook het sofi-nummer is uiteraard een wettelijk voorgeschreven nummer als hier bedoeld.
De voorgestelde bepaling laat in de eerste plaats toe dat een wettelijk voorgeschreven persoonsnummer wordt verwerkt ter uitvoering van de wet waarin het voorschrift over het nummer is opgenomen. De praktijk leert evenwel dat dergelijke nummers ook voor andere doeleinden worden verwerkt. Onder omstandigheden is dit gerechtvaardigd, in andere gevallen echter niet. Algemene randvoorwaarde is dat persoonsgegevens niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9). Uiteraard geldt dit ook voor persoonsnummers. Omdat het gebruik van persoonsnummers – zoals hiervoor beschreven – extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, wordt in het onderhavige artikel daarenboven bepaald dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald. Aldus is een afweging op het niveau van de formele wet in beginsel gegarandeerd. Daarbij is er conform het advies van de Registratiekamer voor gekozen om op dit punt geen delegatie door de formele wetgever toe te staan. Eventuele andere gebruiksdoeleinden dienen derhalve door de formele wetgever zelf te worden vastgesteld.
Het tweede lid is gelijkluidend aan het huidige artikel 6a, tweede lid, WPR. In aanvulling op het eerste lid – dat betrekking heeft op de regeling van het gebruik in de wet waarin het betreffende nummer verplicht wordt voorgeschreven – wordt in deze bepaling de mogelijkheid gecreëerd om bij algemene maatregel van bestuur gevallen aan te geven waarin een persoonsnummer als bedoeld in het eerste lid mag worden gebruikt. In de bedoelde maatregel kan het toegestane gebruik aan nadere voorschriften worden gebonden.

HOOFDSTUK 3 GEDRAGSCODES

Artikel 25

De algemene normen van dit wetsvoorstel lenen zich voor concretisering en nadere uitwerking in gedragsregels per sector van de samenleving. De juridische evaluatie heeft aangetoond dat het systeem van gedragscodes onder de WPR goed heeft gewerkt. Vooral in het bedrijfsleven zijn gedragscodes gerealiseerd en dan met name bij de zakelijke dienstverlening (direct marketing, marktonderzoeksbureaus, handelsinformatiebureaus, bewerkers en wervings- en selectiebureaus) en in informatie-intensieve bedrijfstakken (postorderbedrijven, producenten van (dier)geneesmiddelen, tijdschriftenuitgevers, uitzendbureaus, banken en

verzekeraars). Het Nederlandse systeem heeft mede op dit punt model gestaan voor de Europese richtlijn. Van de andere Unie-landen had slechts het Verenigd Koninkrijk een enigszins vergelijkbare regeling.
In de voorgestelde bepalingen is de richtlijn geïmplementeerd, zijn de nuttig gebleken onderdelen van de WPR behouden, zijn de aanpassingen aangebracht waartoe de evaluaties aanleiding hebben gegeven en is nauwer aansluiting gezocht bij de Awb.
De mate van verbindendheid van de gedragscode kan per sector verschillen. Het is bijvoorbeeld mogelijk dat een gedragscode slechts aanbevelingen bevat. Ten aanzien van de gedragscodes die onder het regime van artikel 15 WPR zijn opgesteld blijkt dat het meerendeel van de codes als lidmaatschapsverplichting verenigingsrechtelijke gelding hebben. Een aantal codes verplichten tevens tot contractuele doorwerking van de regeling in contracten die leden sluiten met derden of zelfs in de arbeidsovereenkomst met hun werknemers. Andere codes laten het over aan de afzonderlijke leden om de gedragscode of onderdelen daaruit op te nemen in contracten òf via algemene leveringsvoorwaarden òf door middel van een zelfstandig beding. Aldus kan de gedragscode binnen één branche een uiteenlopende mate van verbindendheid hebben.[1]

Eerste lid

Het eerste lid geeft uitwerking aan artikel 27, tweede lid, van de richtlijn. Organisaties kunnen alvorens een gedragscode vast te stellen, de Registratiekamer verzoeken te beoordelen of de code voldoet aan de wettelijke vereisten. De Registratiekamer oordeelt derhalve over een ontwerp-code. Dit in tegenstelling tot de regeling van artikel 15 WPR, op grond waarvan de organisaties een reeds vastgestelde code aan de kamer ter beoordeling geven. Materieel zal de regeling in dit wetsvoorstel echter niet veel afwijken van die van artikel 15 WPR. In de praktijk plegen organisaties immers reeds thans overleg met de kamer alvorens de code vast te stellen.
Aanvankelijk was de bevoegdheid van de kamer beperkt tot een toetsing aan dit wetsvoorstel en aan andere ter uitvoering van de richtlijn vastgestelde bepalingen. Naar aanleiding van het advies van de Registratiekamer is de laatste beperking komen te vervallen en vindt de toetsing plaats aan alle wettelijke bepalingen betreffende de verwerking van persoonsgegevens. Dit ligt ook meer in de lijn met het uitgangspunt van dit wetsvoorstel, waarvan het bereik ruimer is dan het communautaire bereik van de richtlijn.
Er is ten opzichte van de WPR in artikel 25, eerste lid, een nuance aangebracht in het toetsingscriterium van gedragscodes. In de WPR kan de Kamer toetsen of de gedragscode voldoet aan (1) de wet en (2) redelijkerwijs ter bescherming van de persoonlijke levenssfeer te stellen eisen. Het is gebleken dat onduidelijkheid bestaat of met dit tweede criterium van de opstellers van een gedragscode een inspanning wordt verwacht die uitstijgt boven de normstelling van de wet en zo ja, welke de rechtsgrondslag is van een dergelijke inspanningsverplichting. In de thans voorgestelde bepaling is in aansluiting op de tekst van de richtlijn het criterium opgenomen «een juiste uitwerking vormen van deze wet». Dit reduceert de toetsingscriteria tot het hierboven genoemde eerste criterium, te weten: overeenstemming met de wet. Integenstelling tot hetgeen de Registratiekamer in haar advies suggereert dient dit criterium niet te eng worden opgevat. In de toetsing staat centraal de vraag of de regels «gelet op de bijzondere kenmerken van de sector van de samenleving» waarom het gaat «een juiste uitwerking vormen van de wet». Er zal dus sprake moeten zijn van een vertaling van de normen van de wet naar de informatiepraktijk van de betrokken sector en vooral op die punten waar de behoefte aan meer concrete waarborgen zich het meest voordoet. Uitgangspunt is echter wel een toetsing aan wettelijke regels.

[1] «De Wet persoonsregistraties, norm, toepassing en evaluatie», mr. G. Overkleeft-Verburg, blz. 241–242.

De regels in de gedragscode dienen wel de wettelijke regels te preciseren naar gelang de sector waarvoor de code geldt. De algemene en flexibele normen van de wet dienen in een gedragscode een nauwkeuriger vertaling te krijgen in het licht van de desbetreffende sector. Dit komt ook de rechtszekerheid ten goede. Een gedragscode kan daarom niet volstaan met het grotendeels eenvoudig herhalen van een aantal wettelijke bepalingen. Dit laat onverlet dat desgewenst een aantal wettelijke bepalingen, indien deze zich in de desbetreffende sector niet goed lenen voor een nadere uitwerking, toch volledigheidshalve kunnen worden overgenomen. De code bevat dan binnen de sector een totaalbeeld van de geldende regels.
De term «gedragscode» dient niet te strikt te worden opgevat. Ook gedragscodes die slechts voor een deel betrekking hebben op de verwerking van persoonsgegevens vallen onder de regeling van artikel 25. De term omvat iedere vorm van collectieve zelfregulering met betrekking tot de omgang met persoonsgegevens. Ook gedragsregels kunnen als zodanig worden aangemerkt.

Derde lid

Artikel 15, tweede lid, van de WPR bepaalde dat de kamer het verzoek een code te beoordelen slechts in behandeling behoeft te nemen indien naar haar oordeel de verzoeker of verzoekers representatief zijn voor de betrokken sector, deze sector in de code nauwkeurig is omschreven en de code zorgvuldig, in het bijzonder in genoegzaam overleg met organisaties van belanghebbenden, is voorbereid. In het derde lid is in afwijking van de WPR niet meer als ontvankelijkheidseis gesteld dat de gedragscode in genoegzaam overleg met belanghebbenden moet zijn opgesteld. Blijkens de juridische evaluatie heeft dit onderdeel van de regelgeving aanleiding gegeven tot problemen, vooral wegens de soms gebrekkige organisatiegraad van geregistreerden. Evenmin bevat de richtlijn daartoe een bepaling. De Nederlandse ervaringen liggen hieraan mede ten grondslag. Wel blijft een toets ingebouwd wat betreft de representativiteit van de betrokken sectoren. Deze dient «voldoende» te zijn. Dit biedt de Registratiekamer de mogelijkheid verzoeken om goedkeuring afkomstig van organisaties met een ontoereikend maatschappelijk draagvlak, niet in behandeling te nemen. De sector dient voorts nauwkeurig te zijn omschreven. Het begrip sector kan ruim worden geïnterpreteerd. Het begrip omvat zowel de zelfregulering op sectorniveau als type economische bedrijvigheid alsook aan sectordoorsnijdende algemene gedragscodes betreffende een bepaalde categorie van gegevensverwerkingen. Uiteraard is wel van groot belang dat de werkingssfeer van een gedragscode duidelijk is.
In het derde lid was aanvankelijk ook nog bepaald dat de Registratriekamer opmerkingen van de betrokkenen of van hun vertegenwoordigers in de behandelingsprocedure in ontvangst kan nemen. Ook in artikel 27, tweede lid, van de richtlijn was deze mogelijkheid vermeld. Terecht merkt de kamer in haar advies op dat deze reeds is geregeld in het vierde lid (artikel 3.13 Awb) en is het derde lid daarop aangepast.

Vierde lid

Blijkens artikel 1.3, eerste lid, Awb wordt onder een besluit verstaan een schriftelijke beslissing van een bestuursorgaan inhoudende een publiekrechtelijke rechtshandeling. De vraag kan worden gesteld of de verklaring op grond van het eerste lid, nu deze niet-bindend is voor de rechter, wel kan worden aangemerkt als een rechtshandeling en daarmee een beroep tegen een dergelijke beslising voortvloeit uit de Awb.[1] Uit de wetsgeschiedenis bij artikel 15 WPR blijkt dat de goedkeuringsbeslissing moet worden gekwalificeerd als een advies aan de rechter, te vergelijken

[1] Zie mede blz. 314 «De Wet persoonsregistraties, norm, toepassing en evaluatie».

met een deskundigenbericht in een civiele procedure of een strafproces. Ten einde alle twijfel uit te sluiten wordt voorts in het zevende lid van dat artikel bepaald dat tegen de beslissing van de kamer geen voorziening van administratieve rechtspraak openstaat[1]. In artikel 25 wordt uitdrukkelijk afstand gedaan van deze opvatting. De verklaring wordt in het vierde lid op één lijn gesteld met een besluit in de zin van de Awb. De gelijkschakeling van de verklaring met een besluit in de zin van de Awb doet recht aan het maatschappelijk belang dat wordt gehecht aan een verklaring en op de behoefte verschillen van inzicht aan de rechter te kunnen voorleggen. Deze twee factoren vereisen immers een zorgvuldige voorbereidingsprocedure van de Registratiekamer alvorens tot een verklaring te komen en een bezwaar- en beroepsmogelijkheid tegen de verklaring als die is vastgesteld. De positieve (commerciële) waarde van een goedkeurende verklaring en – anderzijds – de bedrijfsschade die kan ontstaan door de negatieve publieke beeldvorming bij het weigeren van een goedkeurende verklaring door de kamer, moeten niet worden onderschat. Het advies van de Registratiekamer de beroepsmogelijkheid tegen de verklaring van de kamer te heroverwegen heeft derhalve niet geleid tot een wijziging op dit punt.

Door in het vierde lid onderdelen van de Awb van toepassing te verklaren behoeven een aantal voorschriften uit de WPR niet te worden overgenomen. Op grond van het vierde lid is het thans ook mogelijk beroep in te stellen tegen een verklaring van de Registratiekamer. De rechter kan alsdan een rechtens bindend oordeel vellen over de vraag of de code in overeenstemming is met de wettelijke voorschriften. Hiermee wordt gevolg gegeven aan een van de aanbevelingen van de juridische evaluatie.
In het vierde lid is eveneens bepaald dat de besluit van de Registratiekamer naar aanleiding van een verzoek op grond van het eerste lid binnen een redelijk termijn moet worden genomen met dien verstande dat deze termijn niet langer dan dertien weken mag bedragen. Hiermee wordt de Registratiekamer een ruimere termijn gegund dan in artikel 4.13 Awb in zijn algemeenheid ten aanzien van beschikkingen is bepaald. Daarmee komt het voorschrift tegemoet aan de bezwaren van de Registratiekamer tegen de korte termijn van dat artikel. De termijn komt overeen met die welke de kamer gegund is voor het verrichten van een nader onderzoek in het kader van artikel 31 (artikel 32, vierde lid). Wanneer de termijn niet wordt gehaald, kan worden uitgegaan van een fictieve weigering en kan de verzoeker een bezwaarschrift indienen of een beroep instellen.

Vijfde lid

De verklaring van de Registratiekamer geldt voor de termijn waarvoor de code zal gaan gelden met een maximum van vijf jaren. Voor dit maximum is gekozen opdat rekening kan worden gehouden met mogelijk gewijzigde omstandigheden met betrekking tot het gegevensverkeer in de sector. Omdat een aantal wettelijke voorschriften belangenafwegingen voorschrijven is het ook mogelijk dat in de loop van deze vijf jaren de opvatting over een juiste afweging van de betrokken belangen is gewijzigd. Als voorbeeld kan worden gewezen op artikel 8, onderdeel f, van het wetsvoorstel. De bepalingen in de code kunnen dan worden aangepast aan deze gewijzigde opvattingen.
In het vijfde lid is tevens voorzien in de mogelijkheid wijzigingen in eerder goedgekeurde gedragscodes eveneens aan goedkeuring te onderwerpen. De goedkeuring van de wijzigingen kunnen evenwel geen langere geldingsduur hebben dan de goedkeurende verklaring voor de oorspronkelijke gedragscode in zijn geheel.

[1] Memorie van toelichting, blz. 21 en Memorie van antwoord, blz. 55.

Zesde lid

In het zesde lid is neergelegd dat de verklaring van de Kamer geen consequenties heeft voor de rechtskracht van de gedragscode. Aan het karakter van zelfregulering wordt aldus geen afbreuk gedaan. De verklaring krijgt aldus het karakter van een staand deskundigenadvies aan de rechter. Indien voor de rechter een geschil aanhangig zou worden over de toepassing van de wet, dan behelst de verklaring van de Kamer dat naar haar oordeel naleving van de code ook naleving van de wet betekent. Dit oordeel heeft dezelfde rechtskracht als het advies dat hangende een geschil ingevolge artikel 47, tweede lid, aan de Kamer kan worden gevraagd.

Zevende lid

Het zevende lid verwijst naar de procedure voor de vaststelling van communautaire gedragscodes. De goedkeurende verklaring wordt in dat geval afgegeven door de Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens. Deze ontleent haar juridische basis aan artikel 29 van de richtlijn. Zij bestaat uit vertegenwoordigers van de toezichthoudende autoriteiten van ieder van de lidstaten van de Europese Unie. Zij stelt vast of een communautaire gedragscode in overeenstemming is met de ter uitvoering van de richtlijn vastgestelde nationale bepalingen. De vertegenwoordiger van de Registratiekamer in deze Groep zal er voor Nederland in het bijzonder op toezien dat een communautaire gedragscode ook in overeenstemming is met het onderhavige wetsvoorstel.

Achtste lid

Naar aanleiding van het advies van de Registratiekamer is overeenkomstig artikel 15, vierde lid, van de WPR een voorziening opgenomen over de bekendmaking van de verklaring en de code waarop zij betrekking heeft. Door deze bekendmaking verkrijgt de verklaring zijn werking als rechtshandeling. Het voorschrift geldt als een nadere invulling van het algemene bekendmakingsvoorschrift van artikel 3.42 Awb.

Artikel 26

In artikel 26 keert de inhoud van artikel 16 WPR terug. Naar aanleiding van het advies van de Registratiekamer is het bereik van artikel 26 uitgebreid met artikel 13 van dit wetsvoorstel (beveiligingsvoorschift). Artikel 5 van de richtlijn draagt de lid-staten op nader de voorwaarden te bepalen waaronder de verwerkingen van persoonsgegevens rechtmatig zijn. De mogelijkheid om bij algemene maatregel van bestuur sectorgewijs voorschriften te geven, is één van de instrumenten om uitvoering te geven aan deze opdracht. De evaluaties leveren geen aanwijzingen die pleiten tegen het behoud van deze reeds in de WPR gegeven mogelijkheid.

HOOFDSTUK 4 MELDING EN VOORAFGAAND ONDERZOEK

PARAGRAAF 1 DE MELDING

Artikel 27

Eerste lid

Aanmelding heeft tot doel de transparantie van de gegevensverwerking te bevorderen. De handelingsvrijheid van een ieder om voor op zichzelf

gerechtvaardigde doeleinden gegevens te verwerken, wordt ingeperkt door de grondwettelijk gewaarborgde vrijheid van de betrokkene om niet onnodig aan verwerking van hem betreffende gegevens te worden onderworpen. Dit leidt enerzijds tot het materiële voorschrift dat de belangen van de verantwoordelijke en de betrokkene tegen elkaar moeten worden afgewogen; anderzijds tot het procedurele voorschrift dat de afweging controleerbaar dient te zijn. Artikel 18 van de richtlijn bepaalt in het belang van die controleerbaarheid dat – kort samengevat – een verantwoordelijke alvorens over te gaan tot een of meer geautomatiseerde verwerkingen van gegevens voor een bepaald doel, deze dient aan te melden bij een toezichthoudende autoriteit. Dit beginsel is neergelegd in het eerste lid van artikel 27.

Object van aanmelding in artikel 27 is «een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is». De betekenis van het begrip «verwerking van persoonsgegevens» is in deze bepaling van groot belang. Blijkens artikel 1, onderdeel deel b, wordt hiermee gedoeld op elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. In het kader van artikel 1, onderdeel b, is in de toelichting reeds opgemerkt dat onder «geheel van handelingen» moet worden verstaan een bundeling van verwerkingshandelingen die in het maatschappelijk verkeer als een eenheid wordt beschouwd. In het kader van de meldingsverplichting in het onderhavige artikel betekent dit dat het de verantwoordelijke in beginsel vrijstaat niet elke verwerkingshandeling afzonderlijk te melden, maar alleen verwerkingshandelingen gezamenlijk voor zover deze als een «geheel van verwerkingen» in de zin van artikel 1, onderdeel b kunnen worden beschouwd.

Voor melding van een geheel van verwerkingen bestaat te meer aanleiding indien de betreffende verwerkingen voor de verwezenlijking van een en hetzelfde doel of voor verscheidene samenhangende doeleinden zijn bestemd. In dat geval immers zullen de verwerkingen in het maatschappelijk verkeer al gauw als een eenheid kunnen worden beschouwd. De mogelijkheid om verwerkingen gezamenlijk te melden voor zover zij voor verscheiden samenhangende doeleinden zijn bestemd, is uitdrukkelijk in het eerste lid opengesteld. Daarmee wordt rekening gehouden met de praktijk dat verwerkingen nog al eens in een groter verband geschieden ten behoeve van meerdere doeleinden (zie tevens de toelichting bij artikel 7). Artikel 27, eerste lid, beoogt de aanmeldingsplicht in dit opzicht beter hanteerbaar te maken. Aansluitend bij de realiteit van multifunctionele informatiesystemen is het mogelijk meerdere, uiteenlopende doeleinden voor gegevensverwerking vast te stellen. Bij verwerkingen die geschieden voor meerdere, samenhangende doeleinden kan de aanmelding zo worden ingericht dat ze is gerelateerd aan deze samenhangende doeleinden. Het is daarbij niet relevant of deze doeleinden verenigbaar zijn met de doeleinden waarvoor de desbetreffende gegevens zijn verzameld. Het wordt daarmee mogelijk gemaakt informatiesystemen, die zijn opgezet om diensten te verlenen aan burgers of klanten via één loket voor een scala van activiteiten, via één aanmelding af te doen. Een concern met een breed pakket aan diensten, kan zijn informatiesysteem met behulp van een centrale verwijzingsindex zo inrichten dat enkele medewerkers, wanneer zij de uiteenlopende gegevens behoeven om klanten te woord te staan, uit dit ene informatiesysteem kunnen putten. Voor een dergelijk systeem kan worden volstaan met een enkele aanmelding.

Het criterium inzake de samenhangende doeleinden dient uitdrukkelijk los te worden gezien van de materiële voorschriften van de wet. In artikel 4 WPR wordt thans bepaald dat een persoonsregistratie slechts wordt aangelegd voor «een bepaald doel». Artikel 7 van dit wetsvoorstel verwoordt dezelfde norm ook uitdrukkelijk voor verwerkingen. Dat artikel

bepaalt dat persoonsgegevens voor welbepaalde doeleinden kunnen worden verkregen. In aansluiting hierop bepaalt artikel 9 vervolgens dat persoonsgegevens niet mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen. Deze verenigbaarheidseis geldt echter niet in het kader van de aanmeldingsprocedure: alsdan geldt alleen de voorwaarde dat de doeleinden in het belang waarvan de verwerkingen moeten geschieden, samenhangend zijn. Het materieelrechtelijke voorschrift van verenigbaarheid op grond van artikel 9 speelt dus geen rol bij de aanmeldingsprocedure, hetgeen tot een vermindering van het aantal aanmeldingen leidt. Het al dan niet geoorloofd zijn van de onderscheidene verwerkingen die worden aangemeld wordt dus getoetst aan een ander kader dan de vraag of de aanmelding op een correcte wijze is uitgevoerd. Deze versoepeling die geldt ten aanzien van de aanmeldingsplicht doet niets af aan de plicht van de verantwoordelijke met betrekking tot de onderscheidene verwerkingen de voor hem geldende materieelrechtelijke voorwaarden in acht te nemen.
In paragraaf 9 van het algemeen deel van deze toelichting is reeds uitgebreid ingegaan op de verschillen tussen de aanmeldingsprocedure, zoals geregeld in de WPR en de procedure zoals voorgesteld in dit wetsvoorstel. In aanvulling hierop zij nog het volgende opgemerkt. Anders dan in de artikelen 21 en 26 van de WPR wordt gesteld, heeft de aanmelding in de WBP strikt genomen niet meer het karakter van zelfregulering op het niveau van de individuele verantwoordelijke. In de WBP houdt de melding aan de Registratiekamer in de eerste plaats een feitelijke beschrijving van de desbetreffende gegevensverwerking in. Onder het onderhavige wetsvoorstel is een handelen in strijd met de aanmelding onder omstandigheden het niet-nakomen van de plicht tot melding van een wijziging. Het gaat meer om een procedurevoorschrift strekkende tot transparantie dan om een normering op het niveau van de individuele gegevensverwerking. In de praktijk zal het verschil met de huidige situatie echter niet groot zijn. Het melden van een feitelijke beschrijving omtrent de wijze waarop de gegevens worden verwerkt, impliceert dat de verantwoordelijke in beginsel ook dienovereenkomstig zal moeten handelen.
Het vervallen van de reglementsplicht heeft het voordeel dat het soms kunstmatige onderscheid tussen twee regimes op grond van de WPR vervalt. Het opstellen van een reglement of enige andere vorm van regeling is echter in de praktijk een goede methode gebleken om de werking van een persoonsregistratie te beschrijven. Het vervallen van de reglementsplicht behoeft dus niet te leiden tot het achterwege laten van dergelijke vormen van beschrijving van gegevensverwerking.

Tweede lid

Volgens artikel 18, eerste lid, van de richtlijn heeft de meldingsverplichting betrekking op «een of meer volledig of gedeeltelijk geautomatiseerde verwerkingen van gegevens». Niet geautomatiseerde verwerkingen vallen hierbuiten. Het vijfde lid van dat artikel geeft de Lid-Staten de mogelijkheid te bepalen dat sommige of alle handmatige verwerkingen van persoonsgegevens moeten worden aangemeld, eventueel in vereenvoudigde vorm. Van deze voorziening wordt geen gebruik gemaakt ondanks het feit dat uit de juridische evaluatie is gebleken dat een groot aantal meldingen juist betrekking heeft op handmatige bestanden. Handmatige verwerkingen zijn immers vormen van gegevensverwerking die in de regel minder bedreigend zijn voor de persoonlijke levenssfeer. In paragraaf 9 van het algemeen deel van deze toelichting is al opgemerkt dat om die reden er voor gekozen is deze gegevensverwerkingen vrij te stellen van de aanmeldingsprocedure. Voor zover handmatige verwerkingen wel bedreigend zijn, is het wenselijk deze te onderwerpen aan

voorafgaand toezicht. Artikel 31 geeft hierover nadere regels. Enkel in dit geval is het zinvol handmatige verwerkingen te melden bij de Registratiekamer.
Ook ten aanzien van niet geautomatiseerde verwerkingen geldt dat de verantwoordelijke de mogelijkheid heeft verwerkingen die plaatsvinden voor meerdere, samenhangende doeleinden als zodanig te melden. Verwezen wordt naar hetgeen hieromtrent is opgemerkt onder het eerste lid van dit artikel.
Gesteld kan worden dat voor de handmatig gevoerde bestanden van persoonsgegevens wat betreft de meldingsplicht een apart regime geldt. Bij de handmatige bestanden wordt uitgegaan van een tweedeling: in beginsel vrijstelling tenzij sprake is van voorafgaand onderzoek. Bij de geautomatiseerde verwerking daarentegen kan sprake zijn van een drieslag: voorafgaand onderzoek, melding en vrijstelling.
Het in beginsel niet behoeven aan te melden van handmatige verwerkingen leidt tot een vermindering in transparantie dat in zekere zin echter weer gecompenseerd wordt door het voorschrift van artikel 30, derde lid. Hierin is bepaald dat een verantwoordelijke verplicht is aan een ieder die daarom verzoekt de informatie te verstrekken die grotendeels overeenkomt met de informatie die moet worden verstrekt bij aanmelding van de verwerking (artikel 28, eerste lid, onderdelen a tot en met e).

Derde lid

In artikel 28, tweede lid, van de richtlijn is voorzien in de mogelijkheid voor de Lid-Staten een vereenvoudige aanmelding of een vrijstelling van de aanmeldingsplicht in hun wetgeving op te nemen. Vereenvouding of vrijstelling van de aanmelding is mogelijk voor nader te omschrijven categorieën van verwerkingen waarbij inbreuk op de rechten en vrijheden van de betrokkenen onwaarschijnlijk is. Voorts kan aanmelding bij een functionaris voor de gegevensbescherming in de plaats komen van de aanmelding bij de toezichthoudende autoriteit.
Artikel 29 geeft een wettelijke basis voor een vrijstelling van de aanmeldingsplicht voor nader bij algemene maatregel van bestuur te omschrijven categorieën van verwerkingen. In het belang van de eenvoud en overzichtelijkheid van de aanmeldingssystematiek is er van afgezien in de WBP een vorm van vereenvoudigde aanmeldingen op te nemen. De behoefte daaraan wordt tevens minder groot geacht gezien de voorziening in artikel 27, derde lid. In dit artikel is namelijk de mogelijkheid opgenomen de verwerking aan te melden bij een functionaris voor de gegevensbescherming in plaats van bij de Registratiekamer. Dat de Lid-Staten de mogelijkheden tot vrijstelling van het eerste en het tweede gedachtenstreepje van artikel 18, tweede lid, cumulatief kunnen gebruiken, blijkt uit de keuzemogelijkheid die besloten ligt in de clausule «en/of» aan het slot van het eerste gedachtenstreepje. De onderhandelingen in de desbetreffende raadswerkgroep over dit punt hebben geresulteerd in de aldus tot stand gekomen tekst van de richtlijn.
Volgens de WPR moet melding plaatsvinden aan de Registratiekamer; in de WBP kan deze melding dus worden vervangen door een melding aan de functionaris. Dit betekent dat vrijgestelde gegevensverwerkingen die niet bij de Registratiekamer aangemeld moeten worden, ook niet bij de functionaris te hoeven worden gemeld. De plicht om te melden rust op de verantwoordelijke. Deze heeft dan ook de vrije keuze of hij wil melden bij de Registratiekamer of de functionaris, indien deze binnen het verband waarbinnen de verantwoordelijke werkt is aangesteld. Voor de verantwoordelijke bestaat de mogelijkheid om zich aan één van deze twee keuzemogelijkheden te binden. Dit kan bijvoorbeeld door in de vereniging van verantwoordelijken een functionaris aan te stellen, terwijl in de statuten van de vereniging is opgenomen dat de leden verplicht zijn

wanneer zij persoonsgegevens verwerken, dit te melden bij de functionaris. Artikel 2:34a BW opent hiertoe de mogelijkheid.
Het derde lid verplicht tot aanmelding van een voorgenomen verwerking, dat wil zeggen dat de aanmelding dient te geschieden alvorens tot de verwerking wordt overgegaan. Omdat «verwerking» ook betrekking heeft op het verzamelen, houdt dit in dat de verantwoordelijke voordat hij de beschikking krijgt over persoonsgegevens, de verwerking moet melden. Dit geldt eveneens voor de niet geautomatiseerde verwerkingen die vallen onder het tweede lid.
Daar het meldingenbestand van de Registratiekamer en van de functionaris beide openbaar zijn, kan iedereen, de functionarissen niet uitgezonderd, nagaan of een verantwoordelijke gemeld heeft dat hij persoonsgegevens verwerkt. Denkbaar is dat de Registratiekamer bepaalde afspraken maakt met een functionaris over de uitwisseling van relevante meldingen. Dergelijke afspraken kunnen nodig zijn voor het goed kunnen uitoefenen van beider taak. Is aan dit criterium voldaan, dan kunnen ook de meldingen van natuurlijke personen worden uitgewisseld en verwerkt. De verantwoordelijke dient daarover dan wel in zijn hoedanigheid van betrokkene te worden geïnformeerd, bijvoorbeeld in samenhang met de ontvangstbevestiging van zijn melding.
Voor de regeling van het instituut van de functionaris voor de gegevensbescherming zij verwezen naar artikel 62 tot en met 64 van dit wetsvoorstel.

Artikel 28

Eerste lid

Dit artikel vermeldt de gegevens die bij aanmelding moeten worden verstrekt. Het artikel geeft uitvoering aan artikel 19 van de richtlijn. Het vormt een vereenvoudiging ten opzichte van de artikelen 20 en 24 WPR daar er minder gegevens hoeven te worden aangemeld. Verder is de procedure voor de aanmelding van wijzigingen vereenvoudigd. Het eerste lid bevat een opgave van de te melden gegevens.
Blijkens onderdeel a moet de identiteit van de verantwoordelijke worden gemeld alsmede de gegevens die nodig zijn om met hem te kunnen communiceren. Deze gegevens zijn nodig om met de verantwoordelijke in contact te kunnen treden bij vermeend onrechtmatig gebruik van door hem verwerkte gegevens. Indien bij de verwerking meerdere verantwoordelijken zijn betrokken, dient de identiteit van alle bij de verwerking betrokken verantwoordelijken en, indien dit het geval is, van hun vergenwoordigers te worden gemeld.
Blijkens onderdeel b moeten het doel of de samenhangende doelen van de verwerking worden gemeld. Zij bepalen de aard van de gegevensverwerking en vormen het criterium aan de hand waarvan de omgang met de persoonsgegevens wordt getoetst. In de toelichting bij artikel 27, eerste lid, is reeds gemeld dat de melding betrekking kan hebben op verwerkingen ten behoeve van samenhangende doeleinden, ongeacht of deze onderling verenigbaar zijn.
Onderdeel c schrijft voor dat de categorieën van betrokkenen en de omtrent hen te verwerken gegevens worden gemeld.
Onderdeel d heeft betrekking op de ontvangers van de gegevens. Evenals onder de WPR gaat het daarbij niet alleen om de gevallen dat wordt verstrekt aan derden, doch eveneens om de verstrekking aan personen of afdelingen binnen de organisatie van de verantwoordelijke. Deze verstrekkingen dienen zo mogelijk individueel te worden vermeld. Gaat het evenwel om groepen van ontvangers, dan moeten deze worden beschreven. Dit betekent dat de beschrijving een zo nauwkeurig mogelijk beeld moet geven van de categorieën van ontvangers. De bedoeling is dat het helder en doorzichtig wordt hoe de gegevens worden verwerkt.

Uit onderdeel e blijkt de oorspronkelijk Europese herkomst van de regeling. Dit onderdeel betreft de overdracht van gegevens naar landen buiten de Europese Unie. Naar aanleiding van de vraag van de Registratiekamer in haar advies wordt hier opgemerkt dat het woord «overdracht», dat is ontleend aan artikel 19, eerste lid, onder e, van de richtlijn, op één lijn kan worden gesteld met het woord «doorgifte» in de artikelen 76 en 77 van dit wetsvoorstel. Om te kunnen voldoen aan artikel 25, derde lid, van de richtlijn is het nodig zicht te krijgen op deze verstrekkingen teneinde de regering in staat te stellen de Europese Commissie te verwittigen van gevallen waarin geen passend niveau van bescherming in het derde land aanwezig wordt geacht. Het maakt a contrario duidelijk dat het gegevensverkeer met landen binnen de Unie niet aan een dergelijk bijzonder toezicht is onderworpen.
Onderdeel f strekt ertoe de Registratiekamer in staat te stellen een eerste indruk te krijgen van het beveiligingsniveau. De verantwoordelijke dient een algemene beschrijving te geven van de voorgenomen maatregelen ter beveiliging van de gegevsnverwerkingen. Te denken valt aan de mededeling dat de toegang tot het informatiesysteem is beveiligd met een code, bestaande uit een aantal letters of cijfers, met vermelding van de regelmaat waarmee deze moet worden gewijzigd. Ook is denkbaar dat door de Registratiekamer een soort checklist van beveiligingsmaatregelen wordt opgesteld. Middels het invullen van deze checklist zou de Registratiekamer ook een beeld kunnen krijgen van de voorgenomen beveiligingsmaatregelen door de verantwoordelijke en is voldaan aan dit onderdeel van de meldingsplicht. Met de ontwikkelingen van de techniek wijzigen zich uiteraard voortdurend de maatregelen die passend moeten worden geacht uit een oogpunt van beveiliging want wat vandaag veilig is, is dat morgen niet meer. Zolang dergelijke aanpassingen voldoen aan de algemene beschrijving die is opgenomen in de melding, hoeft deze niet opnieuw te worden gemeld. De vertrouwelijkheid van beveiligingsmaatregelen leidt ertoe dat de melding ingevolge dit onderdeel niet van dien aard kan zijn dat daarop meer dan een voorlopig oordeel kan worden gebaseerd omtrent het wel of niet passend zijn van de beveiligingsmaatregelen. Uit de aard van de materie vloeit voort dat omtrent de beveiligingsmaatregelen geheimhouding is geboden. Dit onderdeel van de melding is dan ook met de nodige waarborgen omkleed. Het is allereerst uitgezonderd van de opname in het in artikel 30, eerste lid, bedoelde openbare register van aanmeldingen. Seperate aanmelding verdient hier de voorkeur ten einde de noodzakelijke afscherming te kunnen realiseren. Eveneens verstrekt de verantwoordelijke dan wel de functionaris bij wie in plaats daarvan de melding heeft plaatsgevonden, ingevolge artikel 30, derde lid, hierover geen informatie indien iemand hem daarom verzoekt. Zou een verdergaande bekendmaking plaatsvinden, dan zou zulks uiteraard, hoe globaal dit onderdeel van de melding ook is, afbreuk kunnen doen aan de effectiviteit van de beveiliging.

Tweede lid

In de toelichting bij artikel 27, eerste lid, is reeds gemeld dat de melding betrekking kan hebben op verwerkingen ten behoeve van samenhangende doeleinden, ongeacht of deze onderling verenigbaar zijn. Artikel 9 bevat de materiële norm dat persoonsgegevens niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Voor de vraag of de verwerkingen op zich geoorloofd zijn dient aan deze norm te worden getoetst. Onderling samenhangend is een meer omvattend begrip dan onderling verenigbaar. Teneinde in dergelijke gevallen toch in voorkomend geval de toets van het gebruik verenigbaar met het oorspronkelijk doel waarvoor is verzameld, te kunnen aanleggen voorziet het tweede lid een aparte voorziening. De melding van de

verantwoordelijke dient eveneens het doel of de doeleinden waarvoor de gegevens of de categorieën van gegevens zijn verzameld, te bevatten. Aanvankelijk was een uitzondering op deze verplichting opgenomen voor de gevallen dat het doel waarvoor de gegevens zijn verzameld, uit de aard van de gegevens of de aard van de verwerking voortvloeit. Zo zal uit een registratie van een bank of een verzekeraar zonder meer de aard van het contract blijken in welk verband de gegevens zijn verzameld. Die aard is bepalend voor het verenigbaar gebruik. Ook wanneer het gaat om een gegevensverwerking voor een enkel doel, blijkt uit dit doel waartoe de gegevens zijn verzameld. Dit is de situatie onder de WPR waarbij blijkens artikel 4 een registratie wordt gedefinieerd volgens een eenduidig doel. De Registratiekamer merkt in haar advies op dat deze uitzondering in de praktijk veel problemen zal geven bij het verrichten en het toetsen van de aanmelding. Uit een oogpunt van duidelijkheid meent zij dat een onvoorwaardelijke verplichting de voorkeur verdient. Omdat de evidente doelen waarop de uitzondering ziet zich ook gemakkelijk laten omschrijven is het advies overgenomen en bevat het tweede lid nu een onvoorwaardelijke verplichting.
Het tweede lid heeft tot gevolg dat bijvoorbeeld bij multifunctionele informatiesystemen met uiteenlopende, mogelijk met elkaar onverenigbare doeleinden, apart duidelijk moet worden gemaakt voor welk doel de daarin opgenomen gegevens zijn vergaard. De verschillende vormen van gebruik, de in dat verband te verlenen autorisaties aan verschillende categorieën van medewerkers en de verwerkingsduur dienen aan dit doel te worden getoetst. Het gebruik van persoonsgegevens die voor de uitvoering van het ene contract zijn verkregen, zijn dus niet altijd zonder meer te gebruiken in het kader van de voorbereiding van een ander contract, zelfs niet binnen eenzelfde branche. Het is wellicht nuttig hiervan een voorbeeld te geven. Wanneer bij voorbeeld een verzekeraar zowel een ziektekosten- als een levensverzekering aanbiedt, dan kunnen de daartoe gevoerde gegevensverwerkingen worden aangemeld als één gegevensverwerking met meerdere samenhangende doeleinden. Uit dat ene informatiesysteem kan worden geput bij de beantwoording van vragen van de klant. Het gebruik van de gegevens van de eerste verzekering, in dit geval de ziektekostenverzekering, voor het bepalen van de hoogte van de premie van de tweede, de levensverzekering, is evenwel een vorm van onverenigbaar gebruik van deze gegevens. De vraag van verenigbaar gebruik is daarom niet beantwoord met de vraag van samenhangende doeleinden. Een afzonderlijke beschrijving van de ontvangers, uitgesplitst naar de verschillende categorieën van opgenomen persoonsgegevens, blijft noodzakelijk.
Het voorgaande is eveneens van belang voor organen met een publieke taak. Het streven verkokering binnen de sectoren van de overheid tegen te gaan heeft geleid tot een omvangrijke uitwisseling van persoonsgegevens tussen verschillende diensten met elk een andere taakopdracht. Voorbeelden hiervan zijn het contact tussen de uitvoeringsorganen van de sociale verzekeringen, de sociale diensten van de gemeenten en de fiscus met het oog op de het tegengaan van fraude via bijvoorbeeld het RINIS-systeem; de uitwisseling van persoonsgegevens tussen de organen betrokken bij de justitiële keten om stagnatie tegen te gaan; het streven om onrechtmatig in Nederland verblijvende vreemdelingen uit te sluiten van een aantal overheidsvoorzieningen. Bij deze voorbeelden zijn voor uiteenlopende maar samenhangende doelen informatiesystemen ingericht, veelal door de inrichting van een centrale verwijzingsindex, al dan niet door tussenkomst van de gemeentelijke basisadministratie. Het sociaal-fiscaal nummer speelt in dit verband de rol van koppelingsinstrument. Niet alle daarin opgenomen gegevens kunnen zonder nadere toets ook voor elk van de doelen van het informatiesysteem worden gebruikt.

Derde lid

Het derde lid geeft invulling aan de opdracht van artikel 19, tweede lid van de richtlijn, namelijk dat een procedure moet worden voorgeschreven voor het melden van wijzigingen. Wijzigingen in de gegevens van de verantwoordelijke, bij voorbeeld een verhuizing, moeten binnen een week worden meegedeeld. Zodra de woonplaats van de verantwoordelijke niet meer bekend is, is het ook niet meer mogelijk iemand aan te spreken op de naleving van de normen. Gelet op de strafbaarstelling van het niet nakomen van de verplichting ingevolge artikel 28 is de norm die aanvankelijk was opgenomen, namelijk dat deze wijzigingen terstonds moeten worden gemeld, geconcretiseerd tot: binnen een week. Ook de Registratiekamer adviseert een dergelijke concretisering.
In het derde lid is tevens, teneinde de administratieve belasting zoveel mogelijk te verminderen, neergelegd dat wijzigingen in de overige gegevens slechts behoeven te worden gemeld, indien na verloop van tijd blijkt dat deze van meer dan incidentele aard zijn. De gegevensverwerking dient eens per jaar daarop te worden gecontroleerd. Uit de evaluaties van de WPR is immers gebleken dat het steeds en voortdurend melden van elke wijziging in de werking van de registratie, in de praktijk op problemen stuit. Zo kan het voorkomen dat een verstrekking wordt gedaan voor een ander, zij het verenigbaar doel dan waarvoor de gegevens worden verwerkt. Indien blijkt dat zulks vaker voorkomt, zal op een gegeven moment moeten worden geconstateerd dat dit andere doel, feitelijk mede een met het eerste samenhangend doel van de verwerking is. Het is dan nodig van deze feitelijkheid opgave te doen.
Deze voorschriften sluiten tot op zekere hoogte aan bij artikel 20 WPR. Onder de WPR kon het voorkomen dat in afwijking van de aanmelding, ook incidenteel gegevens aan derden worden verstrekt, bij voorbeeld om een dringende en gewichtige reden of in verband met wetenschappelijk onderzoek. Artikel 11 WPR beperkt evenwel de verstrekking aan derden voor andere doeleinden. Het onderhavige wetsvoorstel biedt meer souplesse. Bij de derdenverstrekking is sprake van een minder strikte doelbinding. Omdat een melding bij elke doelafwijking zeer onderhoudsintensief is, is verder bepaald dat slechts wanneer de doelafwijking structureel wordt door meerdere verstrekkingen, dit behoeft te worden gemeld.

Vierde lid

De beoordeling of een wijziging al dan niet structureel is kan pas achteraf worden vastgesteld. Zolang de wijzigingen niet zijn doorgevoerd, dient de verantwoordelijke ingevolge het vierde lid de gegevens omtrent verwerkingen die niet geheel overeenstemmen met de melding, zelf op te slaan. Achteraf is aldus steeds vast te stellen aan bijvoorbeeld welke (categorieën van) ontvangers gegevens zijn verstrekt, dan wel of gegevens zijn doorgegeven aan landen buiten de Unie. Deze procedure voor melding van wijzigingen waarborgt aldus de transparantie van de gegevensverwerking.
De Registratiekamer adviseert de beperking tot wijzigingen van meer dan incidentele aard in het derde lid te laten vervallen. Het vierde lid zou dan moeten worden verbreed tot het vastleggen en bewaren van alle afwijkingen. Het advies van de kamer is slechts ten dele opgevolgd: enkel voorzover het het vierde lid betreft. In het belang van de transparantie verplicht het vierde lid thans de verantwoordelijke alle verwerkingen die afwijken van hetgeen is aangemeld (op de identiteit van de verantwoordelijke na) vast te leggen en te bewaren. Op deze wijze zal hij ook tijdens de periodieke controle van de gegevens die zijn aangemeld beter in staat zijn te beoordelen of een wijziging die heeft plaatsgevonden als structureel moet worden beschouwd. Het advies ten aanzien van het derde lid stuit af

op de ervaringen die in de praktijk zijn opgedaan ten aanzien van de aanmeldingsplicht, waarover hier boven al naar is verwezen. Een daadwerkelijk naleven van de aanmeldingsplicht is gebaat bij een zo min mogelijke administratieve belasting.

Vijfde lid

Er kan in de toekomst een behoefte ontstaan nader regels te stellen ten aanzien van de wijze waarop de melding wordt gedaan. Nieuwe technologische ontwikkelingen kunnen te zijner tijd wellicht in het kader van de meldingsprocedure worden ingezet en een regeling behoeven.

Artikel 29

Eerste lid

Indien aan de meldingsplicht onverkort de hand zou worden gehouden, zou afbreuk worden gedaan aan de daarmee beoogde transparantie. Er zouden vele gegevensverwerkingen moeten worden aangemeld waarvan het bestaan evident is. Het gevolg zou slechts zijn dat de gegevensverwerkingen waarvan het wel nodig is dat zij in beeld worden gebracht, ondersneeuwen. Het is daarom nodig de bekende, veel voorkomende vormen van gegevensverwerking waarvan het bestaan in het algemeen bekend mag worden verondersteld, van de meldingsplicht vrij te stellen. De meldingsplicht heeft tot doel dat de verantwoordelijke geprikkeld wordt om zich rekenschap te geven van de doeleinden waarvoor hij persoonsgegevens wil verwerken en verslag te doen van de overwegingen welke persoonsgegevens noodzakelijk zijn voor het bereiken van het doel en van het gebruik van de gegevens in verband met dat doel. Deze functies blijven behouden doordat de doelstelling, de aard van de gegevens en de verstrekkingen in de vrijstelling worden beschreven. De beantwoording van de vraag naar het doel van de verwerking ligt dan besloten in de toets van de verantwoordelijke of wel of niet moet worden aangemeld. Worden de gegevens verwerkt in afwijking van de vrijstelling, dan herleeft de meldingsplicht.
Het is de bedoeling een groot deel van de vele vormen van gegevensverwerking vrij te stellen. Artikel 18, tweede lid, van de richtlijn bepaalt dat vrijstelling van de aanmeldingsplicht mogelijk is wanneer inbreuk op de rechten en vrijheden van de betrokkenen door de verwerkingen onwaarschijnlijk is. Dit betekent dat een zodanige inbreuk bij de vrij te stellen verwerkingen en met inachtneming van de aan de vrijstelling te verbinden voorwaarden onwaarschijnlijk dient te zijn. Uitgangspunt is derhalve of de inbreuk op de persoonlijke levenssfeer onwaarschijnlijk is, bij voorbeeld gegevensverwerkingen die standaard zijn en waarvan in het algemeen bekend is dat deze voorkomen. Als voorbeeld kan de verwerking van persoonsgegevens die voorkomen in archiefbescheiden die op grond van de Archiefwet 1995 naar een archiefbewaarplaats zijn overgebracht, worden genoemd. Bij verwerking van gevoelige gegevens kan de nadere precisering van de vrijgestelde verwerkingen tot de conclusie leiden dat een inbreuk daardoor onwaarschijnlijk is geworden. De vrijstelling van melding van bepaalde verwerkingen van gevoelige gegevens is derhalve niet uitgesloten.
Het is evenwel de bedoeling verwerkingen die geschieden zonder medeweten van de betrokkene niet vrij te stellen. In dergelijke gevallen kan de inbreuk op de persoonlijke levenssfeer bezwaarlijk als onwaarschijnlijk worden aangemerkt. Wanneer bij voorbeeld een werkgever, een verantwoordelijke in de zin van het wetsvoorstel, zijn medewerkers een informatiesysteem voor hun werk aanbiedt en daarbij gegevens opslaat die tot individuele medewerkers herleidbaar zijn, dan dient hij hen daarover in beginsel te informeren. De ondernemingsraad is daarvoor een

geschikt forum. Er zijn omstandigheden denkbaar dat informatie achterwege moet blijven. Een voorbeeld is een concrete verdenking van fraude die via gegevensverwerking kan worden opgelost, terwijl andere opsporingsmiddelen niet als reëel alternatief in aanmerking komen. Wanneer niet reeds in het algemeen vooraf kenbaar is gemaakt dat voor een dergelijk doel gegevens kunnen worden verwerkt, dient een dergelijke onopgemerkte gegevensverwerking middels een melding plaats te vinden. De functionaris dient hierop in het bijzonder controle te kunnen uitoefenen indien de betrokkenen zelf wegens onwetendheid omtrent de gegevensverwerking hiertoe niet in staat zijn.
Vrijstelling heeft een verminderde transparantie tot gevolg. Een compensatie hiervoor ligt in de verplichting van de verantwoordelijke ingevolge artikel 30, derde lid, een ieder, dus ongeacht of het gaat om een betrokkene of niet, desgevraagd in kennis te stellen van de gegevens die hij verwerkt. Dit betekent dat de verantwoordelijke een overzicht moet kunnen geven van de gegevensverwerkingen die onder zijn verantwoordelijkheid plaatsvinden. Is een dergelijk overzicht niet meteen voorhanden, dan zal hij naar aanleiding van een concreet verzoek nader onderzoek moeten verrichten. Hij kan zich niet beroepen op het feit dat hij zelf niet op de hoogte is.

Tweede lid

In de WBP zijn er in het systeem van vrijstellingen vergeleken met de WPR enige veranderingen aangebracht. De WPR kent een open systeem van nader aan vrij te stellen registraties te verbinden voorwaarden. Er zijn in de WPR geen beperkingen aan de nadere normen die bij algemene maatregel van bestuur voor de vrijgestelde registraties kunnen worden vastgesteld. Op grond van de WBP is het strikt genomen niet meer mogelijk dergelijke nadere normen te stellen. In de WBP worden vaste criteria gegeven waaraan een verwerking moet voldoen om vrijgesteld te worden. De uitputtende opsomming van vaste criteria bestaat uit: de doeleinden, de aard van de gegevens, categorieën betrokkenen, de verstrekking en de bewaartermijnen. Er is sprake van deregulering in die zin dat de regering wordt gebonden aan een aantal limitatief omschreven criteria die kunnen worden gebruikt om de vrij te stellen gegevensverwerkingen te omschrijven. De regering is niet bevoegd om in het vrijstellingsbesluit criteria te geven die buiten deze opsomming vallen. Er is aan de andere kant minder souplesse in die zin dat ten aanzien van de vrij te stellen categorieën, deze criteria ook alle aan de orde moeten komen. Theoretisch gaat het hierbij niet om een nadere normering, maar om een aanduiding van de omvang van de vrijstelling. In de praktijk werkt evenwel deze indirecte weg toch normerend.

Derde lid

In het derde lid is de mogelijkheid opgenomen voor bijzondere opsporingsdiensten een apart regime te treffen in het belang van de opsporing van strafbare feiten. Het is de bedoeling een regime vast te stellen vergelijkbaar met dat van artikel 13 van de Wet politieregisters en artikel 8 van het besluit met betrekking tot tijdelijke registers. Daarbij is in het onderhavig wetsvoorstel in ieder geval vastgelegd dat voor dergelijke vrijgestelde gegevensverwerking het gesloten verstrekkingenregime van de Wet politieregisters van overeenkomstige toepassing dient te zijn. De richtlijn voorziet niet in een dergelijke mogelijkheid. Voor zover echter bijzondere opsporingsdiensten niet onder het communautaire recht vallen, kan van deze bepaling gebruik worden gemaakt. De nationale wetgever behoudt, uiteraard binnen de grenzen van het internationale recht, de vrijheid om een dergelijke regel te stellen.

Vierde lid

In het vierde lid ten slotte is een algehele vrijstelling geregeld voor openbare registers die bij de wet zijn ingesteld. Artikel 18, derde lid, van de richtlijn biedt daartoe uitdrukkelijk de mogelijkheid. Het gaat om registers met een specifieke grondslag in de formele wet die in het Staatsblad is gepubliceerd en die op grond van diezelfde wet voor een ieder vrij toegankelijk zijn. Onder die omstandigheden bestaat geen behoefte aan een afzonderlijke meldingsverplichting.
In artikel 1, onder g, van de richtlijn wordt van het begrip «ontvanger» uitgezonderd instanties waaraan gegevens op kunnen worden medegedeeld in het kader van een bijzondere onderzoeksopdracht. Het uitzonderen van dergelijke verstrekkingen van het begrip «ontvanger» heeft met name consequenties voor de meldingsplicht en de informatieplicht van de verantwoordelijke. Aangezien de verstrekkingen niet worden aangemerkt als verstrekkingen aan een ontvanger gelden immers de desbetreffende artikelen niet (artikel 10, onderdeel c, artikel 11, eerste lid, onderdeel c, en 19, eerste lid, onderdeel d, van de richtlijn). Het voorschrift is in het onderhavige wetsvoorstel uitgewerkt in de zin dat het gaat om «verstrekkingen aan een bestuursorgaan ingevolge een wettelijke verplichting». Deze verstrekkingen zijn immers kenbaar en daarmee transparant omdat ze zijn gebaseerd op een wettelijke verplichting.
Met het oog op de strekking van het voorschrift is er voor gekozen het niet te implementeren als een uitzondering op de begripsomschrijving van «ontvanger» maar op te nemen als een uitzondering op de bepalingen waarop het effect zou hebben. Het voorschrift is daarom opgenomen in de vorm van een uitzondering op de meldingsplicht (artikel 29, vierde lid) omdat het noodzakelijk is hierop een specifieke uitzondering te bedingen. Een dergelijke uitzondering is niet noodzakelijk ten aanzien van de informatieplicht van de verantwoordelijke (artikelen 33 en 34) omdat de betrokkene van deze informatie op de hoogte kan worden geacht.
Een voorbeeld van een verstrekking die op grond van het vierde lid van de meldingsplicht is uitgezonderd is de verstrekking door publiekrechtelijke rechtspersonen van persoonsgegevens aan de Dienst voor het Kadaster ten behoeve van de bijhouding van de kadastrale registratie (artikel 54, derde lid, van de Kadasterwet).

Artikel 30

Eerste en tweede lid

De transparantie van de gegevensverwerking vereist dat de meldingen bij de Registratiekamer en de functionaris voor de gegevensbescherming openbaar zijn. Deze norm geeft uitvoering aan artikel 21, tweede lid, respectievelijk eerste lid, van de richtlijn. De gemelde gegevens liggen daarin voor een ieder kosteloos ter inzage, met uitzondering van de gegevens die betrekking hebben op de beveiliging. Onder de WPR was feitelijk het register van aangemelde registraties ook van het begin af reeds openbaar. Na het toepasselijk worden van de Wet openbaarheid van bestuur op de Registratiekamer kreeg deze openbaarheid een juridische onderbouwing.

Derde lid

De verplichting informatie over gegevensverwerkingen op te nemen in het register, geldt slechts voor de meldingsplichtige gegevensverwerkingen. Indien het gaat om vrijgestelde vormen van verwerking, dan is degeen die inlichtingen daarover wil hebben, aangewezen op de verantwoordelijke. Elke verantwoordelijke dient desgevraagd inlichtingen te verstrekken over door hem verwerkte persoonsgegevens voor zover het gaat om vrijge-

stelde verwerkingen. Heeft de verantwoordelijke zelf een functionaris in zijn bedrijf aangesteld, dan behoort het tot de mogelijkheden dat deze alle inlichtingen over gegevensverwerkingen van de verantwoordelijke inventariseert. De wettekst dwingt hiertoe evenwel niet. Het is ook mogelijk de inlichtingen over de gegevensverwerking pas naar aanleiding van een daartoe strekkend verzoek te verzamelen. Het derde lid geeft uitvoering aan artikel 21, derde lid, van de richtlijn.
Naar aanleiding van het advies van de Registratiekamer is de tekst van het derde lid aangepast. Aanvankelijk betrof de informatieverplichting van de verantwoordelijke de plicht de inlichtingen als bedoeld in artikel 28, eerste lid, onderdelen a tot en met e, met betrekking tot al dan niet geautomatiseerde verwerkingen, te verstrekken indien althans deze inlichtingen niet anderszins openbaar zijn gemaakt. In navolging van artikel 21, derde lid, is het bereik van het voorschrift thans beperkt tot het verschaffen van deze inlichtingen met betrekking tot de van de aanmelding vrijgestelde gegevensverwerkingen. Hiermee wordt beter aangesloten bij de bedoelingen van het voorschrift. Voorkomen moet worden dat het misverstand ontstaat dat de informatieverplichting ziet op alle soorten verwerkingen. Eveneens is het voorschrift nu van een sanctie voorzien. Indien de verantwoordelijke een bestuursorgaan is, geldt de beslissing tot afwijzing van een verzoek als een besluit in de zin van de Algemene wet bestuursrecht (artikel 45) en kan de Awb-rechtsgang worden gevolgd. Is de beslissing genomen door een ander dan een bestuursorgaan dan geldt de procedure van artikel 46.
De vraag rijst hoe nauwkeurig een verzoek om inlichtingen omtrent gegevensverwerking moet zijn. Een onbestemde vraag naar een opgave van alle gegevensverwerkingen van een verantwoordelijke kan voor de beantwoording daarvan van deze verantwoord een onevenredige inspanning vergen. Hij kan in dergelijke gevallen – alvorens het verzoek in behandeling te nemen – eerst van de verzoeker verlangen zijn vraag te preciseren. Voldoet deze laatste daaraan niet, dan kan in voorkomend geval de verantwoordelijke de vraag terzijde leggen als zijnde een vorm van misbruik van recht. De verantwoordelijke kan zich dan beroepen op artikel 43, onderdeel e, van dit wetsvoorstel: een gewichtig belang aan zijn kant staat aan inwilliging van het verzoek in de weg. De inspanning die de verantwoordelijke zou moeten leveren om de vraag te beantwoorden, kan hiertoe aanleiding geven, maar niet de aard van de gegevensverwerking. Evenmin is vereist dat de verzoeker een belang aantoont of zelf als betrokkene zou moeten worden aangemerkt.
Het ligt in de rede dat wanneer bij de Registratiekamer navraag wordt gedaan omtrent een gegevensverwerking bij een bedrijf of in een branche waar een eigen toezichthouder werkzaam is, de Registratiekamer de verzoeker naar deze functionaris verwijst. Deze zijn immers ingevolge artikel 63, derde lid, bij de Registratiekamer bekend. Ook is echter mogelijk dat de Registratiekamer zelf de verlangde gegevens verstrekt indien deze haar bekend zijn.

Vierde lid

In het vierde lid is een tweetal uitzonderingen op de inlichtingenplicht van de verantwoordelijke als bedoeld in het derde lid opgenomen. Artikel 13 van de richtlijn laat de lid-staten toe op dit beginsel uitzonderingen te maken. Onder de WPR bestonden zulke uitzonderingen niet. Geen van beide evaluaties hebben op dit punt problemen aan het daglicht gebracht. Daarom is in het onderhavig wetsvoorstel gekozen voor het regime van de WPR. Een uitzondering, waarvan de wenselijkheid echter in de loop der tijd is gebleken, zijn de tijdelijke registers van de bijzondere opsporingsdiensten. Hierboven in op artikel 29, derde lid, gingen wij daarop reeds in. Voorts zijn de openbare registers die bij de wet zijn ingesteld, uitgezonderd. Artikel 21, derde lid, van de richtlijn biedt daarvoor een expliciete

grondslag. Een afzonderlijke inlichtingenplicht voor de verantwoordelijke is overbodig indien reeds uit de wet waarbij het register is ingesteld, de desbetreffende informatie kan worden afgeleid.

PARAGRAAF 2 VOORAFGAAND ONDERZOEK

Artikel 31

Een beperkte categorie van verwerkingen rechtvaardigt het voorschrijven van voorafgaande controlemaatregelen die verder gaan dan aanmelding. Volgens artikel 20, eerste lid, van de richtlijn gaat het daarbij om verwerkingen die specifieke risico's meebrengen voor de rechten en vrijheden van de betrokkenen. De voorafgaande controle bestaat uit het kenbaar maken aan de toezichthoudende autoriteit van de voorgenomen verwerkingen en diens bevoegdheid om een nader onderzoek hiernaar in te stellen. Het een en ander heeft zijn beslag gekregen in de artikelen 31 en 32. De verwerkingen die in aanmerking komen voor een voorafgaand onderzoek moeten bij of krachtens wet worden aangewezen (artikel 31, derde lid). Voor een deel gebeurt dit in dit wetsvoorstel. Het onderzoek heeft in beginsel alleen betrekking op een geheel van verwerkingen, zoals ook de melding sec betrekking heeft op een geheel van verwerkingen. Het onderzoek zal derhalve in de regel geen betrekking hebben op een individuele beslissing om een gegeven te verwerken in de zin dat het zal worden verstrekt aan een ontvanger. Voor een nadere uitleg omtrent het begrip «geheel van verwerkingen» zij verwezen naar de toelichting op artikel 1, onderdeel b, en artikel 27, eerste lid.
Bepaalde lid-staten van de Europese Unie kennen thans al een systeem van voorafgaande toetsing in de vorm van een vergunningverlening, zij het met de mogelijkheid uitzonderingen te maken. Dit systeem werd wat Nederland betreft indertijd ook geïntroduceerd in het rapport «Privacy en persoonsregistratie» uit 1976 van de Commissie-Koopmans dat ten grondslag lag aan de totstandkoming van het voorstel van de Wet op de persoonsregistraties (kamerstukken II 1981/82, 17 207, nrs. 1–2). Dit voorstel is later uit dereguleringsoogpunt ingetrokken en vervangen door een wetsvoorstel dat heeft geleid tot de WPR.
Nu in artikel 20, eerste lid, van de richtlijn de benadering is gekozen dat de Lid-Staten de verplichting hebben nader te bepalen gegevensverwerkingen met bijzondere risico's aan een vorm van preventief toezicht te onderwerpen, is daartoe een regeling in het wetsvoorstel opgenomen. De richtlijn gaat evenwel niet zo ver dat een vergunningensysteem moet worden ingevoerd. In artikel 20 spreekt de richtlijn alleen over een «voorafgaand onderzoek». Tot een besluit strekkende tot toewijzing of afwijzing van een vergunning, behoeft dit onderzoek krachtens de richtlijn niet te leiden.
Het voorafgaand onderzoek wordt uitgevoerd door de Registratiekamer. De toets betreft een rechtmatigheidstoets. De uitkomst van deze toets kan uiteraard anders uitvallen dan wanneer de verantwoordelijke deze zèlf zou hebben gemaakt op grond van bijvoorbeeld artikel 8. Het is evenwel niet de bedoeling het voorafgaand onderzoek door de Registratiekamer daarvoor volledig in de plaats te stellen. Het voorafgaand onderzoek leidt tot een niet-bindende verklaring omtrent de rechtmatigheid van de verwerking die de verantwoordelijke niet ontslaat van de verplichting om zijn eigen afweging te maken. Wel ligt het in de rede dat de verklaring van de Registratiekamer in de afweging door de verantwoordelijke een belangrijke rol zal spelen. Mede met het oog op het belang van de verklaring van de kamer voor de verantwoordelijke, is voorzien in de mogelijkheid van bezwaar en beroep voor het geval de verantwoordelijke zich niet met het oordeel van de Registratiekamer zou kunnen verenigen. De verdere procedure die leidt tot een verklaring is geregeld in artikel 32. Artikel 20, derde lid, van de richtlijn bepaalt tevens dat een voorafgaand

onderzoek kan worden uitgevoerd in het kader van de voorbereiding van wettelijke voorschriften door het parlement. Een dergelijk onderzoek verschilt van het in het eerste lid van dat artikel bedoelde onderzoek in die zin dat het geen opschortende werking heeft. De wettelijke maatregel beoogt immers niet meer dan een wettelijke basis te verschaffen voor een bepaalde gegevensverwerking. Dit onderzoek vindt dan ook plaats in het kader van de algemene adviesbevoegdheid van de Kamer, bedoeld in artikel 51, tweede lid.
De Registratiekamer stelt in haar advies dat artikel 20, tweede lid, van de richtlijn zou voorschrijven dat een voorafgaand onderzoek ook kan plaatsvinden door de functionaris voor de gegevensbescherming als bedoeld in artikel 62. Bij navraag bij de Europese Commissie bleek evenwel dat artikel 20 is bedoeld de lid-staten een optie te geven in die zin dat zij vrij zijn in hun wetgeving te bepalen dat alleen de Registratiekamer bevoegd is het voorafgaand onderzoek te doen. Voor deze optie is gekozen teneinde de rechtsbescherming tegen een negatieve beslissing na het onderzoek goed te kunnen regelen. Zou deze in handen van de functionaris liggen, dan zou de regeling van de rechtsbescherming tegen een negatieve beslissing weer apart moeten worden geregeld.

Eerste lid

Artikel 31, eerste lid, bepaalt dat de aldaar opgesomde gegevensverwerkingen met een bijzonder risico, voorafgaand aan de verwerking onderzocht. Er worden vervolgens een drietal categorieën van verwerkingen genoemd die vanwege de daaraan verbonden bijzondere risico's in elk geval voor een voorafgaand onderzoek in aanmerking komen.

Onderdeel a

Onderdeel a gaat over gebruik van persoonsnummers voor een ander doel dan waarvoor ze specifiek zijn bestemd.
Een persoonsnummer heeft tot doel koppelingen met gegevensverwerkingen van andere verantwoordelijken te kunnen leggen. Met sectorale persoonsnummers kunnen koppelingen worden gemaakt met andere gegevensverwerkingen van andere verantwoordelijkes binnen de sector. Met nationale persoonsnummers kunnen in beginsel koppelingen worden gelegd met elke andere gegevensverwerking waarbij het betreffende nummer wordt gebruikt. Dit laatste onderwerp komt in de richtlijn aan de orde in artikel 8, zevende lid, dat is geïmplementeerd in artikel 24. Gelet op de koppelingsmogelijkheid van andere, dus sectorale, persoonsnummers is ook in de gevallen waarop artikel 24 geen betrekking heeft, de mogelijkheid van een afzonderlijk voorafgaand onderzoek wenselijk indien de koppeling gescheidt voor een ander doel dan waarvoor het persoonsnummer specifiek bedoeld is.
Naar aanleiding van het advies van de Registratiekamer is onderdeel a eveneens beter afgestemd op artikel 24 van dit wetsvoorstel.

Onderdeel b

Onderdeel b vormt een complement op het niet-informeren van de betrokkene van de verwerking van hem betreffende gegevens in bepaalde specifieke situaties. Indien de verantwoordelijke gegevens verkrijgt, is hij op grond van artikel 33 of 34 verplicht de betrokkene te informeren over ten minste zijn identiteit en de doeleinden van de verwerking. In bepaalde gevallen behoeft hij evenwel niet te informeren, nl. indien het informeren van de betrokkene onmogelijk blijkt of een onevenredige inspanning kost (art. 34, vierde lid) dan wel vanwege andere belangen op onoverkomelijke bezwaren stuit (art. 43). Vanwege het feit dat betrokkene niet van de

verwerking op de hoogte wordt gesteld, bestaat er uit hoofde van gegevensbescherming een bijzonder risico.
Om te beoordelen welke waarborgen ter compensatie voor het niet-informeren behoren te gelden, dienen twee casusposities te worden onderscheiden. In de eerste plaats kan het zo zijn dat de verantwoordelijke de gegevens verzamelt bij anderen dan de betrokkene, bijvoorbeeld door gegevens over de betrokkene bij een andere verantwoordelijke op te vragen. Voor die situatie bepaalt artikel 34, vierde lid, tweede volzin dat de verantwoordelijke de herkomst van de gegevens dient vast te leggen. Aldus is er een compenserende waarborg voor het feit dat de betrokkene niet op de hoogte wordt gesteld. Anders wordt het echter indien de verantwoordelijke gegevens vergaart door middel van eigen waarneming zonder dat de betrokkene daarvan op de hoogte is. In die situatie bestaat er een aanmerkelijk risico dat de gegevensverwerking voor de betrokkene onopgemerkt blijft. Alleen op die specifieke situatie heeft onderdeel b betrekking. Als compenserende waarborg voor het niet-informeren geldt hier dus dat de Registratiekamer op grond van artikel 31 de gelegenheid heeft een voorafgaand onderzoek in te stellen. De openbare registers die bij de wet zijn ingesteld, vormen hierop op grond van het tweede lid een uitzondering. Aangenomen mag worden dat in die gevallen reeds de wetgever het betreffende onderzoek heeft uitgevoerd.

Onderdeel c

Onderdeel c betreft de mogelijkheid van voorafgaand onderzoek in het geval de verantwoordelijke strafrechtelijke of daarmee gelijk te stellen gegevens verwerkt ten behoeve van derden. Op de risico's die zijn verbonden aan dergelijke verwerkingen, is reeds in de toelichting op artikel 22 ingegaan. In het derde lid van dat artikel wordt het doorlopen van de procedure inzake voorafgaand onderzoek – voor zover de Wet particuliere beveiligingsorganisaties en recherchebureaus niet van toepassing is – ook als uitdrukkelijke voorwaarde gesteld voor de rechtmatigheid van de verwerking. Verwezen kan worden naar de toelichting op dat artikel.

Tweede lid

Het tweede lid is reeds ter sprake gekomen bij het eerste lid, onderdeel b.

Derde lid

Het derde lid voorziet in de mogelijkheid nieuwe, gelet op de soms snelle informatietechnologische ontwikkelingen vooraf niet te voorziene vormen van gegevensverwerking aan de verplichting van een voorafgaand onderzoek te onderwerpen. Dit kan relatief eenvoudig bij algemene maatregel van bestuur. De Registratiekamer kan daartoe een aanbeveling doen in haar jaarverslag. Deze bepaling is analoog aan die in artikel 16, tweede lid, WPR. Algemene voorwaarde om een gegevensverwerking is dat deze een bijzonder risico vormt voor de persoonlijke rechten en vrijheden van de betrokkene. Dit criterium ligt in de lijn van artikel 20, eerste lid, van de richtlijn.

Vierde lid

Artikel 8, zesde lid, van de richtlijn schrijft voor dat de lid-staten van de Europese Unie de Europese Commissie op de hoogte stellen van regelingen die de verwerking toelaten van strafrechtelijke gegevens. Uit met name de Duitstalige versie van de richtlijn blijkt dat de verplichting de verwerking van strafrechtelijke persoonsgegevens bij de Europese

Commissie te melden, zich niet beperkt tot gevoelige gegevens in de zin van artikel 8, eerste lid, van de richtlijn.
Het onderhavige lid legt de meldingsplicht bij de Registratiekamer, daar deze als eerste kennis draagt van aanvragen tot verwerking van deze gegevens. Het zou onnodige bureaukratische rompslomp met zich brengen wanneer de Registratiekamer eerst de regering zou moeten informeren en deze laatste vervolgens weer de Commissie.

Artikel 32

Eerste lid

De verantwoordelijke maakt bij de melding bekend dat het gaat om een gegevensverwerking waarop artikel 31, eerste lid, van toepassing is. Omdat het voor de Registratiekamer niet in alle gevallen mogelijk is aan de hand van de aangemelde gegevens te beoordelen of het gaat om een zodanige verwerking, dient de verantwoordelijke dit expliciet te vermelden. Ook de Registratiekamer adviseert dit in haar advies. Als voorbeeld kan worden gewezen op de aanmelding van verwerkingen die vallen onder artikel 31, eerste lid, onderdeel b.

Tweede lid

Een verantwoordelijke die een gegevensverwerking aanmeldt ten aanzien waarvan een voorafgaand onderzoek moet worden verricht, dient zijn voornemen deze verwerking te verrichten op te schorten totdat het onderzoek van de Registratiekamer heeft plaatsgevonden dan wel hem is gemeld dat een zodanig nader onderzoek achterwege blijft. De verplichting de verwerking op te schorten volgt reeds uit het feit dat het onderzoek blijkens artikel 31, eerste lid, voorafgaand aan de verwerking dient plaats te vinden. Voor alle duidelijkheid is echter deze verplichting geëxpliciteerd in artikel 32, tweede lid. De verantwoordelijke die desondanks tot verwerken overgaat verwerkt de gegevens in strijd met de wet en kan bijvoorbeeld op grond van artikel 49 tot schadevergoeding verplicht worden. Hetzelfde geldt voor de verantwoordelijke die verzuimd heeft bij de aanmelding te vermelden dat het gaat om een gegevensverwerking waarop artikel 31, eerste lid, van toepassing is.
Het tweede lid geeft uitvoering aan het advies van de Registratiekamer een uitdrukkelijke bepaling op te nemen die de verantwoordelijke verplicht te wachten totdat de bedoelde termijnen zijn verstreken.

Derde lid

De plicht van de verantwoordelijke bij de melding bekend te maken dat het gaat om een verwerking die valt onder artikel 31, eerste lid, ontslaat de Registratiekamer niet van de verplichting – voor zover zij althans daar zicht op hebben – zelf te controleren aan de hand van de gegevens die bij de aanmelding worden overgelegd, of het gaat om een gegevensverwerking in de zin van dat artikel. De formulering van het derde lid sluit hierop aan.
De procedure bestaat uit twee fasen. Allereerst dient de Registratiekamer te bezien of een aangemelde gegevensverwerking die onder het bereik van artikel 31 valt, aanleiding geeft tot een nader onderzoek. De periode die nodig is om te bepalen of nader onderzoek moet worden gedaan, mag niet langer dan vier weken duren. Vervolgens kan er dan een tweede fase volgen waarin de Registratiekamer een uitgebreider onderzoek verricht. Deze periode mag niet langer duren dan dertien weken. De term «voorafgaand onderzoek» ziet zowel op het voorbereidend onderzoek gedurende de eerste vier weken als op het het meer uitgebreide onderzoek dat daarop kan volgen.

De beslissing van de Kamer om al dan niet tot nader onderzoek over te gaan moet schriftelijk worden vastgelegd. Indien binnen vier weken na de melding geen bericht van de Kamer wordt ontvangen, kan de verantwoordelijke er van uitgaan dat geen nader onderzoek wordt ingesteld. Aan de beslissing van de Kamer niet tot nader onderzoek over te gaan kan niet worden ontleend dat de gegevensverwerking als rechtmatig kan worden beschouwd. Genoemde beslissing laat de aansprakelijkheid van de verantwoordelijke voor de verwerking ten volle intact. De beslissing geeft slechts blijk van het gevoelen van de Kamer dat aan de verwerking niet zodanig bijzondere risico's kleven dat een diepgaander onderzoek op grond van artikel 31 gerechtvaardigd is.

Vierde lid

De beslissing over te gaan tot nader onderzoek is voor bezwaar en beroep vatbaar. Het betreft een besluit in de zin van de Awb omdat beoogd wordt de opschorting van de gegevensverwerking van de verantwoordelijke te verlengen totdat het uitgebreide onderzoek van de Kamer is voltooid. In dit besluit dient de Kamer te hebben aangegeven binnen welk termijn zij het vermoeden heeft het onderzoek te kunnen afronden. Deze termijn is niet fataal, in die zin dat na afloop van de termijn de Kamer kan worden geacht het onderzoek te hebben afgerond en de houder tot verwerking mag overgaan. De termijn geeft niet meer dan een indicatie van de duur van het onderzoek en beoogt de verantwoordelijke enige rechtszekerheid te verschaffen. Na afloop van de termijn kan de verantwoordelijke de Kamer rappeleren. Mocht de Kamer tijdens het onderzoek blijken dat de in het besluit bepaalde termijn te kort is, dan ligt het in de rede dat zij de verantwoordelijke hierover bericht. Wel is de uiterlijke duur van het onderzoek in het vierde lid gebonden aan een maximum, namelijk dertien weken. Deze termijn is wèl fataal. Mocht de Kamer de maximumtermijn van dertien weken in haar besluitvorming overschrijden dan kan de verantwoordelijke er vanuit gaan dat het nader onderzoek is afgerond en er geen reden meer is zijn voornemen tot gegevensverwerking verder op te schorten.

Vijfde en zesde lid

Het uitgebreide onderzoek leidt tot een verklaring van de Kamer dat de gegevensverwerking al dan niet rechtmatig is. Deze verklaring is niet bindend. Zij is derhalve ook geen besluit in de zin van de Awb. De Registratiekamer meent in haar advies dat het de voorkeur verdient de verantwoordelijke eerst bijzondere rechtsbescherming te bieden op het moment dat hij wordt aangesproken in rechte of naar aanleiding van het onderzoek onderworpen wordt aan bestuursdwang. Wij hebben dit advies niet opgevolgd. Er mag immers niet worden voorbij gegaan aan het maatschappelijk gewicht van de verklaring. Het feit dat de verklaring juridisch niet bindend is, doet daaraan geen afbreuk. De verklaring van de Kamer naar aanleiding van een voorafgaand onderzoek kan wat dat betreft op één lijn worden gesteld met de verklaring dat de in een gedragscode opgenomen regels een juist uitwerking zijn van de wet (artikel 25, eerste lid). De verantwoordelijke kan door een negatieve verklaring daadwerkelijk in zijn belangen worden geschaad. Om die reden is er behoefte aan rechtsbescherming en is in het vijfde lid – analoog aan de regeling inzake de gedragscodes – uitdrukkelijk bepaald dat een verklaring als een besluit geldt in de zin van de Awb. Voorts is – eveneens analoog aan de gedragscodes – bepaald dat met het oog de voorbereiding van de verklaring Afdeling 3.4 van de Awb van toepassing is. Langs deze weg worden de belangen van de verantwoordelijken en eventuele andere belanghebbenden op adequate wijze gewaarborgd.
Uit een oogpunt van rechtsbescherming verschilt de verklaring van de

mededeling van bevindingen als bedoeld in artikel 60, tweede lid. In het laatste geval gaat het meer om een regulier onderzoek in het kader van het toezicht op de naleving van de wettelijke voorschriften. Het onderzoek vormt in bepaalde gevallen de voorbereiding van mogelijke maatregelen die voor bezwaar en beroep vatbaat zijn (bijv. bestuursdwang). Om die reden is er geen behoefte aan een afzonderlijke rechtsgang tegen de mededeling als bedoeld in artikel 60. In artikel 32 gaat het evenwel om een onderzoek dat voorafgaat aan de verwerking dat bovendien – mede vanwege de bijzondere risico's die aan de betreffende verwerkingen verbonden zijn – doorgaans van groter gewicht zal zijn voor alle betrokken partijen. Om die reden is de procedure omtrent het voorafgaand onderzoek met extra waarborgen omkleed.

HOOFDSTUK 5 INFORMATIEVERSTREKKING AAN DE BETROKKENE

Artikelen 33 en 34

1. Inleiding

De artikelen 10 en 11 van de richtlijn bevatten een regeling voor de informatieverstrekking aan de betrokkene in verband met de verkrijging van gegevens al dan niet bij de betrokkene zelf. Het wetsvoorstel voert deze bepalingen uit in de artikelen 33 en 34. Deze bepalingen vormen een uitwerking van het transparantiebeginsel en van het in artikel 6 neergelegde beginsel van «fair processing»: behoudens uitzonderingen is de gegevensverwerking slechts «behoorlijk» in de zin van artikel 6, indien de betrokkene daarvan overeenkomstig de regels van de artikelen 33 of 34 op de hoogte wordt gebracht. De verplichting van de verantwoordelijke op eigen initiatief de betrokkene op de hoogte te stellen van het bestaan van de gegevensverwerking is een belangrijk instrument om het gegevensverkeer transparant te maken. De ratio van de informatieverplichting is dat de verwerkingen van de verantwoordelijke voor de betrokkene aanspreekbaar zijn in rechte. De betrokkene is in staat te volgen hoe gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten.
De omvang van de informatieplicht hangt af van wat nodig is om een «fair processing» te waarborgen. De regeling leidt ten opzichte van de WPR tot een verbetering van de rechtsbescherming. In de WPR is naast het principe van rechtmatige verkrijging alleen sprake van een mededelingsplicht wanneer over de betrokkene voor de eerste keer gegevens in een register worden opgenomen. In het licht van de sterk toegenomen mogelijkheden tot vergaring van persoonsgegevens bestaat reeds behoefte aan transparantie in het stadium waarin de gegevens worden verkregen. De omstandigheid dat de onderhavige regeling een uitwerking vormt van het beginsel dat in artikel 6 is neergelegd heeft tot gevolg, dat overtredingen van de informatieplicht zullen leiden tot onrechtmatige verwerkingen. Daarnaast kan het zijn, dat onder omstandigheden verdergaande informatie geboden is om «een eerlijke verwerking» te waarborgen. De richtlijn brengt dit tot uitdrukking door de woorden «ten minste» in de aanhef van beide artikelen.
Er kunnen twee vormen van actieve informatieverstrekking worden onderscheiden. In aansluiting op de richtlijn wordt daarbij onderscheid gemaakt tussen de verkrijging van de gegevens bij de betrokkene en op een andere wijze. Worden de gegevens verkregen bij de betrokkene zelf, bijvoorbeeld wanneer hij aan de hand van een formulier gegevens over zichzelf moet invullen voor een bepaald doel, dan dient deze op de hoogte te worden gesteld op het moment van vergaring van gegevens. Deze vorm komt aan de orde in artikel 33. Artikel 34 regelt de situatie dat de

gegevens op een andere wijze worden verkregen, dus buiten de betrokkene om, hetzij bij derden, bijvoorbeeld gegevens omtrent iemands kredietwaardigheid bij een handelsinformatiebureau, hetzij door eigen observatie, bij voorbeeld naar aanleiding van het gebruik van een netwerk in beheer van de verantwoordelijke. Gezien de onderlinge samenhang tussen beide artikelen en ten einde overlappingen te voorkomen worden de artikelen te zamen toegelicht.

2. Wanneer bestaat de informatieplicht?

De artikelen 33 en 34 bepalen dat de verantwoordelijke verplicht is zijn identiteit bekend te maken aan de betrokkene en deze te informeren over de doeleinden van de verwerking, tenzij de betrokkene daarvan «reeds op de hoogte is». Deze tekst is ontleend aan de artikelen 10 en 11 van de richtlijn. Artikel 28 van de WPR bepaalt dat een mededeling van eerste opname achterwege kan blijven, als de betrokkene weet of «redelijkerwijs kan weten» dat hij in een bepaalde registratie is opgenomen. Bij de voorbereiding van de richtlijn is in Brussel van verschillende zijden, onder meer door Nederland, aangedrongen op een versoepeling van de tekst van de artikelen 10 en 11 in die zin dat de informatieverplichting van de verantwoordelijke vervalt indien hij kan aannemen dat de betrokkene «redelijkerwijs» op de hoogte «kan zijn». Een dergelijke tekst zou in overeenstemming zijn geweest met artikel 28 WPR. De huidige tekst van de richtlijn, waarin het woord «redelijkerwijs» ontbreekt, is het resultaat van een compromis. Dit regime is strakker dan onder de WPR. Voor een nader begrip van de reikwijdte van de informatieplicht, kan aansluiting worden gezocht bij bestaande noties die in het Nederlands privaatrecht tot ontwikkeling zijn gekomen.
Artikel 6:228, tweede lid, BW bepaalt dat iemand zich bij het sluiten van een overeenkomst niet kan beroepen op dwaling, indien deze zijn oorsprong vindt in omstandigheden die volgens de in het verkeer geldende opvattingen voor rekening van de dwalende behoren te blijven. De bepaling geeft uitdrukking aan het beginsel dat bij de totstandkoming van een overeenkomst in het algemeen een balans bestaat tussen de informatieplicht van de één en de onderzoeksplicht van de ander. Naar welke kant de balans in een concreet geval doorslaat, is afhankelijk van omstandigheden zoals de deskundigheid van betrokkenen en de wetenschap die men bij elkaar mag veronderstellen. Een dergelijke balans doet zich ook voor in situaties waarin geen sprake is van een overeenkomst. Artikel 28 WPR preciseert een dergelijke balans in de verhouding tussen de verantwoordelijke en de betrokkene. Op grond van artikel 28 kan een mededeling van eerste opname achterwege blijven, als de betrokkene redelijkerwijs kan weten dat hij in een bepaalde registratie is opgenomen. Dit laat ruimte voor een beperkte onderzoeksplicht voor de betrokkene. Onder het regime van dit wetsvoorstel zal de verantwoordelijke zich echter pas ontslagen mogen achten van zijn informatieplicht, als hij weet dat de betrokkene op de hoogte is. De artikelen 33 en 34 van dit wetsvoorstel gaan ervan uit dat er geen onderzoeksplicht van de betrokkene is. De hieraan ten grondslag liggende gedachte is die van een ongelijkwaardigheid van partijen. Vanuit het gezichtspunt van een hoog niveau van consumentenbescherming, zoals neergelegd in het mede aan de richtlijn ten grondslag liggende artikel 100A, derde lid van het EG-Verdrag, is het evenwicht van de balans verlegd ten gunste van de betrokkene, zijnde de in het algemeen maatschappelijk zwakkere partij. Dit betekent geenszins dat de verantwoordelijke in alle gevallen dat hij gegevens vergaart bij de betrokkene of bij een derde, zich van de bewustzijnsinhoud van de betrokkene hoeft te vergewissen. Het «op de hoogte zijn» mag de verantwoordelijke op uiteenlopende wijze, afhankelijk van de omstandigheden, aannemen. Beschikt de betrokkene over de informatie, bijvoorbeeld omdat deze hem is overhandigd of toegezonden,

dan is hij daarmee op de hoogte, ongeacht of hij het initiatief heeft genomen de informatie ook tot zijn bewustzijn te brengen. De Duitse tekst van de richtlijn brengt dit bijvoorbeeld tot uitdrukking door te eisen dat de informatie moet «vorliegen». Indien de betrokkene op de hoogte is, is geen nadere informatieverstrekking meer nodig. Hoewel de verantwoordelijke dus niet zonder meer ervan mag uitgaan dat de betrokkene in een bepaalde situatie wel kan weten of weet dat, door wie en hoe de gegevens worden verwerkt, kunnen ook bepaalde gedragingen of verklaringen van de verantwoordelijke aanleiding geven tot het gerechtvaardigde vermoeden dat de betrokkene daarvan op de hoogte is. Het gaat om gedragingen of verklaringen die in het maatschappelijk verkeer de betrokkene kunnen worden toegerekend als blijk van het feit dat hij op de hoogte is. Het is de gedachte die ook ten grondslag ligt aan artikel 3:36 BW. De verantwoordelijke mag uitgaan van de zin die onder de gegeven omstandigheden aan een verklaring of een gedraging van de betrokkene redelijkerwijze mocht worden toegekend. Artikel 3:59 BW verklaart deze bepaling van toepassing buiten het vermogensrecht, voor zover de aard van de rechtsbetrekking zich daartegen niet verzet. Dit laatste is hier niet het geval. De stelling van de Registratiekamer in haar advies dat de verantwoordelijke enkel mag afgaan op een gedraging van betrokkene waarvan de strekking onmiskenbaar duidelijk is, kan daarmee niet worden onderschreven. Deze legt immers een te zware onderzoeksverplichting op de verantwoordelijke. Als de betrokkene middels een gedraging laat blijken op de hoogte te zijn van de informatie en deze gedraging in het maatschappelijk verkeer ook als zodanig mag worden opgevat, kan van de verantwoordelijke geen verdergaande actie ten aanzien van zijn informatieplicht worden gevergd. De betrokkene kan dan worden toegerekend dat zijn gedraging op die wijze door de verantwoordelijke wordt geïnterpreteerd. Mocht hij een andere bedoeling hebben gehad met zijn gedraging dan heeft hij een hem verwijtbaar risico geschapen van een misverstand met de verantwoordelijke.
Voorbeelden van het vorenstaande zijn de volgende. Een reisbureau kan ervan uitgaan dat degene die een reis boekt weet dat de gegevens worden verwerkt om de reis daadwerkelijk te kunnen boeken en te zorgen voor de financiële afwikkeling. Het is algemeen bekend dat de boeking van een vliegreis niet kan plaatsvinden zonder dat de persoonsgegevens aan de vliegmaatschappij worden doorgegeven. Een afzonderlijke mededeling van een dergelijke gegevensverwerking zou tot absurde situaties leiden. Zo kan ook de restauranthouder ervan uitgaan dat iemand die in een restaurant na afloop van een etentje een credit card aan de ober geeft, dat slechts doet in de wetenschap dat persoonsgegevens worden doorgegeven aan de credit-cardmaatschappij en vervolgens aan de bank van de betrokkene ten einde de rekening voor dat etentje te betalen. De mededeling op dat moment hoe één en ander geregeld is, wordt niet door de onderhavige bepaling geëist.
De omvang van de informatieverplichting is mede afhankelijk van de wijze waarop het contact tot stand komt. In beginsel zal op de verantwoordelijke een extra verantwoordelijkheid tot informeren rusten als hij zelf het initiatief neemt tot het contact met de betrokkene. De betrokkene die de verantwoordelijke zelf benadert, zal veelal reeds op de hoogte zijn van diens identiteit en oogmerken. Dan moet wel nog het concrete doel van de gegevensverwerking en eventueel aanvullende informatie worden verstrekt, terwijl in geval dat redelijkerwijs twijfel mogelijk is, ook de identiteit van de verantwoordelijke dient te worden bekendgemaakt.
In de gevallen dat de verantwoordelijke er niet op mag vertrouwen dat de betrokkene op de hoogte is, dient hij ten minste zijn identiteit bekend te maken en de betrokkene te informeren over het doel van de gegevensverwerking.

3. Wijze waarop de informatie kan worden verstrekt

Uitgangspunt is dat de informatie zodanig moet worden verstrekt dat de betrokkene daarover daadwerkelijk beschikt. In de praktijk kan dit op velerlei wijze. In een rechtstreeks individueel contact tussen (een vertegenwoordiger van) de verantwoordelijke en betrokkene kan de informatie mondeling of schriftelijk worden verstrekt. Bij interactieve telecommunicatie, wanneer daarbij de mogelijkheid bestaat ook datacommunicatie te doen plaatsvinden, kan de informatie in de vorm van data worden verstrekt. Ter verduidelijking wordt hieronder nader ingegaan op het een en ander.
Bij de primaire gegevensvergaring (artikel 33) moet de informatie aan de betrokkene worden verstrekt op het moment van verzamelen. Gebeurt dit verzamelen via een formulier dan kan de informatie op het formulier worden voorgedrukt. Wanneer de betrokkene het formulier invult kan hij de informatie lezen. Het is dan niet nodig dat hij met zijn handtekening te kennen geeft ook deze informatie te hebben gelezen. Hij is op de hoogte in de zin van deze bepaling wanneer hij op een relevant moment over de informatie beschikt. Het is aan de betrokkene om in dergelijke omstandigheden voor zichzelf te bepalen of hij eerst kennis wil nemen van de informatie of dat hij, zonder kennis te nemen van de informatie waarover hij beschikt, de van hem verlangde persoonsgegevens verstrekt.
Hetzelfde geldt voor de overhandiging van een folder of een exemplaar van standaardvoorwaarden bij het sluiten van een contract. Weigert de betrokkene de folder of het exemplaar aan te nemen, dan komt dit voor zijn rekening. De verantwoordelijke heeft dan aan zijn verplichtingen voldaan. Onvoldoende is dat op een formulier wordt verwezen naar elders verkrijgbare informatie.
Wanneer de betrokkene persoonsgegevens via de elektronisch communicatie verstrekt, dan zal het voor de verantwoordelijke weinig bezwaarlijk zijn om langs dezelfde weg de betrokkene vooraf uitgebreid te informeren over wat er met de gegevens gebeurt. Op het eerste scherm dat na het inloggen verschijnt en waarbij de betrokkene in de gelegenheid wordt gesteld gegevens over zichzelf in te voeren, kan een extra regel op het scherm verwijzen naar bijvoorbeeld via doorklikken beschikbare informatie over de verwerkingen die geschieden met de gegevens. Zolang elektronische communicatie nog niet op alle gebieden in onze maatschappij ingeburgerd is, bijvoorbeeld zolang vliegreizen of theaterreserveringen nog telefonisch worden geboekt, zal evenwel de verantwoordelijke de betrokkene mondeling moeten informeren, indien niet anderszins is voorzien in informatie over hoe de gegevens worden verwerkt.
Is informatie over de gegevensverwerking opgenomen in een reisgids of een theaterprogramma waarvan de betrokkene bij een telefonische boeking kennelijk gebruik maakt, dan kan de verantwoordelijke ervan uitgaan dat de betrokkene op de hoogte is. Staat dit niet vast, dan zal in het telefonische contact alsnog de informatie moeten worden verstrekt. Geeft de betrokkene blijk daarin niet te zijn geïnteresseerd, dan zal de verantwoordelijke zich van zijn informatieplicht verder ontslagen kunnen achten. De bepalingen van het wetsvoorstel strekken niet tot verplichte communicatie tussen verantwoordelijke en betrokkene tegen de verklaarde wil van de laatste in. In het geval van gegevensvergaring bij een ander dan de betrokkene (artikel 34) zal de verantwoordelijke de betrokkene moeten informeren indien de gegevens worden vastgelegd op het moment van de vastlegging dan wel, indien verstrekking van de gegevens aan derde wordt overwogen, uiterlijk op het moment van eerste verstrekking. Er vindt in dat geval bij de vergaring geen (direct) contact plaats tussen de betrokkene en de verantwoordelijke. Dit contact zal de verantwoordelijke daarentegen zoeken bij vastlegging respectievelijk eerste verstrekking. Daarbij zal het contact specifieker zijn naarmate het

aantal bij de verwerking betrokkenen specifieker bepaalbaar is. Gaat het om één bepaalde betrokkene, dan zal deze specifiek op de hoogte moeten worden gesteld. Gaat het daarentegen om meerdere betrokkenen, dan kan de wijze van informeren algemener zijn. Voor de vraag of het moment van vastlegging dan wel verstrekking aan derden geldt als moment van informatieverstrekking zijn de objectieve bedoelingen van de verantwoordelijke doorslaggevend. Heeft hij geen oogmerk te verstrekken dan geldt het moment van vastleggen. Hij dient dan de betrokkene zo spoedig als redelijkerwijs mogelijk is van informatie te voorzien. Heeft de verantwoordelijke daarentegen wel de bedoeling aan derden te verstrekken, dan kan in ieder geval met de verstrekking geen begin worden gemaakt dan nadat de betrokkene is geïnformeerd. De bedoeling kan worden afgelezen aan het uitwendig kenbaar gedrag waaraan in een bepaalde maatschappelijke context, redelijkerwijs een bepaalde bedoeling kan worden afgelezen.
Wanneer de informatie aan een groep personen moet worden verstrekt, kan deze groep de informatie ter beschikking worden gesteld via een medium waarvan vaststaat dat deze groep daarmee wordt bereikt. Gaat het bijvoorbeeld om leden van een vereniging, dan kan de verstrekking van informatie door een bekendmaking in een verenigingsorgaan plaatsvinden. Hetzelfde geldt voor een werkgever die zijn werknemers in kennis stelt van nieuwe vormen van gegevensverwerking via een personeelsblad dat onder alle werknemers verspreid wordt. Het staat dan immers vast dat de informatie de betrokkene zal bereiken. Verder is er sprake van een zodanige betrokkenheid van de groep personen bij het personeelsblad, medium van verspreiding, dat ervan uitgegaan kan worden dat de betrokkene in kennis is gesteld. Wanneer de gegevensverwerking leden van een bepaalde beroepsgroep betreft, waarvan het voor een behoorlijke uitoefening van het beroep noodzakelijk is vakliteratuur bij te houden, kan de informatieverstrekking door bekendmaking in de desbetreffende vakliteratuur plaatsvinden.
Daarentegen kan bijvoorbeeld niet worden aangenomen dat de leden van een beroepsgroep zijn bereikt wanneer mededeling wordt gedaan in een vakbondsblad, als niet vaststaat dat 100 % van de desbetreffende beroepsgroep lid is van deze bond. In dat geval kan er immers niet van worden uitgegaan dat iedere betrokkene wordt bereikt. Wat betreft het grote publiek kan evenmin worden aangenomen dat advertenties in de landelijke of plaatselijke bladen toereikend zijn om aan te nemen dat betrokkenen zijn geïnformeerd. Dit is echter anders wanneer de informatie wordt vergaard via een formulier dat in deze bladen is opgenomen en wanneer hierbij meteen de informatie over de gegevensverwerking wordt meegedeeld. Evenmin kunnen huis aan huis verspreide bladen worden aangemerkt als informatiebron van de betrokkene. Weliswaar wordt dan een ieder bereikt, doch de context van deze vorm van informatieverspreiding is onvoldoende specifiek om van de betrokkene te vergen dat hij erop attent is dat voor hem relevante informatie wordt overgedragen. Weliswaar zou de betrokkene bij naspeuringen in dergelijke gevallen kunnen weten dat mogelijk over hem informatie wordt verwerkt, doch de ratio van de bepalingen in de richtlijn is dat hij een dergelijke onderzoeksplicht juist niet heeft.
De verantwoordelijke kan ervan uitgaan dat de betrokkene kennis zal nemen van informatie die wordt verspreid binnen de kring van personen waartoe de betrokkene zichzelf blijkens zijn gedragingen rekent. De betrokkene kan niet worden aangesproken als onderdeel van het algemene publiek. 4. De inhoud van de informatieverstrekking

4. Inhoud van de informatie

Het is steeds nodig dat de identiteit van de verantwoordelijke en het doel van de verwerking waarvoor de gegevens zijn bestemd, aan de betrokkene worden meegedeeld. De artikelen 10 en 11 van de richtlijn

laten in dit opzicht geen uitzonderingen toe. Dit uitgangspunt is neergelegd in artikel 33, tweede lid, en artikel 34, eerste lid, van dit wetsvoorstel. Ter zake van de doeleinden waarvoor de gegevensverwerking kan zijn bestemd wordt verwezen naar artikel 7.
Het derde lid van laatstgenoemde artikelen bepaalt echter dat de verantwoordelijke in het algemeen niet kan volstaan met het mededelen van zijn identiteit en de doeleinden van de verwerking. Hij zal de betrokkene in deze gevallen nader moeten informeren opdat er sprake is van een gegevensverkrijging die als rechtmatig kan worden aangemerkt («fair processing»). Deze nadere informatie wordt geboden uit overwegingen van maatschappelijke zorgvuldigheid die de verantwoordelijke ten opzichte van de betrokkene in acht moet nemen. De aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, bepalen of deze nadere informatie nodig is. De verantwoordelijke zal zich telkens moeten afvragen of deze omstandigheden met zich brengen dat verwacht mag worden dat de betrokkene een reëel belang heeft bij nadere informatie en zo ja, wat de omvang van deze informatie is. Deze voorwaarde is een aanvulling op de in hoofdstuk 2 neergelegde algemene voorwaarden voor de rechtmatigheid van gegevensverwerkingen.
Voorbeelden van omstandigheden waarbij aanvullende informatie is aangewezen, zijn de volgende. Wanneer informatie wordt gevraagd in het kader van een te sluiten overeenkomst of bij de aanvraag van een beslissing door een bestuursorgaan, kan het voorkomen dat bij voorbeeld om statistische redenen of met het oog op toezending van geadresseerde reclame, informatie van de betrokkene wordt gevraagd, de beantwoording waarvan niet essentieel is voor het sluiten van de overeenkomst of het afgeven van de beschikking. Het geven van een antwoord kan achterwege blijven zonder dat daarmee het gevraagde in gevaar komt. In dergelijke gevallen behoort het tot de eisen van een zorgvuldige gegevensverwerking de betrokkene van deze omstandigheid in kennis te stellen. De verantwoordelijke zal dan niet alleen duidelijkheid moeten bieden over de doeleinden die door hem worden beoogd, maar ook moeten aangeven welke gegevens waarvoor zijn bestemd en wat de gevolgen zijn indien bepaalde gegevens niet worden verstrekt.
In het kader van artikel 34 kan gedacht worden aan het geval dat de gegevens worden verkregen door koppeling van diverse bestanden. De verantwoordelijke, die binnen de grenzen van het wetsvoorstel bestanden wil koppelen om een nieuwe gegevensverzameling op te bouwen, moet de betrokkene informeren over de wijze waarop hij deze nieuwe gegevens heeft verkregen. Koppeling legt dan een extra verantwoordelijkheid bij de verantwoordelijke. De informatieplicht in het geval van koppelen omvat bijvoorbeeld de verplichting de betrokkene op de hoogte te stellen van het feit dat de gegevens zijn verkregen middels een koppeling van bestanden, een omschrijving van de soort bestanden die zijn gekoppeld en het wijzen van de betrokkene op zijn recht op toegang en verbetering van de gegevens.
Indien de verantwoordelijke op grond van het derde lid van de artikelen 33 of 34 de betrokkene nader heeft geïnformeerd, en zich een wijziging voordoet in de informatie, bijvoorbeeld doordat de verantwoordelijke de gegevens aan andere personen wil verstrekken dan de categorieën ontvangers die hij de betrokkene heeft medegedeeld, dan zal hij de betrokkene van deze wijziging op de hoogte moeten stellen. De aard van de gegevens, de aard van de gegevensverwerking, de omstandigheden waaronder de verantwoordelijke de gegevens verzameld, of het gebruik dat van de gegevens wordt gemaakt, bepalen of het nodig is aanvullende informatie te verstrekken (derde lid). De afhankelijke positie van de betrokkene ten opzichte van de verantwoordelijke kan bijvoorbeeld aanleiding zijn deze uitgebreider te informeren.
Als aan de informatieplicht overeenkomstig de artikelen 33 of 34 is

voldaan, zijn deze artikelen uitgewerkt en zal er ook geen sprake meer kunnen zijn van een onrechtmatige verkrijging wegens niet nakoming van deze plicht. De betrokkene is daardoor in de gelegenheid van zijn kant het initatief te nemen om navraag te doen naar de gegevensverwerking. Wel is het denkbaar dat specifieke omstandigheden met zich brengen, dat informatie moet worden verstrekt om een «behoorlijke en zorgvuldige verwerking» te waarborgen. Daarbij valt te denken aan latere ontwikkelingen van zodanige aard, dat zij aan de betrokkene bij de verkrijging hadden moeten worden medegedeeld indien zij op dat tijdstip bekend waren geweest.

5. Het moment van de informatieverstrekking

De WPR hanteert in artikel 28 als aanknopingspunt voor de bepaling van het moment waarop de informatieverplichting ontstaat: het tijdstip waarop de verantwoordelijke voor de eerste keer gegevens van de betrokkene opneemt in een persoonsregistratie. Er wordt in de WPR geen onderscheid gemaakt tussen gegevensvergaring bij de betrokkene zelf dan wel vergaring op een andere wijze.
Het moment waarop de verantwoordelijke informatie omtrent de gegevensverwerking aan de betrokkene moet verstrekken, hangt in dit wetsvoorstel af van de vraag of de persoonsgegevens worden verzameld bij de betrokkene zelf of op andere wijze.
Artikel 33 kiest voor het ontstaan van de informatieverplichting van de verantwoordelijke in geval van verkrijging bij de betrokkene zelf, voor het moment voorafgaande aan de daadwerkelijke verkrijging van de gegevens. Bij de vergaring moet dus de informatie bij de betrokkene aanwezig zijn, hetzij omdat hij al op de hoogte is, hetzij omdat de verantwoordelijke hem daarvan op de hoogte heeft gesteld. Artikel 34 regelt de situaties waarin artikel 33 niet van toepassing is. Uitgangspunt is dat de informatie moet worden verstrekt op het moment van vastlegging. Artikel 28 WPR behoudt hier in dit opzicht zijn werking. Artikel 11, eerste lid, van de richtlijn bepaalt dat in bepaalde gevallen de informatie ook mag worden verstrekt «uiterlijk op het moment van de eerste verstrekking». Deze omschrijving moet aldus worden verstaan dat het gaat om gevallen waarin verstrekking van gegevens aan een derde reeds bij de verkrijging is beoogd en de gegevens dus bestemd waren om aan een derde te worden verstrekt. De formulering van onderdeel b sluit hier op aan. Zie in dit verband ook overweging 39 bij de richtlijn.

6. Uitzonderingen op informatieplicht

De gedachte achter het informeren van de betrokkene is de transparantie van de gegevensverwerking. De verantwoordelijke moet actief en ongevraagd de betrokkene van de gegevensverwerking op de hoogte stellen, tenzij deze reeds op de hoogte is. Dit kan bijvoorbeeld het geval zijn als de vorige verantwoordelijke informatie verstrekt heeft. Wordt op dit beginsel een uitzondering gemaakt, dan zal de transparantie op andere wijze gecreëerd moeten worden.
De plicht om de betrokkene van deze nieuwe gegevensverwerking in kennis te stellen is niet absoluut (artikel 34, vierde lid). Het is niet altijd mogelijk de betrokkene te achterhalen. Ook zijn er gevallen waarin het theoretisch mogelijk zou zijn om de betrokkene op de hoogte te stellen, maar waarbij de vereiste inspanning in geen verhouding staat tot het doel dat daarmee wordt gediend. De vraag of er sprake is van een «onevenredige inspanning» is mede afhankelijk van bijvoorbeeld de mate waarin andere wegen openstaan om de betrokkenen op adequate wijze van informatie te voorzien en het medium waarvan mag worden aangenomen dat het de betrokkene voor een groot gedeelte bereikt. Indien het naleven van de informatieplicht een onevenredige inspanning zou vergen, kan

worden afgezien van de informatieverstrekking aan de betrokkene (artikel 34, vierde lid). In dat geval moet er echter zijn voorzien in compenserende waarborgen. Het wetsvoorstel voorziet in het vierde lid van artikel 34 in dergelijke compenserende waarborgen door te bepalen dat de verantwoordelijke, in de gevallen dat hij niet alle betrokkenen in kennis heeft kunnen stellen van de gegevensverwerking, vastlegt van wie en op welke wijze hij de gegevens heeft verkregen. Dit stelt de betrokkenen in staat achteraf bij de verantwoordelijke na te gaan welke keten van verstrekkingen heeft plaatsgevonden. Ingevolge artikel 35, tweede lid, kan dan altijd de betrokkene achteraf op zijn verzoek de informatie krijgen om de keten van verstrekkingen voor zichzelf te reconstrueren.
Indien een gegevensverwerking plaatsvindt door instellingen voor wetenschappelijk onderzoek of statistiek ten behoeve van statistische of wetenschappelijke doeleinden, wordt hier kortheidshalve verwezen naar de bijzondere regeling in artikel 44.
Een uitzondering geldt voorts op grond van het vijfde lid van artikel 34 in geval de registratie of de verstrekking van gegevens plaatsvindt ingevolge een wettelijk voorschrift. Zo laat artikel 9 van de Wet op het Centraal bureau en de Centrale Commissie voor de statistiek (Stb. 1996, 258) toe dat het CBS gebruik maakt van gegevens van het Rijk. Voor het bedrijfsleven geldt een regeling op grond van van de wet van 28 december 1936 houdende maatregelen tot het verkrijgen van juiste economische statistieken (Stb. 1936, 639 DD). Het informeren van de betrokkene kan dan achterwege blijven. Voor deze uitzondering geldt dat de wettelijke basis zodanig specifiek dient te zijn, dat de betrokkene uit de wet kan weten welke verantwoordelijke hij desgewenst kan aanspreken. De richtlijn eist in artikel 11, derde lid, verder dat in een dergelijke wettelijke regeling passende waarborgen zijn gegeven. Deze liggen besloten in artikel 11 van de eerstgenoemde wet dat bepaalt dat de ontvangen gegevens uitsluitend worden gebruikt voor statistische doeleinden. Voorts bepaalt het vijfde lid dat de verantwoordelijke de betrokkene wanneer hij daarom verzoekt op de hoogte moet stellen van het specifieke wettelijke voorschrift dat tot de verstrekking of vastlegging van hem betreffende gegevens heeft geleid. Deze waarborg sluit aan bij die in de Duitse wetgeving in dergelijke gevallen is voorzien (artikel 13 van de Bundesdatenschutzgesetz).

7. Verhouding tussen de artikelen 33 en 34

Artikel 33 regelt de situatie dat de gegevens worden verkregen bij de betrokkene zelf. Dat wil zeggen dat de betrokkene zelf, actief zijn persoonsgegevens ter beschikking stelt dan wel een vertegenwoordiger dit namens hem doet. De betrokkene bepaalt of en – zo ja – welke gegevens worden verstrekt. Hij zal dit doen nadat hij – indien hij daarvan niet al op de hoogte is – is geïnformeerd over de identiteit van de houder en de doeleinden van de verwerking. Hij zal zich ook bewust moeten zijn van het feit dat hij gegevens verstrekt. De verstrekking moet zijn beoogd. In het kader van artikel 33 hoeft er geen sprake te zijn van een direct contact tussen de betrokkene en de verantwoordelijke. De betrokkene kan eveneens door een bewerker worden benaderd en aan deze zijn persoonsgegevens verstrekken. De gegevensvergaring met behulp van videocamera's kan onder artikel 33 worden geschaard indien het geen geheime observatie betreft. Indien de betrokkene op de hoogte is van de aanwezigheid van camera's en hij eveneens weet voor welk doel deze gebruikt worden, heeft hij de mogelijkheid zich hieraan te onttrekken. Doet hij dat niet dan kan gesteld worden dat hij zijn persoonsgegevens voor het desbetreffende doel bewust ter beschikking heeft gesteld. Soortgelijke opmerkingen kunnen worden gemaakt ten aanzien van iemand die zijn chipkaart gebruikt om een specifieke betaling te kunnen verrichten. Overhandigt hij zijn kaart met dit doel aan een daartoe aangewezen

persoon, dan kan gesteld worden dat hij zijn persoonsgegevens verstrekt ten einde die betaling mogelijk te maken. De overhandiging symboliseert de fysieke overdracht van zijn gegevens, de omvang van de gegevens die daadwerkelijk verwerkt mogen worden wordt bepaald door hetgeen in het maatschappelijk verkeer gebruikelijk is om een betaling te kunnen verrichten.
Artikel 34 bestrijkt alle gevallen die niet onder het bereik van artikel 33 vallen.
Indien de verantwoordelijke de betrokkene heeft geïnformeerd op grond van artikel 33 zal hij de gegevens vervolgens kunnen verwerken. Mocht deze verdere verwerking inhouden dat hij de gegevens aan derden verstrekt, dan zal hij in beginsel niet wederom verplicht zijn de betrokkene te informeren. In zoverre heeft de informatieverplichting een eenmalig karakter. De derde zal echter wel op grond van artikel 34 verplicht zijn de betrokkene op de hoogte te stellen van het feit dat hij zijn gegevens heeft verkregen. Deze verplichting geldt niet indien de betrokkene reeds van deze derdenverstrekking op de hoogte is, bijvoorbeeld omdat de verstrekkende verantwoordelijke overeenkomstig artikel 33, derde lid, hem reeds van de voorgenomen derdenverstrekking op de hoogte heeft gesteld.
Een soortgelijke opmerking kan worden gemaakt ten aanzien van artikel 34. Indien de verantwoordelijke de betrokkene in overeenstemming met dit voorschrift heeft geïnformeerd, zal hij de gegevens vervolgens verder kunnen verwerken voor zover dat in lijn ligt met de informatie die aan betrokkene is verstrekt. Het eenmalig karakter van de informatie-verplichting komt in dit artikel tot uitdrukking met de woorden «op het moment van vastlegging».

HOOFDSTUK 6 RECHTEN VAN DE BETROKKENE

De regeling van de rechten van de betrokkene in de artikelen 35 tot en met 39 geeft uitvoering aan artikel 12 van de richtlijn. Deze regeling volgt in grote lijnen de desbetreffende regeling in de WPR. De overige artikelen in hoofdstuk 6 voeren de artikelen 14 en 15 van de richtlijn uit.

Artikel 35

Eerste lid

Een belangrijk onderdeel van het transparantiebeginsel is dat een ieder in beginsel in de gelegenheid moet zijn om na te kunnen gaan of zijn gegevens worden verwerkt. De betrokkene die de wijze waarop zijn gegevens worden verwerkt onrechtmatig vindt, moet in staat zijn dit zelf in rechte aan te vechten. Het gaat om het grondrecht vermeend onrecht ter toetsing aan de rechter voor te kunnen leggen (artikel 13 EVRM). Hij moet zich daartoe, zonder geconfronteerd te worden met bovenmatige kosten, tot de verantwoordelijke kunnen wenden (zie ook de toelichting op het begrip «verantwoordelijke» in artikel 1, onder d). Daar waar er ingevolge artikel 43 uitzonderingen gelden op dit beginsel, kan hij de tussenkomst van de Registratiekamer inroepen.
Artikel 12, aanhef van onderdeel a, van de richtlijn bevat de clausule «met redelijke tussenpozen». Deze clausule, die ook voorkomt in artikel 8, onder b, van het Verdrag inzake gegevensbescherming, is in het eerste lid overgenomen. Als gevolg hiervan is het de betrokkene niet toegestaan de verantwoordelijke meer dan gemiddeld en noodzakelijk te benaderen met verzoeken om informatie. Overigens de verantwoordelijke buitensporige verzoeken om informatie ook reeds afwijzen op grond van artikel 43, onder e. Op grond van het laatstgenoemde artikel kan het recht op toegang van de betrokkene worden beperkt wanneer rechten en vrijheden van anderen dan van de betrokkene, bijvoorbeeld van de verantwoorde-

lijke, daartoe noodzaken. Ook op grond van artikel 30, onder e, WPR, werd reeds aangenomen dat een betrokkene geen buitensporige verzoeken kan doen aan de verantwoordelijke. Voor verdere nuanceringen zij verwezen naar de toelichting op artikel 43.
Sommige wetten kennen een nader uitgewerkt regime voor de kennisneming van persoonsgegevens, bij voorbeeld de artikelen 14 e.v. van de Archiefwet 1995. Deze bepalingen zijn in overeenstemming met de richtlijn. Uit de aard van deze bepalingen vloeit voort dat zij – wanneer het gaat om persoonsgegevens die zijn opgenomen in archiefbescheiden die zijn overgebracht naar een archiefbewaarplaats in de zin van deze wet – voorgaan voor de algemene bepalingen van het onderhavige artikel. Soortgelijke opmerkingen kunnen worden gemaakt ten aanzien van de openbaarheidsregeling in de Kadasterwet, te weten in de artikelen 99 tot en met 107. In deze bijzondere wetten is tevens voorzien in een onkostenvergoeding in de gevallen dat een verzoek om inzage wordt gedaan. Artikel 39 is in dergelijke gevallen dan eveneens niet van toepassing.

Tweede lid

Het tweede lid vergt van de verantwoordelijke dat indien inderdaad gegevens worden verwerkt hij de betrokkene een volledig overzicht ter beschikking stelt van de gegevens met inlichtingen over doel, de aard van de gegevens en van de ontvangers, alsmede over de herkomst van de gegevens.
De hiervoor genoemde rechten van de betrokkene vloeien voort uit artikel 12, onder a, eerste en tweede streepje van de richtlijn. Artikel 35 sluit aan bij artikel 29, eerste en tweede lid, WPR met dien verstande dat het antwoord van de verantwoordelijke aan de betrokkene, in het geval diens gegevens worden verwerkt, aan nadere eisen is onderworpen: het doel van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers aan wie de gegevens worden verstrekt, dienen dan te worden meegedeeld.
Het voorschrift dat de beschikbare informatie over de herkomst van de gegevens van de gegevens moet worden meegedeeld, sluit aan bij de formulering van artikel 29, tweede lid, slot, WPR, met dien verstande dat het wetsvoorstel – anders dan de WPR – tot uitdrukking brengt dat geen bijzondere plicht in het leven wordt geroepen om gegevens over de herkomst vast te leggen. Voor zover echter hierover, hetzij in algemene zin, danwel in het concrete geval, bijzonderheden aan de verantwoordelijke bekend zijn, dienen deze ook aan de betrokkene te worden kenbaar gemaakt.
Niet uit te sluiten valt dat honorering van een inzageverzoek van betrokkene tevens enig inzicht zal geven in gegevens die op anderen betrekking hebben. De betrokkene kan daar ook belang bij hebben. Dit kan bijvoorbeeld het geval zijn indien bij de registratie van gegevens over de betrokkene tevens wordt aangegeven van wie die gegevens afkomstig zijn. Onder omstandigheden zal de verantwoordelijke verplicht zijn ook deze gegevens te verstrekken. Verwezen zij naar hetgeen daarover in de vorige alinea is opgemerkt. Verstrekking van dergelijke informatie aan de betrokkene op grond van artikel 35 kan derhalve niet worden uitgesloten. Op grond van de belangenafweging die de verantwoordelijke zal hebben te verrichten, zal moeten worden bezien of inzage kan worden toegestaan en zo ja, in hoeverre in verband met de rechten en vrijheden van anderen als bedoeld in artikel 43 afscherming van op anderen betrekking hebbende informatie dient plaats te vinden. In verband met het waarborgen van de belangen van derden in deze afweging zij voorts verwezen naar het derde lid.
De uitoefening van het recht van toegang is geen inbreuk op het auteursrecht. Ingevolge de richtlijn betreffende de rechtsbescherming van databanken[1] rust op een lijst van abonnees die langs geautomatiseerde

[1] Gemeenschappelijk standpunt van 21 juni 1995.

weg toegankelijk is, een auteursrecht, althans een daarmee vergelijkbaar recht. In beginsel is het zonder toestemming van de rechthebbende niet toegestaan uit de inhoud van een auteursrechtelijk werk openbaar te maken. Dit recht van de rechthebbende gaat echter niet zover dat het aan de uitoefening van het recht op kennisneming door de betrokkene in de weg staat. Het gaat immers slechts om de bekendmaking aan een enkele persoon, die op een dergelijke bekendmaking krachtens een bijzonder recht aanspraak kan maken. De grondslag van dit recht op kennisneming ligt in het feit dat het gegeven de betrokkene betreft. Het recht van de auteur wijkt, voor zover het betreft persoonsgegevens, voor het recht van de persoon op kennisneming van de hem betreffende gegevens. Dit raakpunt tussen het auteursrecht en het recht op gegevensbescherming gaat niet verder dan alleen de bekendmaking aan dat individu c.q. de verbetering van die gegevens. De verstrekking aan de betrokkene van hem betreffende persoonsgegevens is geen openbaarmaking in de zin van het auteursrecht.

Derde lid

In de toelichting bij het tweede lid is reeds ingegaan op de betrokkenheid van derden-belanghebbenden bij de beslissing omtrent verzoeken om kennisneming. Om de belangen van derden in dergelijke situaties te waarborgen is nodig dat deze op de hoogte worden gesteld van een eventueel voornemen tot honorering van het verzoek en in de gelegenheid worden gesteld daaromtrent hun zienswijze kenbaar te maken. Deze mogelijkheid is essentieel omdat juist in de fase waarin kennisneming door de betrokkene nog niet heeft plaatsgevonden, schade aan de belangen van derden kan worden voorkomen. Daartoe dient het derde lid. Voor de publieke sector vormt de bepaling een verbijzondering ten opzichte van artikel 4:8 Awb.
Met betrekking tot de verplichting van het derde lid gelden enkele restricties. Uiteraard behoeft de verantwoordelijke een derde alleen te horen indien deze daar een gerechtvaardigd belang bij heeft. Blijkens de formulering is dit het geval indien de voorgenomen mededeling aan de betrokkene gegevens bevat die de derde betreffen en voorts redelijkerwijs verwacht mag worden dat de derde tegen die mededeling bedenkingen zal hebben. Dit laatste is bijvoorbeeld niet het geval indien de derde bij de verstrekking van gegevens aan de verantwoordelijke heeft ingestemd met een eventuele, op die gegevens betrekking hebbende mededeling aan de betrokkene. Voorts geldt de verplichting niet indien nakoming daarvan onmogelijk blijkt of een onevenredige inspanning kost. Bij de kennisgeving en raadpleging van de derde kunnen zich dezelfde problemen voordoen als bij de informatieverplichting op grond van artikel 34. Om die reden is hier de dezelfde uitzonderingsclausule opgenomen. In dit verband zij verwezen naar de toelichting op artikel 33 en 34.

Vierde lid

Het vierde lid bevat een bijzondere bepaling in geval bijzondere computerprogrammatuur een wijze van verwerking mogelijk maakt die de betrokkene niet reeds duidelijk is uit de mededeling ingevolge het tweede lid. Een dergelijke mededeling kan in algemene bewoordingen worden gedaan. Blijkens overweging 41 van de richtlijn, kan deze verplichting geen afbreuk mag doen aan het zakengeheim of aan de intellectuele eigendom en met name aan het auteursrecht dat de software beschermt. Zulks mag er evenwel niet toe leiden dat de betrokkene alle informatie wordt geweigerd.

Artikel 36

eerste lid

Dit voorschrift vormt een implementatie van onderdeel b van artikel 12 van de richtlijn en sluit grotendeels aan bij artikel 31 WPR. Ook op grond van artikel 36 kan de betrokkene correctie verzoeken indien de gegevens feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijke voorschrift worden verwerkt. Het hoeft niet altijd te gaan om een de verantwoordelijke verwijtbare onrechtmatige gedraging. Indien bepaalde persoonsgegevens feitelijk onjuist zijn, heeft de betrokkene ook recht op verbetering zonder dat de verantwoordelijke tekort is geschoten in zijn zorgplicht voor de juistheid van die gegevens. Voorts biedt het artikel de verantwoordelijke de mogelijkheid gegevens af te schermen, indien de verwerking ervan onrechtmatig zou zijn. Het is bijvoorbeeld nodig dergelijke gegevens toch te bewaren met het oog op mogelijke gerechtelijke procedures. Deze mogelijkheid werd overigens ook reeds op grond van artikel 31 WPR aanwezig geacht.

derde en vierde lid

Het derde lid verplicht de verantwoordelijke de verbeteringen aan te brengen.
Het vierde lid voorziet in dit opzicht in een bijzondere regeling. Sommige gegevens worden verwerkt op gegevensdragers die technisch geen wijzigingen toelaten, bijvoorbeeld op microfiche of CD-ROM. De betrokkene kan echter niet van zijn rechten worden ontbloot louter op grond van de beslissing van de verantwoordelijke inzake de door hem te gebruiken techniek. Aan de andere kant is het onwenselijk dat de wet de toepassing van bepaalde technieken zou verbieden. Een oplossing van dit dilemma kan daarin worden gevonden dat de verantwoordelijke aanvullende voorzieningen treft om toch bij het gebruik van de opgeslagen gegevens de gebruiker te voorzien van de juiste gegevens. Dit kan bijvoorbeeld aldus dat bij raadpleging van een duurzame gegevensdrager, de gebruiker telkens wordt gewezen op de noodzaak een aanvullend bestand te raadplegen waarin eventuele verbeteringen zijn opgenomen. De juridische evaluatie heeft de wenselijkheid van een bijzondere regeling voor duurzame gegevensdragers aan het licht gebracht. Correctie behoeft dus niet in alle omstandigheden te betekenen dat de onjuist gebleken persoonsgegevens worden verwijderd of vernietigd. Zo geldt ook voor archiefbescheiden die zijn overgebracht naar een archiefbewaarplaats als bedoeld in de Archiefwet 1995 de praktijk van handhaving van de onjuiste gegevens met daarnaast deponering van de lezing van betrokkene bij het betwiste stuk (zie eveneens paragraaf 15.2 van het algemeen deel van de toelichting).

vijfde lid

Het vijfde lid stelt buiten twijfel dat het wetsvoorstel aanvullend is ten opzichte van bijzondere regelingen die een eigen procedure voor verbetering kennen. Voor zover deze bijzondere regelingen onder het communautaire recht vallen, dienen deze uiteraard wel aan de eisen die de richtlijn voldoen.

Artikel 37

Dit voorschrift komt overeen met het derde tot en met vijfde lid van artikel 29 WPR. Niet in alle gevallen kan het gewenst zijn dat de verzoeker een schriftelijk bericht van de verantwoordelijke ontvangt. Het kan in het

belang van de betrokkene zijn om de reactie van de verantwoordelijke mondeling te vernemen, bijvoorbeeld om te voorkomen dat van de betrokkene vervolgens door derden gevraagd wordt deze informatie te overhandigen. Indien daarvoor gegronde redenen zijn zal de verantwoordelijke op andere wijze aan het verzoek tot het geven van informatie moeten voldoen (eerste lid).
De verantwoordelijke moet de identiteit van de verzoeker vaststellen om te voorkomen dat iemand door het gebruik van de naam van een ander gegevens over deze kan krijgen (tweede lid). Welke waarborgen in een bepaald geval voldoende zijn hangt af van de aard van de registratie. Zo zouden bijvoorbeeld, wanneer het belang van de betrokkene daardoor niet kan worden geschaad, de gegevens slechts naar het adres dat in de registratie staat vermeld kunnen worden verzonden. In andere gevallen zal de verzoeker eventueel in persoon moeten verschijnen.

Artikel 38

Dit voorschrift, dat een implementatie is van artikel 12, derde lid, van de richtlijn, sluit in zekere zin aan bij artikel 35 WPR. De verantwoordelijke die naar aanleiding van een verzoek op grond van artikel 36 persoonsgegevens heeft verbeterd, aangevuld, verwijderd of afgeschermd, is verplicht om aan derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, kennis te geven van de verbetering, aanvulling, verwijdering of afscherming, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost. Er is echter een belangrijk verschil.
De mededelingsplicht geldt niet indien het doen van een mededeling onmogelijk blijkt of een onevenredige inspanning kost. De clausulering van de uitzondering op deze mededelingsplicht verschilt enigszins van die van artikel 35 WPR, waar is bepaald dat de verantwoordelijke een mededeling dient te doen aan degenen aan wie hij naar zijn weten in het jaar voorafgaand aan het verzoek en in de sinds dat verzoek verstreken periode de betrokken gegevens heeft verstrekt. Deze bepaling moet worden gelezen tegen de achtergrond van artikel 32, tweede lid, tweede volzin, WPR. Beide bepalingen tezamen betekenen een indirekte protocolplicht in die zin dat elke individuele verstrekking moet worden vastgelegd, indien de verantwoordelijke ten tijde van de verstrekking redelijkerwijs kan aannemen dat het belang van de geregistreerde door de verstrekking onevenredig kan worden geschaad. Dit vereist dat de verantwoordelijke ten tijde van de verstrekking een afweging maakt.
Een dergelijke protocolplicht kent het onderhavige wetsvoorstel niet. Slechts is voorgeschreven in artikel 28, derde lid, dat verstrekkingen die afwijken van de melding van de gegevensverwerking bij de Registratiekamer of de functionaris, worden vastgelegd. De nieuwe bepaling geeft de verantwoordelijke meer houvast, omdat hij niet meer zoals onder de WPR, vooraf bij elke verstrekking hoeft af te wegen of vastlegging (protocollering) nodig is. De melding kan categorieën van ontvangers betreffen en zolang een individuele verstrekking plaatsvindt aan een persoon die valt onder één van de aangemelde categorieën, behoeft geen vastlegging van de individuele verstrekking plaats te vinden.
Onder de werking van artikel 35, eerste lid, WPR moest de houder alle derden aan wie hij verstrekt heeft in het afgelopen jaar voor zover hij die heeft vastgelegd, en die hij dus daarom «weet», inlichten over eventuele verbeteringen. In het onderhavig wetsvoorstel reikt de protocolplicht van de verantwoordelijke minder ver, maar daar staat tegenover dat in het enkele geval dat daadwerkelijk een verbetering noodzakelijk is, op de verantwoordelijke ook een onderzoeksplicht rust om na te gaan aan wie hij heeft verstrekt.
Van deze onderzoeksplicht kan overigens weer worden afgezien als een dergelijk onderzoek onmogelijk zou zijn, of een onevenredige inspanning zou vergen. Het gaat hier om een afweging achteraf en is beperkt tot de

gevallen waarin daadwerkelijk tot verbetering is overgegaan. In dit opzicht is het onderhavig wetsvoorstel minder duidelijk. De evaluaties hebben evenwel duidelijk gemaakt dat het aantal gehonoreerde verzoeken om verbetering van gegevens schaars is.
Mededeling aan derden in de zin van deze bepaling is onmogelijk indien de verantwoordelijke niet meer de beschikking heeft over de informatie aan welke derden hij de gegevens heeft verstrekt. Eveneens mag kennisgeving achterwege blijven indien dit onevenredig veel inspanning vergt. Van de verantwoordelijke van een groot, landelijk verspreid adressenbestand, zoals bijvoorbeeld een telefoonboek, waarin een typefout in de naam van iemand is ontdekt, kan moeilijk gevergd worden dat hij iedereen die dit bestand heeft ontvangen op de hoogte stelt. Hetzelfde geldt voor omvangrijke openbare registers – zoals bijvoorbeeld de door het Kadaster gehouden kadastrale registratie – die door een ieder vrijelijk kunnen worden geraadpleegd. Evenmin kan in de regel van de verantwoordelijke worden verwacht derden op de hoogte te stellen aan wie hij in het verre verleden eens de gegevens heeft verstrekt.
Bij de vraag hoever de onderzoeksplicht reikt, speelt een rol de aard van de verbetering en de aard van de persoonsgegevens waar het om gaat. De verbetering van strafrechtelijke gegevens, bijvoorbeeld dat de betrokkene is vrijgesproken van een telastgelegd strafbaar feit, kan eerder verplichten derden uit een ver verleden op de hoogte te stellen dan de verbetering van een adresgegeven. De formulering van artikel 38 veronderstelt, net als artikel 35, een zekere afweging tussen de belangen van de betrokkene en die van de verantwoordelijke. De betrokkene moet een zeker redelijk belang hebben bij de mededeling van de verantwoordelijke aan de derde dat bepaalde gegevens verbeterd zijn. Ontbreekt een dergelijk belang dan zal eerder sprake zijn van een onevenredige inspanning van de kant van de verantwoordelijke. De afwezigheid van enig belang kan ook blijken indien de verzoeker te kennen heeft gegeven daarop geen prijs te stellen. Waar artikel 35, derde lid WPR dit thans nog met zoveel woorden zegt, dwingt de richtlijn ertoe deze omstandigheid in het geheel van belangen te wegen.
Dit betekent dat onder de WPR volgens een zacht criterium moet worden geprotocolleerd, opdat al de personen aan wie blijkens het protocol was verstrekt over een verbetering kunnen worden geïnformeerd. Volgens het onderhavige wetsvoorstel moet volgens een hard criterium worden geprotocolleerd, namelijk in het geval dat in afwijking van de melding een verstrekking plaatsvindt. Dit zijn echter uitzonderingen, omdat toch alle structurele verstrekkingen ingevolge artikel 28, tweede lid ten van hoogste een jaar terug moeten zijn aangemeld. Een reële vermeerdering van de lastendruk kan daarom op grond van deze bepaling niet worden verwacht.
Het tweede lid van artikel 38 komt overeen met het tweede lid van artikel 35 WPR, zij het dat de verplichting van de verantwoordelijke om de betrokkene in te lichten over degenen aan wie verbeteringen zijn doorgegeven is beperkt tot de situatie dat de betrokkene daar uitdrukkelijk om vraagt. Dit is een precisering van de rechten van de betrokkenen onder de werking van de richtlijn en een beperking ten opzichte van de WPR.

Artikel 39

Dit artikel sluit aan bij artikel 36 WPR. De omvang van de vergoeding zal naar alle verwachting niet wijzigen. Op grond van het besluit van de Minister van Justitie van 5 juli 1989, houdende vaststelling van de maximale vergoeding van de kosten van een bericht als bedoeld in de artikelen 29 en 32 van de Wet persoonsregistraties (Stb. 281), bedraagt de vergoeding ten aanzien van de berichten als bedoeld in de artikelen 29 en 32 WPR tien gulden.De mogelijkheid is aanwezig de omvang van de vergoeding bij ministeriële regeling vast te stellen. Wanneer de verant-

woordelijke weigert aan het verzoek te voldoen op één van de gronden, genoemd in artikel 43 is er geen sprake van een bericht als bedoeld in artikel 35 en geldt artikel 39 niet.
Het derde lid stelt buiten twijfel dat wanneer bijzondere wettelijke regelingen bestaan voor de vergoeding van kosten, deze bijzondere regeling voorgaat. Een voorbeeld is artikel 108 van de Kadasterwet.

Artikel 40

Deze bepaling richt zich op een rechtmatige gegevensverwerking, die pas onrechtmatig wordt nadat de betrokkene op grond van een bijzondere situatie verzet aantekent en dit verzet gerechtvaardigd wordt geacht. Het begrip «verzet» is overgenomen uit artikel 14 van de richtlijn. Verzet kan worden aangetekend tegen verwerkingen op grond van artikel 8, onderdelen e en f.
Artikel 8, onderdeel e, biedt grondslag aan de gegevensverwerking door een bestuursorgaan voor de vervulling van een publieke taak. De beantwoording van de vraag of een gegevensverwerking voor dat doel daadwerkelijk noodzakelijk is laat aan de verantwoordelijke een zekere beoordelingsruimte over. Bij de beoordeling van de noodzaak zullen bijvoorbeeld de beginselen van proportionaliteit en subsidiariteit een belangrijke rol spelen. De beslissing die de verantwoordelijke vervolgens neemt zal slechts rekening houden en ook kunnen houden met de hem kenbare, normale omstandigheden van het geval. Deze omstandigheden afwegende kan hij tot de beslissing komen dat de gegevensverwerking gerechtvaardigd is. Het is echter mogelijk dat de bijzondere persoonlijke omstandigheden van een bij de verwerking betrokkene de balans doen doorslaan naar de andere kant. De betrokkene kan in dat geval verzet aantekenen tegen de verwerking door de verantwoordelijke.
Voorts is verzet mogelijk tegen verwerkingen die zijn gebaseerd op artikel 8, onderdeel f. Dit artikel vereist reeds expliciet van de verantwoordelijke dat hij een afweging maakt van de meespelende belangen, hij dient een afweging te maken van enerzijds het gerechtvaardigd belang van de verantwoordelijke of van een derde; anderzijds het belang van de betrokkene op bescherming van de persoonlijke levenssfeer. De verhouding tussen deze bepaling en artikel 8, onder f, is de volgende. Ook hier geldt dat de verantwoordelijke de belangen afweegt zoals deze aan hem bekend zijn, maar onder omstandigheden zal van hem kunnen worden verwacht nader onderzoek te doen naar het gewicht van deze belangen. De afweging zal in dit stadium evenwel in de regel een enigszins algemeen karakter hebben. Er blijft daardoor altijd de mogelijkheid, hoe zorgvuldig en nauwkeurig deze afweging ook heeft plaatsgevonden, dat in een individueel geval een belangenafweging anders had moeten uitvallen. De oorzaak kan liggen in een omstandigheid die de verantwoordelijke niet bekend was en niet had kunnen zijn. Deze omstandigheid kan reeds hebben bestaan bij het begin van de gegevensverwerking, maar ook later opgekomen zijn. In dergelijke gevallen heeft de betrokkene aanspraak op een hernieuwde afweging in zijn concrete geval. Het ligt dan uiteraard op zijn weg deze afweging aan de orde te stellen. Als voorbeeld valt te denken aan een situatie dat op een centraal punt medische gegevens zijn vergaard voor epidemiologisch onderzoek en dat alle geldende regels in acht zijn genomen. De situatie kan zich voordoen dat een patiënt, wiens gegevens daar in een herleidbare vorm zijn opgeslagen, verneemt dat een bekende van hem, voor wie hij zijn ziekte verborgen wil houden, als onderzoeker bij dat centrum is aangesteld. Hij kan er dan persoonlijk een gerechtvaardigd belang bij hebben dat de hem betreffende gegevens worden verwijderd, of zodanig worden bewerkt dat zij redelijkerwijs niet meer tot hem herleidbaar zijn. Deze bepaling kent hem de aanspraak toe dat het betreffende gegeven ook daadwerkelijk wordt verwijderd.

Het verzet kan betrekking hebben op alle vormen van gegevensverwerking. Zo is het mogelijk dat de betrokkene weliswaar een gerechtvaardigd belang geldend kan maken dat de hem betreffende gegevens niet aan bepaalde ontvangers worden verstrekt, zonder dat daaraan evenwel de conclusie kan worden verbonden dat die gegevens ook worden gewist. In dat geval zal bij de gegevens een aantekening moet worden geplaatst dat de desbetreffende verstrekkingen niet kunnen plaatsvinden. In gevallen van on-line raadpleging zullen wijzigingen in de computerprogrammatuur moeten plaatsvinden die de aan de orde zijnde verspreiding van de desbetreffende gegevens onmogelijk maakt (blokkering).
Voor een bijzondere categorie van gevallen bepaalt het onderhavige artikel dat het recht van verzet niet van toepassing is. Het betreft de openbare registers die bij wet zijn ingesteld. Voor deze categorie geldt dat de bijzondere wetgever reeds heeft beslist dat er in het belang van het rechtsverkeer sprake dient te zijn van bepaalde registers met een nauw omschreven inhoud die door een ieder moeten kunnen worden geraadpleegd. In dergelijke situaties is er voor een nadere belangenafweging door de verantwoordelijke geen plaats meer. Om die reden wordt het recht van verzet voor deze registers in het vierde lid uitgesloten.
Het aantekenen van verzet is vormvrij: de betrokkene is vrij in de wijze waarop hij zich tot de verantwoordelijke richt met zijn bezwaren tegen de gegevensverwerking. Indien de betrokkene verzet heeft aangetekend is de verantwoordelijke gehouden binnen een termijn van vier weken de bij de verwerking spelende belangen opnieuw tegen elkaar af te wegen, daarbij rekening houdend met de door de betrokkene aangevoerde bijzondere omstandigheden. De verantwoordelijke is niet verplicht de aangevochten verwerking terstonds te staken. Een afwijzing van verzoek tot honorering van het verzet geldt krachtens artikel 45 als een besluit in de zin van artikel 1:3 Awb. Tegen een dergelijke beslissing staat voor de betrokkene bezwaar en beroep open. Heeft de betrokkene een dringend belang bij het onmiddelijk staken van de verwerking dan dient hij een voorlopige voorziening bij de bestuursrechter te vragen. Wordt het verzoek van de betrokkene alsnog gehonoreerd door de rechter dan dient de rechterlijke uitspraak uiteraard terstonds door de verantwoordelijke te worden uitgevoerd. De betrokkene heeft echter geen recht op schadevergoeding op grond van artikel 49 van dit wetsvoorstel aangezien de verwerking pas een onrechtmatig karakter krijgt indien de verantwoordelijke de verwerking voorzet nadat de rechter heeft geoordeeld dat het verzet van de betrokkene gerechtvaardigd is.

Artikel 41

a. Het begrip «direct marketing»

Bedrijven hebben in beginsel een gerechtvaardigd commercieel belang bij het onderhouden van rechtstreekse contacten met hun klanten. Verder hebben zij belang bij het verwerven van nieuwe klanten. Eén van de vormen die zij daarbij gebruiken is het benaderen van individuele, op naam geselecteerde klanten teneinde hun een commerciële aanbieding te doen via de post, per telefoon, of met gebruikmaking van een ander interactief te gebruiken medium. Deze activiteit pleegt te worden aangeduid met het Engelse begrippenpaar «direct marketing».[1] De Nederlandse vertaling, «rechtstreeks, persoonlijk vermarkten», mag zich nog niet verheugen in toereikende inburgering in het algemeen taalgebruik. Vergelijkbare technieken voor het instandhouden van het contact met de achterban worden gebruikt door non-profitinstellingen die personen benaderen voor charitatieve doeleinden. Het begrip «fund raising» kan worden vertaald met fondsenverwerving.
De in de wetsbepaling voorgestelde omschrijving van direct marketing is

[1] In het Spellingbesluit (Stb. 1996, 394) houdende voorschriften omtrent de schrijfwijze van de Nederlandse taal, komen beide begrippen afzonderlijk wel voor.

ontleend aan elders gegeven omschrijvingen. In de gedragscode van het Direct Marketing Instituut Nederland[1] die is goedgekeurd door de Registratiekamer, wordt het begrip «direct marketing» omschreven als «het marketingsysteem gericht op het tot stand brengen of houden van een directe relatie tussen aanbieder en diens afnemers». Deze omschrijving gebruikt een aantal nieuwe begrippen die in de context van de wet afzonderlijke definiring zouden behoeven en is daarom niet in deze vorm overgenomen. De Aanbeveling[2] van 25 oktober 1985 van het Comité van Ministers van de Raad van Europa over direct marketing[3] geeft de omschrijving «alle activiteiten die het mogelijk maken om goederen of diensten aan te bieden of andere boodschappen te verzenden aan een deel van de bevolking via de post, telefoon of andere middelen, gericht op het informeren van of het uitlokken van een reactie van de betrokkene alsmede enige daarmee verband houdende dienst». Deze omschrijving omvat mede de fondsenwerving voor liefdadige doeleinden, maar sluit niet direct aan bij het begrip gegevensverwerking. De in het wetsvoorstel opgenomen omschrijving bevat evenwel alle genoemde elementen, zij het dat niet nodig bleek ook de middelen die worden gebruikt om het contact te onderhouden te omschrijven. Het omvat mede de toezending van mededelingen dat een bedrijf verhuisd is of dat de uitverkoop is begonnen, voor zover dergelijke mededelingen worden gedaan met het oog op het in het eerste lid genoemde doel.
Direct marketing moet enerzijds worden onderscheiden van huis-aan-huisverspreiding, anderzijds van marktonderzoek. Bij huis-aan-huisverspreiding vindt geen gebruik van persoonsgegevens plaats. Bovendien blijken in de praktijk op de brievenbus geplakte stickers waarmee de betrokkene te kennen geeft geen prijs te stellen op ongevraagde post, toereikend te werken. Bij marktonderzoek worden echter (persoons-) gegevens verwerkt om bijvoorbeeld de ontwikkelingen in de vraag naar een bepaald produkt te voorspellen. Het is daarbij niet van belang of een dergelijk onderzoek plaatsvindt op wetenschappelijke, beleidsmatige of commerciële gronden. Zolang deze gegevens niet worden gebruikt om rechtstreeks de betrokkene te benaderen met een aanbod, is er geen sprake van direct marketing en is de bepaling niet van toepassing.
Direct marketing gebeurt tot dusver meestal via de post. De bepaling richt zich echter evenzeer op toekomstige wijzen om een klant te benaderen. Via telefoon, fax of elektronische communicatie is het ook mogelijk iemand rechtstreeks te benaderen. Deze gevallen worden ook door de onderhavige bepaling bestreken. De richtlijn televerkopen is hierop van toepassing. Artikel 12 van het ontwerp van de richtlijn over de bescherming van de persoonlijke levenssfeer en telecommunicatie (PbEG van 24 oktober 1996, nr C 315/30) geeft bijzondere regels voor de direct marketing met gebruikmaking van automatische oproepsystemen zonder menselijke tussenkomst en faxen. Betrokkenen moeten daarmee uitdrukkelijk vooraf hebben ingestemd. Deze richtlijn zal worden geïmplementeerd in de nieuwe Telecommunicatiewet. Geen bijzondere regels zijn er nog voor direct marketing via elektronische post, bij voorbeeld Internet. Deze vallen daarom onder het voorgestelde artikel 41. Bij de ontvangst van berichten via dit medium is het echter eenvoudig per ommegaande bezwaar te maken tegen toezending. Degene die de boodschappen verzond is dan jegens de betrokkene gehouden maatregelen te treffen om dit bezwaar te honoreren.

b. De toelaatbaarheid van gegevensverwerking voor direct marketing

Op de toelaatbaarheid van de verwerking van persoonsgegevens voor direct marketing zijn wij ingegaan in de toelichting op artikel 9 op het begrip «verenigbaar gebruik» en in de toelichting op de artikelen 33 en 34 onder punt 3. Het gebruik kan in beginsel toelaatbaar worden geacht

[1] Stcrt. 1992, 194.
[2] Aanbeveling R (85) 20 van 25 oktober 1985.
[3] Zie de editie Schuurman & Jordens van de Wet persoonsregistraties, nr 199, tweede druk, blz. 349 e.v.

wanneer het gaat om produkten of diensten die verband houden met of verwant zijn aan de relatie in het kader waarvan de gegevens worden gevraagd. De graad van verwantschap hangt af van wat gebruikelijk is in de markt op een bepaald moment. In andere gevallen is de toestemming van de betrokkene vereist.
De wegen die een commerciële aanbieder van produkten of diensten kan bewandelen om tot contact met (potentiële) klanten te komen, kunnen heel verschillend zijn. De eerste mogelijkheid is die waarbij de aanbieder gebruik maakt van de gegevens die hij zelf tot zijn beschikking heeft. Dit kunnen bijvoorbeeld de gegevens uit zijn eigen klantenbestand zijn. De aanbieder kan bijvoorbeeld zo zijn klanten op de hoogte stellen van nieuwe produkten.
Een tweede mogelijkheid is dat de aanbieder gebruik maakt van een gegevensbestand van een ander, al dan niet samengesteld volgens bepaalde criteria. Vaak zal het gaan om een bedrijf dat het adressenbestand van zijn klanten heeft verkocht aan een ander bedrijf en dit bedrijf kan dan contact opnemen met deze personen, teneinde deze op zijn beurt als zijn klanten te werven. Artikel 34 vergt dat in een dergelijk geval de verkoper – indien althans de verstrekking niet onverenigbaar is met het oorspronkelijke doel – de betrokkenen van deze verstrekking op de hoogte stelt, tenzij dit onmogelijk blijkt of onevenredige inspanning kost. In dat geval dient hij vast te leggen aan wie hij welke gegevens heeft verstrekt, zodat steeds achteraf een keten van verstrekkingen kan worden gereconstrueerd.
De derde mogelijkheid is dat de aanbieder van produkten en diensten een bedrijf de opdracht geeft om, meestal tegen betaling, reclame van de aanbieder te zenden aan de mensen die in het gegevensbestand voorkomen van dat bedrijf. Hierdoor wordt voorkomen dat dat de aanbieder (de derde) zelf de beschikking krijgt over deze adressen.
In al deze drie gevallen is de bepaling van toepassing dat de (oorspronkelijke) verantwoordelijke zorg moet dragen dat slechts reclame wordt toegezonden aan de personen die niet hebben laten weten geen prijs te stellen op de toezending van reclame of ander wervend materiaal. Het is daarbij niet van belang of het gaat om primair gebruik (overeenkomstig het oorspronkelijk doel van de gegevensverwerking), dan wel secundaire gebruik (in afwijking van het oorspronkelijk doel) van gegevens. Dit kan betekenen dat de verantwoordelijke zal moeten vastleggen wie een dergelijk bezwaar heeft gemaakt.
Het bovenstaande is van overeenkomstige toepassing in de verhouding tussen liefdadige instellingen en (potentiële) donateurs. Dit is evenwel niet van toepassing indien een uitgever bij toezending van een tijdschrift aan zijn abonnees een folder van hemzelf of van een derde invoegt. Van een uitgever van een tijdschrift kan niet worden verlangd dat hij bij ieder tijdschrift apart bepaalt of wel of niet een reclamefolder zal worden toegevoegd. Hetzelfde geldt voor bij voorbeeld aankondigingen van nieuwe diensten gevoegd bij de toezending van een bankafschrift of in druk toegevoegd op dit afschrift zelf. Dan is immers geen sprake van de afzonderlijke verwerking van persoonsgegevens voor direct marketing. Dit zou anders zijn wanneer bijvoorbeeld abonnees van een tijdschrift konden worden geselecteerd voor bepaalde reclameboodschappen. De gegevens die een abonnee aan een uitgever bekend heeft gemaakt, zouden dan niet alleen worden gebruikt om het contract uit te voeren dat zij sloten door zich te abonneren op het tijdschrift, maar ook om aan te geven welke informatie ze wel en welke ze niet zouden krijgen. Op de persoon toegespitste mededelingen op een bankafschrift waarbij aandacht zou worden gevraagd voor nieuwe produkten, zouden het resultaat zijn van een afzonderlijke verwerking van persoonsgegevens voor doeleinden van direct marketing en daarom onderworpen aan de onderhavige bepaling.
Indien na toetsing blijkt dat het gerechtvaardigd belang van de verant-

woordelijke of van een derde in de zin van artikel 8, onder f, zwaarder weegt dan het belang van de betrokkene, is de verwerking van persoonsgegevens voor fondsenwerving of direct marketing toelaatbaar. In het geval van gebruik van gegevens in afwijking van het oorspronkelijk doel (het z.g. secundair gebruik), dient daarenboven te worden getoetst of het gebruik van persoonsgegevens voor direct marketing verenigbaar is met het oorspronkelijk doel waarvoor de gegevens zijn verzameld. Wanneer een bedrijf gegevens over zijn cliëntèle gebruikt om produkten of diensten aan te bieden die gelijk of verwant zijn aan produkten of diensten die aanleiding waren voor eerdere contacten, kan het in het algemeen als verenigbaar gebruik worden beschouwd. Wanneer de gegevens voor geheel andere produkten of diensten worden gebruikt of aan derden worden verstrekt, is de mate van gevoeligheid van het criterium op grond waarvan de persoonsgegevens zijn geselecteerd van belang bij de beoordeling van de vraag naar de verenigbaarheid. Het gaat daarbij niet alleen om de gevoelige gegevens die benoemd zijn in het wetsvoorstel, maar ook om andere gegevens die als gevoelig worden aangemerkt, zoals iemands welstand.
Ook in gevallen waarin gegevens niet aan derden worden verstrekt, dient te worden bezien of is voldaan aan de verenigbaarheidseis van artikel 9. Het komt voor dat een bedrijf activiteiten ontplooit in meerdere branches. Wanneer een dergelijk bedrijf een klant zou benaderen met reclame voor een dienstaanbod dat is afgestemd op de gegevens ontleend aan de ene branche, terwijl die dienst met die branche als zodanig niets van doen heeft, is in het algemeen niet aan de verenigbaarheidseis voldaan.
De bijzondere voorschriften van hoofdstuk 2 inzake gevoelige gegevens zijn eveneens van toepassing op de direct marketing. Dergelijke gegevens kunnen hiertoe slechts worden gebruikt indien daarvoor uitdrukkelijk een wettelijke rechtvaardiging is geschapen. Zo zal een ziektekostenverzekeraar de cliënten die hij wil wijzen op een nieuw produkt, niet mogen selecteren op basis van hem bekende gegevens omtrent hun ziekte. Evenmin mogen opticiens die klanten willen informeren over een nieuw middel om lenzen te reinigen, hun zending preciseren door gebruik te maken van de hen ter beschikking staande gegevens over de aanschaf van lenzen. Een dergelijke aanschaf duidt immers op een medisch gegeven, te weten de gesteldheid van de ogen en voor een dergelijk gebruik van gevoelige gegevens bestaat geen wettelijke basis.

c. Het recht van verzet

Het beginsel dat ten grondslag ligt aan artikel 8, onder f, leidt ertoe dat het belang van de verantwoordelijke of van een derde afgewogen moet worden tegen het belang van de geregistreerde. Deze plicht rust op de schouders van de verantwoordelijke. Artikel 40 opent de mogelijkheid dat op verzoek van de betrokkene daarenboven een hernieuwde belangenafweging plaatsvindt op grond van zijn bijzondere omstandigheden. Op het terrein van de direct marketing is aan dit recht in de wet in formele zin een nadere concretisering gegeven door te bepalen dat het verzet van de betrokkene in alle gevallen dient te worden gehonoreerd. Het is niet nodig dat hij zijn belang bij verzet motiveert opdat dit kan worden afgewogen tegenover dat van de verantwoordelijke. Het bezwaar van de betrokkene is daarmee een onweerlegbaar rechtsvermoeden dat zijn belang de doorslag moet geven. De serviceverlening van bedrijven aan hun klanten, bestaande uit alle maatregelen gericht op het attenderen van klanten op (nieuwe) produkten of acties, dient dus achterwege te blijven in de gevallen dat betrokkenen daartegen bezwaar hebben gemaakt. Van direct marketing is eveneens sprake wanneer een betrokkene die via de elektronische snelweg het dienstaanbod raadpleegt, gedurende de wachttijd wordt geconfronteerd met speciaal op hem gerichte reclame.
Het verzet betreft de gegevensverwerking in al zijn fasen en omvat dus

mede het gebruik van de gegevens voor het vervaardigen van een persoonsprofiel of de verstrekking aan derden voor dit doel. Het verzet kan dus worden aangetekend bij elke verantwoordelijke in de keten van verstrekkingen die voor het doel van direct marketing wordt gedaan. Elke verantwoordelijke in de keten die weet of redelijkerwijs kan weten dat de verstrekking van de gegevens het doel van direct marketing dient, dient het verzet te honoreren en daartoe eventueel maatregelen te treffen. Het is daarbij niet relevant of de gegevens al dan niet afkomstig zijn uit open bronnen. De plicht het verzet te honoreren beperkt zich aldus niet tot de laatste in de keten die uiteindelijk de betrokkene de boodschap voor commerciële of charitatieve doeleinden toezendt.

De ratio is dat de burger de gelegenheid heeft te voorkomen dat hem ongevraagd informatie wordt aangeboden op basis van een profiel van zijn persoon. Sommige mensen ervaren dit als een inbreuk op hun persoonlijke levenssfeer en de onderhavige bepaling strekt ertoe dergelijke gevoelens in rechte te honoreren. De burger is daardoor in de gelegenheid te bepalen welke in het bijzonder op hem gerichte boodschappen hem bereiken. De bepaling is als het ware een instrument voor de betrokkene tot de inrichting van zijn bewustzijnshuishouding. Degenen die gebruik maken van direct-marketingtechnieken moeten de consument in kennis stellen van de mogelijkheden om bezwaar te maken. Dit kan door publikaties in daarvoor passende media, bijvoorbeeld door middel van advertenties in de krant of door een mededeling op het reclamemateriaal dat wordt toegezonden. Daarbij behoort ook een advertentie door een branche-organisatie waarin de individuele verantwoordelijke in een lijst worden opgesomd, tot de mogelijkheden. In het artikel is aansluiting gezocht bij de tekst van artikel 3.12, eerste lid, Awb. Na ten hoogste een jaar moet de publikatie worden herhaald. Daarbij is invulling gegeven aan het voorschrift van de richtlijn dat de nodige maatregelen moeten worden genomen om te waarborgen dat de betrokkenen kennis hebben van de mogelijkheden van verzet.
Van de beide opties die de richtlijn biedt, is uit een oogpunt van beperking van de kosten voor het bedrijfsleven gekozen voor de oplossing waarbij het initiatief voor het verzet wordt overgelaten aan de betrokkene. Een groot aantal bedrijven dat het instrument van direct marketing gebruikt, zijn aangesloten bij de Nederlandse Associatie voor direct marketing, distance selling en sales promotion (DMSA). Zij hebben een gemeenschappelijk adres waar gratis de uitoefening van het recht van verzet kan worden kenbaar gemaakt. Het adres is: DMSA, Antwoordnummer 666, 1000 TL Amsterdam.
Daarmee is afstand genomen van de oorspronkelijke gedachte dat bij de eerste verstrekking van persoonsgegevens aan een derde voor direct marketing, de betrokkene individueel vooraf moet worden genformeerd. Deze gedachte kwam voort uit het oogpunt van consumentenbescherming en biedt de betrokkene de gelegenheid om tegen dit gebruik van de hen betreffende gegevens verzet aan te tekenen. Het onderzoek dat in opdracht van de Europese Commissie in Nederland is verricht naar de financiële gevolgen van de richtlijn maakte duidelijk dat vooral de banken een grote kostenpost op dit punt vreesden. Mede naar aanleiding van deze constatering is in het wetsvoorstel deze bepaling niet opgenomen en is er gekozen voor de optie dat de betrokkene initiatief tot verzet moet nemen. Het onderzoeksteam spreekt in zijn studie de verwachting uit dat met deze optie de kosten verwaarloosbaar zijn[1]. De gekozen optie maakt het in beginsel mogelijk persoonsgegevens voor doeleinden van direct marketing te verstrekken aan derden zonder vooraf de betrokkenen daarvan in kennis te stellen. Dit laat onverlet dat deze derden zelf ingevolge artikel 34 in beginsel gehouden zijn de betrokkenen te informeren over tenminste hun eigen identiteit en hun doeleinden van de gegevensverwerking.

[1] Zie samenvatting blz.17, punt 6.

Het bovenstaande betekent een verruiming van de mogelijkheden ten opzichte van het Besluit genormeerde vrijstelling. Dit besluit stelt een aantal standaardregistraties vrij van aanmelding, mits zij aan bepaalde voorwaarden voldoen. Indien al de mogelijkheid wordt geopend voor gebruik voor direct marketing dan dient de verantwoordelijke telkens voorafgaand aan het gebruik de betrokkenen daarover te informeren en gedurende een redelijke termijn de gelegenheid te geven daartegen bezwaar te maken. De verruiming van het regime bestaat eruit dat kan worden volstaan met een periodieke bekendmaking in daarvoor aanmerking komende media dat er de mogelijkheid bestaat bezwaar te maken tegen het gebruik van persoonsgegevens voor direct marketing. Ook de absolute verboden van het Besluit genormeerde vrijstelling vervallen, bij voorbeeld voor personeelsen salarisadministraties. De richtlijn laat niet toe in de vrijstellingen hieraan beperkingen te stellen. Dit past in het algemene beeld van een accentverlegging van een meer bevoogdende bescherming door middel van regelgeving naar een regime waarin meer aan de betrokkenen wordt overgelaten met de instrumenten die de wet hem biedt, desgewenst zelf vorm te geven aan de wijze waarop zijn persoonsgegevens door anderen worden gebruikt. De Registratiekamer heeft hierbij een complementaire functie.
Een andere EG-regeling, waarover een gemeenschappelijk standpunt is bereikt, beschermt consumenten bij overeenkomsten die op afstand worden gesloten. De regeling schrijft voor dat wanneer (potentiële) klanten worden benaderd via fax of via een geautomatiseerd telefonisch oproepsysteem, niet kan worden volstaan met een systeem van geen bezwaar, doch uitdrukkelijk de voorafgaande toestemming van de betrokkene is vereist. Voor andere communicatiemiddelen die een individuele communicatie mogelijk maken geldt een systeem van geen bezwaar (het z.g. opt-out).
Tot slot wijzen wij op artikel 100 van de Wet gemeentelijke basisadministratie persoonsgegevens. Hierin is bepaald dat bij gemeentelijke verordening gegevens uit de bevolkingsboekhouding kunnen worden verstrekt, onder meer voor direct marketing. In dat geval dienen gemeenten gevolg te geven aan een verzoek om de gegevens te blokkeren zolang de betrokkene het niet heeft ingetrokken[1]. De Wet gemeentelijke basisadministratie is aldus in overeenstemming met de richtlijn. Tevens vormt dit artikel de wettelijke basis die wordt aanbevolen in artikel 7 van de Aanbeveling nr R (91) 10 van het Comité van Ministers van de Raad van Europa inzake de verstrekking aan derden uit openbare registers.

Artikel 42

eerste lid

Deze bepaling vormt de implementatie van artikel 15 van de richtlijn over geautomatiseerde individuele besluiten. Zij vindt haar oorsprong in artikel 2 van de Franse wet van 6 januari 1978 waarin besluitvorming wordt verboden ten aanzien van enige natuurlijke persoon op grond van een profielschets of een persoonlijkheidsschets die langs geautomatiseerd weg tot stand is gebracht. De achterliggende gedachte is dat beslissingen op grond van bepaalde gegevens over iemand, diens persoonlijke levenssfeer minder aantast dan wanneer door de veelheid van informatie van hem een min of meer uniek beeld ontstaat. Het moet dan gaan om een zodanige hoeveelheid van gegevens dat sprake is van een beeld van een bepaald aspect van zijn persoonlijkheid. De precieze betekenis van deze bepaling zal in de jurisprudentie nadere inhoud moeten krijgen.
Het is daartoe niet vereist dat dit beeld inzicht geeft in de totale persoonlijkheid. Voldoende is dat het beeld bepaalde aspecten tot uitdrukking brengt. De richtlijn noemt als voorbeelden van dergelijke aspecten de

[1] artikel 102, eerste lid.

beroepsprestatie, kredietwaardigheid, betrouwbaarheid of gedrag. Daarbij wordt een kwalificatie over een persoon gegeven op grond van een interpretatie van uiteenlopende gegevens. De menselijke waardigheid vereist dat dergelijke beslissingen over iemand ook door een andere persoon, en niet slechts door een geautomatiseerd systeem, worden genomen. Het profiel mag geen grond zijn voor besluitvorming over die persoon zonder daadwerkelijke menselijke tussenkomst. Dit laat onverlet dat het geautomatiseerd systeem wel als hulpmiddel kan worden aangewend.

tweede en derde lid

Het tweede lid, onder a, in verband met het derde lid, heeft betrekking op overeenkomsten. De bepaling opent de mogelijkheid dat een computer aldus is geprogrammeerd dat iemand bij voorbeeld op basis van een veelheid van gegevens geen tegoeden meer uit een geldautomaat kan opnemen, bij voorbeeld op grond van een zwarte lijst binnen de branche. Het gaat dan immers om de uitvoering van een rekening-courantovereenkomst. Wel schrijft zij voor dat een bank zich niet achter dit programma kan verschuilen, doch passende maatregelen dient te nemen ter bescherming van het gerechtvaardigd belang van de betrokkene. Een dergelijke maatregel kan, blijkens het derde lid, daarin bestaan dat iemand in de gelegenheid wordt gesteld zijn standpunt uiteen te zetten. Daarop dient inhoudelijk te worden ingegaan. Dit gaat echter weer niet zover dat een bedrijf, wanneer het desondanks zou persisteren in de afwijzing, gehouden zou zijn dit schriftelijk te motiveren. Voldoende is een gesprek waarin inhoudelijk op de argumentatie van de betrokkene wordt ingegaan. De bepaling laat overigens toe dat ook alternatieve passende maatregelen worden genomen. Het gaat er daarbij om steeds dat om dat wanneer sprake is van profielschetsen, de computer niet de mens vervangt.
Blijkens onderdeel b van het tweede lid, geldt ook buiten de situatie van een overeenkomst, dus ook in de publieke sfeer, dat geen beslissingen op grond van een profielschets worden genomen. De Awb, in het bijzonder de artikelen 4:7 e.v., geeft waarborgen die kunnen voorkomen dat beslissingen uitsluitend op grond van een beeld van de persoonlijkheid dat langs geautomatiseerd weg is vervaardigd, worden genomen. Deze bepalingen kunnen worden geacht de maatregelen te bevatten als bedoeld in onderdeel b.

vierde lid

Het vierde lid vormt een uitwerking van artikel 12, eerste lid, derde gedachtenstreepje, van de richtlijn. Voor een nadere toelichting wordt verwezen naar de toelichting op artikel 35, derde lid.

HOOFDSTUK 7 UITZONDERINGEN EN BEPERKINGEN

Artikel 43

Het recht op bescherming van de persoonsgegevens kan niet in absolute zin worden geformuleerd. De samenleving kan niet functioneren wanneer niet onder bepaalde omstandigheden op de vastgestelde beginselen een uitzondering kan worden gemaakt.
De mogelijkheid een uitzondering te maken geldt inzake:
– het beginsel van het verenigbaar gebruik, te weten de verenigbaarheid met het oorspronkelijk doel waarvoor de gegevens zijn vergaard (artikel 9),
– de algemene informatieplicht jegens een ieder, ongeacht zijn belang, over verwerkingen van persoonsgegevens (artikel 30, derde lid),

– de informatieplicht tegenover de betrokkene in geval van verwerking van hem betreffende gegevens (de artikelen 33 en 34) en
– de uitoefening van het recht op kennisneming (artikel 35) aan welke bepaling de uitoefening van het recht op verbetering is verbonden.

De gronden om een uitzondering te maken zijn in de bepaling zelf opgenomen. De toepasselijkheid van deze gronden is onderworpen aan het «noodzakelijkheids»-criterium. Onder punt 4.2 van het algemeen deel van deze toelichting zijn wij daarop reeds ingegaan. Een strikte uitleg van dit begrip is aangewezen daar de gronden zelf slechts in algemene zin kunnen worden geformuleerd. Het betreft de veiligheid van de staat, de criminaliteitsbestrijding, de overheidsfinanciën en economische belangen van de overheid, de toezichthoudende taak van de overheid en als sluitstuk in algemene zin de bescherming van de betrokkene of van de rechten en vrijheden van anderen.
De bepaling gaat terug op artikel 9, tweede lid, van het Verdrag inzake gegevensbescherming en artikel 13, eerste lid, van de richtlijn.
Het artikel sluit aan bij de artikelen 11, tweede lid, en 30 van de WPR. Wat betreft de afwijking van het verenigbaar gebruik op grond van een dringende en gewichtige reden als bedoeld in artikel 11, tweede lid, van de WPR is deze bepaling vorm gegeven overeenkomstig de richtlijn zonder daarmee een inhoudelijke wijziging te beogen. Artikel 11, tweede lid, van de WPR en de desbetreffende bepaling in de richtlijn steunen ook beide op hetzelfde artikel 9, tweede lid, onder a, van het Verdrag inzake gegevensbescherming.
De verschillende gronden spreken overigens voor zich. Wij gaan slechts nader in op een aspect van de laatste uitzondering: de bescherming van de betrokkene of van de rechten en vrijheden van anderen. Naar aanleiding van het advies van de Registratiekamer komt de formulering thans overeen met die van artikel 13, eerste lid, onderdeel g, van de richtlijn en artikel 9, tweede lid, onderdeel b, van het Verdrag inzake gegevensbescherming. Daarbij is wat betreft het recht op kennisneming in zekere zin een aanscherping beoogt van het huidige artikel 30, onder e, van de WPR, waar wordt gesproken van «gewichtige belangen van anderen dan de verzoeker, de houder daaronder begrepen». De voorgestelde formulering sluit beter aan bij artikel 8, tweede lid, van het EVRM en de daarop gebaseerde jurisprudentie. Niet ieder gewichtig belang van een ander dan de verzoeker zal kunnen worden aangemerkt als een recht of vrijheid in de zin van dit verdrag.
Een ander verschil tussen artikel 43, onder e, en artikel 30, onder e, WPR is dat in laatstgenoemde bepaling de verantwoordelijke (onder de WPR: de houder) nog uitdrukkelijk wordt genoemd. Hiermee wordt evenwel geen inhoudelijke wijziging beoogd. Buiten twijfel staat dat in onderdeel e onder «anderen» ook de verantwoordelijke moet worden begrepen. Wel geldt de in de vorige alinea bedoelde aanscherping ook voor de verantwoordelijke. Dit betekent bijvoorbeeld dat de verantwoordelijke niet uitsluitend op grond van zijn belang om administratieve lasten te beperken, een verzoek om informatie als bedoeld in artikel 35, eerste lid, zal mogen afwijzen. De verantwoordelijke zal conform artikel 43, onder e, aannemelijk moeten maken dat door inwilliging van een dergelijk verzoek de administratieve lasten zodanig disproportioneel zijn dat hij in een van zijn rechten en vrijheden wordt aangetast of dreigt te worden aangetast. Aldus impliceert artikel 43, onder e, ten opzichte van de huidige WPR een verzwaring van de bewijslast voor de verantwoordelijke. Voor zover het het inzagerecht betreft, valt overigens te wijzen op de inherente beperking die reeds ingevolge artikel 35, eerste lid, uit de formulering van het recht zélf voortvloeit. In laatstgenoemd artikel wordt immers bepaald dat betrokkene zijn verzoek om informatie slechts mag doen «met redelijke tussenpozen». Voor zover de administratieve lasten voor de verantwoordelijke voortvloeien uit de hoge frequentie waarmee een specifieke

betrokkene verzoeken tot een bepaalde verantwoordelijke richt, kunnen deze reeds op grond van artikel 35, eerste lid, worden beperkt.
Het artikel verschaft ook de mogelijkheid af te wijken van het beginsel van het verenigbaar gebruik (artikel 9). Artikel 9 bepaalt dat persoonsgegevens enkel mogen worden verwerkt voor een doel dat verenigbaar is met het doel waarvoor ze zijn verzameld. Onder omstandigheden is het mogelijk ook af te wijken van een dergelijk verenigbaar doel en dus gegevens te verwerken voor een doel dat niet alleen afwijkt van het doel waarvoor ze verzameld zijn, maar daarmee ook onverenigbaar is. Artikel 43 geeft daarvoor de nadere voorwaarden: de verwerking dient noodzakelijk te zijn voor één van de gronden die in dat artikel zijn opgesomd.

Artikel 44

Eerste lid

Dit voorschrift geeft uitvoering aan artikel 11, tweede lid, resp. artikel 13, tweede lid, van de richtlijn. In artikel 11, tweede lid, wordt voorzien in een uitzondering op de informatieverplichting voor zover de verstrekking van informatie aan de betrokkene onmogelijk blijkt of onevenredig veel moeite kost, dan wel de registratie of verstrekking bij wet is voorgeschreven. Verwerkingen voor statistische, historische of wetenschappelijke doeleinden worden in deze bepaling met name genoemd. In artikel 44, eerste lid, wordt ter concretisering van artikel 11, tweede lid, van de richtlijn vastgelegd dat bij verwerkingen voor statistische of wetenschappelijke doeleinden niet behoeft te worden geïnformeerd, omdat sprake is van een onevenredige inspanning als bedoeld in artikel 11, tweede lid, van de richtlijn. Aldus vormt artikel 44, eerste lid, een precisering als bedoeld in artikel 5 van de richtlijn.
Daarnaast vormt artikel 44, eerste lid, de implementatie van artikel 13, tweede lid, van de richtlijn. Laatstgenoemde bepaling voorziet voor dezelfde doeleinden in de mogelijkheid tot beperkingen van de in artikel 12 van de richtlijn bedoelde rechten. Artikel 44, eerste lid, concretiseert deze beperking door voor instellingen of diensten voor wetenschappelijk onderzoek of statistiek de mogelijkheid te creëren tot weigering om aan een verzoek als bedoeld in artikel 35 te voldoen. Naar ons oordeel is er conform de in artikel 13, tweede lid, gestelde eis geen sprake van gevaar voor inbreuken op de persoonlijke levenssfeer nu in artikel 44, eerste lid, is bepaald dat de nodige voorzieningen moeten worden getroffen om te verzekeren dat de betreffende persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden kunnen worden gebruikt en voorts de uitzondering beperkt blijft tot instellingen voor diensten voor wetenschappelijk onderzoek of statistiek.
Voor de in artikel 44, eerste lid, opgenomen uitzonderingen stelt de richtlijn als algemene voorwaarde dat passende waarborgen moeten worden getroffen. De vereiste waarborgen zijn deels ontleend aan het bestaande artikel 18 van het Besluit genormeerde vrijstelling. Deze hebben betrekking op de categorieën van verantwoordelijken (alleen onderzoeksinstellingen of instellingen voor statistiek) en de exclusiviteit in het gebruik van de gegevens (de gegevens mogen niet voor andere doeleinden worden gebruikt).
Deze beperkingen leiden ertoe dat wanneer zij worden overgeschreden, de toepasselijkheid van de uitzonderingsgrond komt te ontvallen en de mededelingsplicht, het recht op kennisneming en verbetering herleven. Naar aanleiding van het advies van de Registratiekamer is de oorspronkelijk opgenomen eis dat de gegevens niet langer dan een termijn van zes maanden worden bewaard, vervallen. In plaats daarvan is de eis opgenomen dat de «nodige» voorzieningen zijn opgenomen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden kunnen worden gebruikt. Het begrip

«nodige» duidt op een proportionaliteit tussen enerzijds het belang van de bescherming van persoonsgegevens en anderzijds de kosten en inspanningen die zijn verbonden aan de bedoelde voorzieningen. De aard van de vereiste voorzieningen zal wijzigen met de ontwikkeling van de stand van de techniek. Wat op het ene moment nog als proportionele maatregel kan worden gezien, is dat op een volgend moment niet meer. In die zin is deze norm technologie-onafhankelijk.
De Registratiekamer wijst op het belang de gegevens omtrent de identiteit van de betrokkenen af te schermen van de overige gegevens. Dit is een voor de hand liggende modaliteit van bescherming. De mogelijkheid de relatie tussen beide te herstellen wanneer dat voor statistische en wetenschappelijke doeleinden nodig is, zou dan in overeenstemming met regels van zelfregulering aan bijzondere, controleerbare procedures moeten worden onderworpen.

Doorslaggevend is dat geen gebruik wordt gemaakt en, gegeven de getroffen beschermingsmaatregelen, redelijkerwijs ook niet kan worden gemaakt, met het oog op enig onderzoek of maatregel van de gegevens in relatie tot de individuele betrokkene. Onder maatregel wordt mede begrepen de beslissing om de betrokkene te benaderen, hetzij om hem bepaalde voor hem mogelijk van belang zijnde informatie onder de aandacht te brengen, hetzij voor het stellen van nadere vragen bij voorbeeld voor aanvullend wetenschappelijk onderzoek of statistiek.

Tweede lid

Zoals in het algemene deel van de toelichting onder paragraaf 15.2 reeds is uiteen gezet, zijn de archiefbescheiden die naar een archiefbewaarplaats zijn overgebracht in beginsel ouder dan twintig jaar. Het zijn die archiefbescheiden die na selectie behoudenswaardig worden geacht met name om redenen van rechtsvinding, wetenschap en cultuurhistorie. Selectie van archiefbescheiden en overbrenging van de geselecteerde archiefbescheiden naar een archiefbewaarplaats zijn wettelijk voorgeschreven.
Gelet op de grote hoeveelheden archiefbescheiden die worden overgebracht naar de archiefbewaarplaatsen, zou het informeren van de betrokkene als bedoeld in artikel 34, de verantwoordelijke in het kader van de uitvoering van de Archiefwet voor onoverkomelijke problemen stellen. Om die reden is in artikel 44, tweede lid, een uitzondering opgenomen. Een dergelijke uitzondering omdat mag worden aangenomen dat de burger ermee bekend is dat overheidsorganen de onder hen berustende archiefbescheiden na verloop van tijd overbrengen naar archiefbewaarplaatsen. Voorts is van belang dat de Archiefwet 1995 zélf reeds een procedure bevat die erop is gericht belanghebbenden te informeren omtrent de wijze waarop de overheid voornemens is om te gaan met haar archiefbescheiden. Ten behoeve van de overbrenging dient de zorgdrager – bijvoorbeeld een minister – een selectielijst te maken die aan een aantal wettelijke eisen dient te voldoen. Een van die eisen betreft een systematische opsomming van de categoriëen van archiefbescheiden in het kader waarvan bij elke categorie is aangegevn of de bescheiden bewaard worden – en dus naar een archiefbewaarplaats worden overgebracht – dan wel na welke termijn zij voor vernietiging in aanmerking komen. Een dergelijke ontwerp-selectielijst wordt ter inzage gelegd en een ieder is in de gelegenheid daaromtrent zijn zienswijze kenbaar te maken. De openbare voorbereidingsprocedure van de Awb is daarbij van toepassing. Op grond van het voorgaande kan worden gesteld dat een burger – ook indien geen toepassing wordt gegeven aan artikel 34 – toch op hoofdlijnen geacht kan worden te zijn geïnformeerd omtrent de aanwezigheid van hem of haar betreffende persoonsgegevens in archiefbewaarplaatsen. Onder deze omstandigheden dient het daarnaast afzonderlijk informeren

van de betrokkene als een onevenredige inspanning worden beschouwd. Wellicht ten overvloede zij erop gewezen dat de informatieplicht van artikel 34 wel geldt zolang de archiefbescheiden nog niet zijn overgebracht, maar berusten bij de zorgdrager die ze heeft opgemaakt of ontvangen.

HOOFDSTUK 8 RECHTSBESCHERMING

Artikel 45

In het algemeen deel van deze toelichting is reeds uiteengezet dat voor zover het gaat om de rechtsbescherming in de publieke sector aansluiting wordt gezocht bij het systeem van de Awb. In verband hiermee wordt in artikel 45 bepaald dat een beslissing van een bestuursorgaan op een verzoek als bedoeld in artikel 30, derde lid, 35, 36 of 38, tweede lid, alsmede een beslissing naar aanleiding de aantekening van verzet als bedoeld in de artikelen 40 of 41 gelden als een besluit in de zin van de Awb. Strikt genomen kan een dergelijke bepaling in veel gevallen als overbodig worden beschouwd. Aangenomen moet worden dat een zodanige beslissing – in het verlengde van de WOB-jurisprudentie – door de bestuursrechter vaak als een besluit zal worden aangemerkt. Het betreft een weigering of toewijzing door een bestuursorgaan van een recht dat aan de betrokkene krachtens het wetsvoorstel is toegekend, hetgeen als een rechtshandeling in de zin van artikel 1:3 Awb kan worden beschouwd.
Niettemin achten wij een uitdrukkelijke wetsbepaling noodzakelijk. Evenals de WPR is de WBP een regeling die zich zowel tot de private als de publieke sector uitstrekt. Introductie van de Awb-rechtsgang brengt een wijziging teweeg ten opzichte van de WPR die alleen de civiele verzoekschriftenprocedure kent. Tegen deze achtergrond achten wij een uitdrukkelijke bepaling uit een oogpunt van rechtszekerheid noodzakelijk. Met artikel 45 wordt buiten twijfel gesteld dat de Awb van toepassing is en op dit punt derhalve een verandering is beoogd. Daar waar bijzondere regelgeving de toepasselijkheid vna de Awb uitsluit, gaat deze uiteraard als lex specialis vor de onderhavige bepaling. Een voorbeeld zijn artikelen 56a e.v. en 112 e.v. van de Kadasterwet.
De door de wet aan de betrokkene toegekende rechten betreft in beginsel alleen gegevens die op de betrokkene zélf betrekking hebben. Aannemelijk is echter dat het niet altijd te vermijden zal zijn dat honorering van bijvoorbeeld een inzageverzoek van betrokkene tevens enig inzicht zal geven in gegevens die op anderen betrekking hebben. De betrokkene kan daar ook belang bij hebben. Dit kan bijvoorbeeld het geval zijn indien bij de registratie van gegevens over de betrokkene tevens wordt aangegeven van wie die gegevens afkomstig zijn. Verstrekking van dergelijke informatie aan de betrokkene op grond van artikel 35 kan niet worden uitgesloten. In verband met de hieruit voortvloeiende behoefte aan rechtsbescherming voor derden-belanghebbenden is krachtens artikel 45 niet alleen de afwijzing, maar ook de toewijzing van een verzoek vatbaar voor bezwaar en beroep op de bestuursrechter. Voorts zij in dit verband verwezen naar het nieuwe artikel 35, derde lid.
Wellicht ten overvloede zij er op gewezen dat ook bezwaar en beroep openstaat tegen de weigering om een besluit als bovenbedoeld te nemen, alsmede het niet tijdig nemen van een besluit. Dit volgt uit artikel 6:2 Awb. Voorts staat overeenkomstig het huidige artikel 34 WPR beroep open indien niet volledig aan een verzoek wordt voldaan. Een dergelijke beslissing is te beschouwen als een (gedeeltelijke) afwijzing als bedoeld in dit artikel.

Artikel 46

Indien de Awb niet van toepassing is, kan de verzoekschriftprocedure volgens het Wetboek van Burgerlijke Rechtsvordering worden gevolgd. Deze procedure staat thans op grond van de WPR ook reeds open. Deze procedure kan ook worden gevolgd indien een gegevensverwerking plaatsvindt overeenkomstig het recht van een van de andere landen van de Europese Unie. De Registratiekamer vraagt zich in haar advies af of op dit punt een bijzondere wettelijke voorziening zou moeten worden getroffen. Zij wijst erop dat artikel 22 van de richtlijn duidelijk verwijst naar de mogelijke toepassing van buitenlands recht door de Nederlandse rechter, zoals ook in het internationaal privaatrecht het geval is. De bepaling heeft echter een algemene strekking zonder te verwijzen naar het toepasselijke recht. Een bijzondere wettelijk voorziening lijkt daarom niet nodig.
In afwijking van het huidige artikel 34 WPR staat de verzoekschriften-procedure niet alleen open voor de betrokkene, maar voor alle belanghebbenden die via de rechtbank op willen komen tegen een beslissing van de verantwoordelijke op grond van de artikelen 30, derde lid, 35, 36, 38, tweede lid, 40 of 41. Deze verruiming ligt in het verlengde van de reikwijdte van de Awb-rechtsgang, zoals deze voortvloeit uit artikel 45. Voor zover het gaat om de rechtsbescherming van derden-belanghebbenden zal de verzoekschriftenprocedure niet altijd soelaas bieden. Dit is bijvoorbeeld het geval indien het gaat om een toewijzing van het verzoek om inzage door de betrokkene waardoor een derde in zijn belangen is geschaad. Aangezien in een dergelijk geval reeds feitelijk inzage zal zijn verleend, zal het doorgaans alleen nog gaan om de vraag of de inzage rechtmatig was en zo niet, in hoeverre een schadevergoeding behoort te worden toegekend. De verzoekschriftenprocedure is daarvoor niet het geëigende kader. Wel kan de derde-belanghebbende via de verzoekschriftenprocedure de rechtbank verzoeken om de beslissing van de verantwoordelijke tot toewijzing van een correctieverzoek of tot honorering van het verzet, ongedaan te maken. Met het oog op de rechtsbescherming van derden-belanghebbenden bij verzoeken om kennisneming zij overigens verwezen naar artikel 35, derde lid, op grond waarvan de verantwoordelijke in beginsel verplicht is derden-belanghebbenden te horen alvorens hij tot honorering van een verzoek om kennisneming overgaat. Juist in deze fase kan eventuele schade aan derden-belanghebbenden voorkomen kunnen worden omdat op dat moment de feitelijke inzage door de betrokkene nog niet is geëffectueerd.
In het tweede tot en met vijfde lid zijn enige bepalingen van de WPR overgenomen. Deze vormen een noodzakelijke aanvulling op het algemene recht op het bijzondere gebied van de gegevensverwerking. De evaluaties noch de richtlijn geven aanleiding tot een wijziging op dit punt. Een uitzondering wordt evenwel gevormd door de tweede volzin van het derde lid. Hierin is vastgelegd dat alvorens de rechtbank beslist, het zonodig belanghebbenden in de gelegenheid stelt hun zienswijze naar voren te brengen. Voor de betrokkene zelf spreekt dit min of meer vanzelf. De bepaling is dan ook in het bijzonder van belang in de specifieke situatie waarin de belangen van derden in het geding zijn. Zoals eerder in deze toelichting is aangegeven kan zich dit onder meer voordoen indien bij de registratie van gegevens over de betrokkene tevens is aangegeven van wie die gegevens afkomstig zijn. In dergelijke gevallen zal de rechtbank zo nodig derden-belanghebbenden in de gelegenheid moeten stellen hun opvatting in de procedure kenbaar te maken. De bepaling ligt in het verlengde van de – uitgebreidere – regeling die op dit punt in hoofdstuk 8 van de Awb is opgenomen.

Artikel 47

Ook in dit artikel is de regeling van de WPR overgenomen, met dien verstande dat overeenkomstig de artikelen 45 en 46 de mogelijkheid thans openstaat voor alle belanghebbenden. De procedure van bemiddeling van de Registratiekamer geldt voor zowel de publieke als de private sector. Het begrip «voorafgaand» impliceert dat de bemiddeling kan worden ingeroepen gedurende de periode dat de procedure kan worden ingesteld. Verwezen kan worden naar de termijnen in artikel 46, tweede lid en artikel 6:7 Awb. In het geval de bemiddeling van de Registratiekamer wordt ingeroepen wordt de termijn waarbinnen beroep kan worden ingesteld, dan wel de verzoekschriftenprocedure aanhangig kan worden gemaakt geschorst. Voor zover het gaat om de schorsing van de beroepstermijn als bedoeld in de Awb, betekent de schorsing een afwijking van artikel 6:7 Awb. Dit laatste is in het eerste lid expliciet tot uitdrukking gebracht.

Artikel 48

Het is wenselijk dat de Registratiekamer inzicht heeft in de jurisprudentie in den lande. Daartoe dient zij over de uitspraken die krachtens het onderhavige wetsvoorstel worden gedaan te beschikken. De regeling wijkt niet af van die van de WPR.

Artikel 49 en 50

In deze artikelen zijn grote delen van de artikelen 9 en 10 WPR overgenomen. Deze artikelen bevatten dwingend recht en afwijkende bepalingen in overeenkomsten zijn nietig. Op twee punten verschillen de bepalingen van de huidige WPR: de aanpassing van de risicoaansprakelijkheid en de schrapping van de bepaling inzake het collectief actierecht.
In de eerste plaats is de vergaande vorm van risico-aansprakelijkheid die besloten lag in artikel 9, eerste lid, WPR, in overeenstemming met de richtlijn afgezwakt. De bewijslast dat de schade niet aan de verantwoordelijke kan worden toegerekend rust evenwel op de schouders van de laatste. Op dit punt betekent de implementatie van de richtlijn theoretisch een verzwakking van de rechten van de burger. Uit de in het algemeen deel genoemde evaluaties blijkt echter dat de risico-aansprakelijkheid van artikel 9, eerste lid, WPR in de praktijk nauwelijks een rol gespeeld heeft. Krachtens de voorgestelde regeling kan in de eerste plaats de verantwoordelijke worden aangesproken. Vanzelfsprekend is alleen aansprakelijk de verantwoordelijke voor de verwerking met betrekking waartoe in strijd is gehandeld met de wettelijke voorschriften. De bepaling impliceert voorts dat ook indien er een bewerker is die gegevens verwerkt ten behoeve van een verantwoordelijke, ook steeds die verantwoordelijke daarvoor aansprakelijk is. De verwerking blijft immers altijd onder de verantwoordelijkheid van de verantwoordelijke plaatsvinden. Dit laat onverlet dat hij mogelijk een regresrecht heeft op de bewerker. Daarnaast is de bewerker ook zelfstandig aansprakelijk voor zijn aandeel in de schade.
Het is aannemelijk dat in geval van schade de jurisprudentie aansluiting zal zoeken bij artikel 6:75 BW dat bepaalt dat een tekortkoming de verantwoordelijke niet kan worden toegerekend indien zij niet te wijten is aan zijn schuld, noch krachtens de wet, rechtshandeling of in het verkeer geldende opvattingen voor zijn rekening komt. Het is evenwel mogelijk dat de jurisprudentie van het Europese Hof van Justitie dwingt tot een afwijkende interpretatie van deze bepaling. Gegeven deze laatste mogelijkheid is deze afzonderlijke regeling opgenomen ter implementatie van de richtlijn.
Het tweede punt waarop het wetsvoorstel verschilt van de WPR betreft het collectief actierecht. In artikel 10, tweede lid, WPR is hieromtrent een afzonderlijke bepaling opgenomen. Thans dient deze als overbodig te

worden beschouwd, omdat hiervoor recentelijk algemene wettelijke voorzieningen zijn getroffen. Voor het bestuursrecht betreft dit artikel 1:2, derde lid, Awb, voor het privaatrecht zij verwezen naar artikel 3:305a BW. Aan een afzonderlijke bepaling in de WBP bestaat derhalve geen behoefte meer.

HOOFDSTUK 9 TOEZICHT

PARAGRAAF 1 DE REGISTRATIEKAMER

Inleiding

De artikelen 51 tot en met 61 voorzien in een regeling voor de inrichting en de bevoegdheden van de Registratiekamer die ten dele afwijkt van de bestaande. Deze bepalingen geven uitvoering aan artikel 28 van de richtlijn. Het voorstel sluit aan bij de Aanwijzingen voor zelfstandige bestuursorganen.

Artikel 51

Eerste lid

Artikel 51, eerste lid, vormt de implementatie van artikel 28, eerste lid, van de richtlijn, waarin in zijn algemeenheid wordt gesproken van toezicht op de toepassing van de ter uitvoering van de richtlijn vastgestelde «bepalingen»(«wettelijke of bestuursrechtelijke bepalingen» ofwel «administrative measures or regulations»).
De toezichthoudende taak van de Registratiekamer, neergelegd in artikel 51, eerste lid, is niet beperkt tot het terrein van het onderhavige wetsvoorstel, maar strekt zich ook uit tot andere wetten, algemene maatregelen van bestuur en andere wettelijke regelingen op grond waarvan persoonsgegevens worden verwerkt. De omschrijving van het eerste lid beoogt daarmee enerzijds aan te sluiten bij de omschrijving van artikel 37, tweede lid, van de WPR en anderzijds, in verband met artikel 28, eerste lid, van de richtlijn, duidelijk te stellen dat de toezichthoudende taak van de kamer zich afspeelt binnen het wettelijk kader waaraan het verwerken van persoonsgegevens moet voldoen. Dit wettelijk kader biedt overigens voldoende ruimte. De in de WBP vervatte open normen stellen de Registratiekamer in staat erop toe te zien dat de verwerking van persoonsgegevens – mede in het licht van artikel 10 Grondwet en artikel 8 EVRM – op een rechtmatige wijze plaatsvindt. Materieel leidt dit niet tot een wijziging ten opzichte van de WPR.
In § 4 van het Algemeen deel van de toelichting «Algemene normen en sectorale invulling» noemden wij twee modellen van aanvullende wetten: het eerste waarbij uitputtend de gegevensbescherming in een wet is geregeld en het tweede waarbij in aanvulling op de Wet bescherming persoonsgegevens nadere regels zijn gesteld.
Wordt het eerste model gevolgd, dan wordt de toepasselijkheid van het onderhavige wetsvoorstel uitdrukkelijk uitgesloten. Dit is gebeurd in artikel 2, tweede lid. In de regel worden dan in de bijzondere wetten alsnog de bevoegdheden van de Registratiekamer opgesomd. Een voorbeeld is de Wet gemeentelijke basisadministratie. Een uitzondering is de Wet op de inlichtingen- en veiligheidsdiensten waarbij op dit moment uitsluitend de Nationale ombudsman een toezichthoudende functie heeft, zowel ten aanzien van het optreden van functionarissen van deze dienst als ten aanzien van de gegevensverwerking. Het ligt in de aard van het werk van deze diensten het getal der toezichthouders te beperken. De richtlijn heeft op dit terrein geen betrekking.
Wordt het tweede model gevolgd, dan is de Registratiekamer op grond van het wetsvoorstel bevoegd. Een voorbeeld is de Wet geneeskundige

behandelingsovereenkomst, thans neergelegd in afdeling 5 van titel 7 van boek 7 BW.
Voor de praktische uitvoering van het toezicht zij onder meer verwezen naar artikel 61.

Tweede lid

In het tweede lid is de adviserende taak van de Registratiekamer vastgelegd. De regering is verplicht om de Registratiekamer om advies te vragen over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. De adviesverplichting vloeit voort uit artikel 28, tweede lid, van de richtlijn. Dit betekent dat ook andere wetten en algemene maatregelen van bestuur die onderwerpen regelen die onder het communautair recht vallen, krachtens de richtlijn in ontwerp om advies aan de Registratiekamer dienen te worden voorgelegd. Dit vormt een noodgedwongen afwijking van het Nederlandse beleid dat gericht is op het tegengaan van adviesverplichtingen. Niettemin zal de adviesverplichting geen substantiële verandering betekenen ten opzichte van de bestaande praktijk. Op dit moment wordt in veel gevallen waarop de adviesverplichting betrekking heeft, reeds advies gevraagd. De afgelopen jaren is gebleken dat de Registratiekamer vanuit zijn bijzondere deskundigheid door middel van advisering een nuttige bijdrage kan leveren aan de kwaliteit van de regelgeving op het terrein van de privacybescherming. De gewijzigde formulering van de adviesverplichting in dit voorschrift ten opzichte van artikel 37, derde lid, van de WPR leidt niet tot een wijziging van de bestaande praktijk. Deze wijziging beoogt, in aansluiting op de toezichthoudende taak van de kamer in het eerste lid van artikel 51, duidelijk te stellen dat de adviserende taak van de kamer zich afspeelt binnen het wettelijk kader waaraan het verwerken van persoonsgegevens moet voldoen.
De adviesverplichting heeft betrekking op wetgeving die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. De reikwijdte van de verplichting blijft derhalve niet beperkt tot de onderhavige wetsvoorstel en de algemene maatregelen van bestuur die hierop worden gebaseerd. Van belang is dat de richtlijn niet uitsluitend wordt geïmplementeerd in de WBP, maar ook in de bijzondere wetgeving die ten opzichte van de WBP een aanvullende werking hebben. Om die reden is tot uitdrukking gebracht dat de adviesverplichting in algemene zin betrekking heeft op alle formele wetgeving en algemene maatregelen van bestuur die geheel of voor een belangrijk deel de verwerking van persoonsgegevens betreffen. Uiteraard geldt de adviestaak niet voor de wetgeving die in artikel 2 van de werkingssfeer van de WBP is uitgezonderd, tenzij in de betreffende bijzondere wet anders wordt aangegeven.
De adviesverplichting blijft beperkt tot wetsvoorstellen en ontwerpen van algemene maatregelen van bestuur. Dit laat vanzelfsprekend onverlet dat verantwoordelijken in zowel de publieke als de private sector de Registratiekamer desgewenst kunnen raadplegen over de wijze waarop de wettelijke normen hun nadere invulling moeten krijgen of in concrete gevallen moeten worden toegepast. Het beantwoorden van allerhande vragen over de toepassing van de wet blijft een essentiële activiteit in het kader van de toezichthoudende en uitvoerende taken van de Registratiekamer.
De Registratiekamer kan de Minister ook uit eigen beweging advies uitbrengen. Dit vloeit voort uit de Kaderwet adviescolleges (Stb. 1996, 378). Blijkens artikel 1, onder a, is de Registratiekamer een adviescollege in de zin van die wet. Dit leidt ertoe dat ingevolge artikel 18 spontane advisering mogelijk is. Van een voornemen daartoe dient de Minister van

Justitie en de beide kamers der Staten-Generaal onverwijld in kennis te worden gesteld.

Artikel 52

Eerste lid

Naast de toezichthoudende en adviserende taken, bedoeld in artikel 51, vervult de Kamer andere taken, haar bij wet en verdrag opgedragen.
Zo kan de Kamer adviseren over gegevensverwerkingen met een bijzonder risico. Ook is zij overeenkomstig artikel 65 bevoegd in te grijpen in een proces van gegevensverwerking en maatregelen te treffen. Voorts kan de betrokkene voorafgaand aan een bezwaarschriftenprocedure bij een bestuursorgaan of de gerechtelijke procedure bij de arrondissementsrechtbank zich op grond van artikel 47 wenden tot de Registratiekamer met het verzoek te bemiddelen of te adviseren in zijn geschil met de verantwoordelijke.
De uitvoerende taken van de Kamer bestaan uit de bevoegdheid om in aanvulling op de wettelijke bepalingen die de verwerking van gevoelige gegevens toestaan, goed te keuren dat deze gegevens worden verwerkt (artikel 23, eerste lid, onder e). De Kamer kan een vergunning afgeven voor de doorgifte van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt (artikel 77, tweede lid). Het gaat hier om besluiten in de zin van artikel 1.3 Awb waartegen bezwaar en beroep openstaat. Daarnaast houdt de Kamer een register bij van de aangemelde gegevensverwerkingen en een lijst van de ingevolge artikel 63, tweede lid, aangemelde functionarissen voor de gegevensbescherming.
Aan de Registratiekamer zijn ook diverse internationale taken opgedragen. Zij is aangewezen als bevoegde autoriteit in de zin van het Verdrag van Straatsburg. Voorts is zij vertegenwoordigd in de Gemeenschappelijke Controle Autoriteit op grond van de Uitvoeringsovereenkomst van het Akkoord van Schengen. Op grond van het Europolverdrag zal dit ook gaan gelden voor het daarin voorziene gemeenschappelijke controle-orgaan. Inmiddels is de Registratiekamer ook vertegenwoordigd in de Groep bedoeld in artikel 29 van de richtlijn.

Tweede lid

De noodzaak van een onafhankelijke positie van de Registratiekamer is reeds in het algemeen deel van deze memorie toegelicht. De bevoegdheden die de Minister van Justitie tegenover de Kamer heeft als zelfstandig bestuurorgaan, doen geen afbreuk aan deze onafhankelijkheid.

Artikelen 53 en 54

Onder de WPR heeft zich een werkwijze ontwikkeld waarbij de meeste werkzaamheden door de leden van de Registratiekamer met ondersteuning van het secretariaat worden uitgevoerd. Van de inzet van plaatsvervangende en buitengewone leden is slechts spaarzaam gebruik gemaakt. De aanvankelijke gedachte dat de Registratiekamer veel zittingen van meervoudige kamers zou houden die telkens die inzet van andere leden zou vergen, is in de praktijk niet gerealiseerd. Per jaar vinden slechts enkele hoorzittingen plaats, die dan door het lid dat verantwoordelijk is voor de desbetreffende zaak in enkelvoudige samenstelling worden gehouden. Wel hebben buitengewone leden een belangrijke bijdrage verleend aan het verrichten van EDP-audits door de Registratiekamer. Nu aan de inschakeling van plaatsvervangende of buitengewone leden voor de normale taakvervulling weinig behoefte blijkt te bestaan, verdient hun positie heroverweging.

Aan deskundige ondersteuning zal de Registratiekamer ook in toekomst behoefte hebben. Met name gelet op de uiteenlopende werkterreinen van de Kamer zal behoefte bestaan aan bijstand van een brede kring van deskundigen uit diverse maatschappelijke sectoren, bijvoorbeeld in de vorm van een raad van advies. Het eerste lid van artikel 53 beoogt beter het onderscheid tussen de leden die met de dagelijkse gang van zaken zijn belast en de buitengewone leden naar voren te brengen. Eveneens is om die reden artikel 38, derde lid, van de WPR niet meer overgenomen. De spreiding van de onderscheidene maatschappelijke sectoren onder de buitengewone leden is noodzakelijk indien deze leden deel uitmaken van het dagelijkse bestuur van de Registratiekamer (vergl. Aanwijzing 124r inzake zelfstandigige bestuursorganen). De aard van de bestuurstaak moet daartoe noodzaken. Daarvan is in de nieuwe constellatie niet meer sprake. Aan het instituut van plaatsvervangende leden bestaat, gelet op het feit dat het college uit drie leden bestaat, in de praktijk geen behoefte. Voor korte periodes kan met minder leden worden volstaan. Ingeval van vacatures kan naar verwachting tijdig in aanvulling worden voorzien.
De onafhankelijkheid van de Registratiekamer komt tot uitdrukking in de regeling van benoeming en ontslag. De rechtspositie van de voorzitter is ingevolge het tweede lid vergelijkbaar met die van leden van de rechterlijke macht. In tegenstelling tot de WPR is een expliciete regeling hiervan opgenomen ten einde de onafhankelijke positie te benadrukken. Voor de regeling van het ontslag en het toezicht op het gedrag van de leden van de Kamer is aangesloten bij de regeling ter zake voor de rechterlijke macht. De voorzitter en de andere leden – inclusief de buitengewone leden – worden bij koninklijk besluit, op voordracht van de Minister van Justitie, benoemd. De benoemingstermijn van zes jaren respectievelijk vier jaren als geregeld in artikel 38 WPR is gehandhaafd. In de bij algemene maatregel van bestuur krachtens artikel 55 te stellen regels inzake de rechtspositie van de leden van de Kamer zal nader inhoud worden gegeven aan de onafhankelijkheid van de Kamer.
De waarborg van de onafhankelijkheid en deskundigheid van de Registratiekamer is voorts gelegen in de persoon van de leden. Deskundigheid ziet in dit verband naast juridische deskundigheid op specifieke deskundigheid met betrekking tot bij voorbeeld de gegevensverwerking in een of meer door het wetsvoorstel bestreken sectoren. De maatschappelijke vertegenwoordiging kan daarnaast geschieden middels de benoeming van buitengewone leden. Daarbij wordt een maatschappelijk evenwichtige spreiding beoogd. Er is behoefte aan de mogelijkheid een lid meer dan eens te herbenoemen (artikel 53, derde lid).
Artikel 54 komt overeen met artikel 39 WPR.

Artikel 55

In het eerste lid van deze bepaling is de inhoud van artikel 40 van de Wet persoonregistraties, voor zover het nodig bleek deze in dit wetsvoorstel over te nemen, neergelegd. Voor zover het niet is overgenomen is het de bedoeling de regels van de WPR op te nemen in de algemene maatregel van bestuur over de rechtspositie van de leden van de Kamer. Het lijkt niet nodig nader te formaliseren wie eerste en wie tweede plaatsvervangend voorzitter is. Dit kan worden overgelaten aan de Kamer zelf. Artikel 42, tweede lid, WPR is dan ook niet overgenomen.
Het tweede lid beoogt – in het verlengde van de eerder genoemde notitie «Herstel van het primaat van de politiek bij de aansturing van zelfstandige bestuursorganen» – veilig te stellen dat de bestuursleden van de Kamer geen commerciële nevenactiviteiten kunnen verrichten die gezien hun aard of omvang onverenigbaar zijn met hun werkzaamheden voor de Registratiekamer. Ten aanzien van de voorzitter van de Kamer bevatte artikel 40, derde lid, WPR al een dergelijke voorziening.

Artikel 56

Deze bepaling bouwt voort op de artikelen 41 en 42 WPR.
In het derde lid is overeenkomstig aanwijzingnummer 124K inzake zelfstandige bestuursorganen de regeling van interne aangelegenheden opgedragen aan de Registratiekamer. In het bestuursreglement wordt – naast de onderwerpen die in het derde lid zijn opgesomd – bij voorbeeld ook geregeld hoe het bestuur vergadert en hoe het besluiten neemt. Het reglement behoeft overeenkomstig aanwijzingnummer 124l, vierde lid, inzake zelfstandige bestuursorganen de goedkeuring van de Minister. Het reglement bevat geen voorschriften met betrekking tot de werkwijze van de Registratiekamer. De onafhankelijke taakuitoefening, bedoeld in artikel 52, tweede lid, vereist dat de Registratiekamer de vrijheid heeft haar werkwijze binnen de haar gegeven verdragsrechtelijke en wettelijke kaders te bepalen. Een goedkeuringsrecht van de Minister van Justitie verdraagt zich hier niet mee.

Artikel 57

Het eerste lid regelt de externe vertegenwoordigingsbevoegdheid van de Kamer. De leden van de Registratiekamer zijn elk voor zich bevoegd de Kamer te vertegenwoordigen volgens nader overeen te komen taakverdeling. In de praktijk vertegenwoordigen namelijk zowel de voorzitter als de beide leden, tevens plaatsvervangend voorzitter, de Registratiekamer bij haar uiteenlopende werkzaamheden. Er is geen behoefte gebleken aan een gedetailleerde regeling van de interne inrichting van de Kamer als opgenomen in de artikelen 43 en 44 WPR. Daarvoor in de plaats bepaalt het tweede lid van dit wetsvoorstel thans dat de leden een verdeling van taken vaststellen en hierbij zoveel mogelijk de buitengewone leden betrekken. De buitengewone leden kunnen daarmee een brede maatschappelijke inbreng in de afhandeling van zaken bewerkstelligen.

Artikel 58

De Kamer stelt overeenkomstig aanwijzing 124s inzake zelfstandige bestuursorganen jaarlijks een verslag op van het gevoerde beleid en beheer in het afgelopen kalenderjaar. Artikel 37, vijfde lid, WPR verplichtte de Kamer reeds jaarlijks een openbaar verslag uit te brengen van haar werkzaamheden en bevindingen.

Artikel 59

Dit artikel bepaalt dat de Registratiekamer desgevraagd aan de Minister de voor de uitoefening van zijn taak benodigde inlichtingen moet verstrekken met betrekking tot haar werkzaamheden die deze behoeft voor diens taakuitoefening ten opzichte van de Kamer. Daarmee wordt invulling gegeven aan de politieke verantwoordelijkheid van de Minister voor de Registratiekamer voor zover de taak van de Minister strekt. Het zal daarbij in hoofdzaak gaan om zaken betreffende formatie, budget en personeel. Een algemene aanwijzingsbevoegdheid met betrekking tot het boetebeleid is opgenomen in artikel 74. De formulering van het eerste lid sluit aan bij aanwijzing 124t inzake zelfstandige bestuursorganen. De formulering van de bepaling impliceert dat de noodzaak tot het vragen van inlichtingen naar objectieve maatstaven dient te worden vastgesteld. Ook het tweede lid houdt rekening met de bijzondere positie van de Registratiekamer. Daar de Kamer ook een toezichthoudende functie heeft tegenover de overheid, dient zij de mogelijkheid te hebben, wanneer een onderzoek zich tegen de overheid richt, dit te kunnen afronden zonder het

in gevaar te brengen. Zij kan dan de naleving van de informatieverplichting opschorten lopende het onderzoek. Daartoe dient het tweede lid.
Ten slotte bevat het derde lid een uitzondering op de in het eerste lid neergelegde verplichting voor zover de betreffende informatie aan de Registratiekamer is verstrekt door een derde onder de voorwaarde dat het geheime karakter daarvan wordt gehandhaafd. De toezichthoudende taak van de Kamer zou kunnen worden belemmerd indien de Kamer jegens degenen aan wie informatie worden gevraagd, niet kan garanderen dat deze absoluut vertrouwelijk wordt behandeld. Een vergelijkbare regeling is opgenomen in artikel 19, vierde lid, van de Wet Nationale Ombudsman. Uiteraard geldt deze uitzondering alleen indien de betreffende de derde uitdrukkelijk heeft bedongen dat de Kamer de gegevens geheim dient te houden. Daartoe kan bijvoorbeeld reden zijn indien de gevraagde inlichtingen of bescheiden gevoelige bedrijfsinformatie bevatten.

Artikel 60

De Kamer beschikt over een aantal onderzoeksbevoegdheden. De artikelen 60 en 61 bevatten een uitwerking van deze bevoegdheden. Artikel 28, vierde lid, van de richtlijn schrijft voor dat een ieder bij de Registratiekamer een verzoek moet kunnen indienen met betrekking tot de bescherming van zijn persoonlijke levenssfeer in verband met verwerking van zijn persoonsgegevens, meer in het bijzonder verzoeken om een onderzoek te doen naar de rechtmatigheid van een dergelijke verwerking. In het verlengde hiervan bepaalt artikel 60 dat de Kamer bevoegd is ambtshalve of op verzoek een onderzoek in te stellen naar een bepaalde verwerking van persoonsgegevens. Dit onderzoek kan zowel betreffen de overeenstemming met de wet, als de vraag of de verwerking op een behoorlijke en zorgvuldige wijze is geschied (artikel 6). Deze bevoegdheid ligt in het verlengde van die van artikel 46 WPR.
Indien het onderzoek ambtshalve geschiedt, kan het leiden tot een meer vrijblijvende rapportage, bij voorbeeld in het jaarverslag van de Kamer, maar onder omstandigheden evenzeer tot een van de sancties, genoemd in hoofdstuk 10. Geschiedt het onderzoek op verzoek van een betrokkene of een belanghebbende, dan leidt het tevens tot een mededeling of bericht over de bevindingen van de Kamer aan deze. Tegen deze mededeling of dit bericht staat – wegens ontbreken van een rechtsgevolg – geen bezwaar of beroep open. Het onderzoek en de weergave van de bevindingen vormt een onderdeel van de uitoefening van de toezichthoudende taak van de Registratiekamer en kan een voorbereiding zijn op nadere besluitvorming. In dat verband bestaat er wel rechtsbescherming tegen een mogelijk daarop volgende beschikking tot toepassing van bestuursdwang of een weigering daartoe.
De onderzoeksbevoegdheid, bedoeld in artikel 60, onderscheidt zich van het voorafgaand onderzoek, geregeld in de artikelen 31 en 32 vanwege het karakter er van. De algemene onderzoeksbevoegdheid heeft tot doel te komen tot een vorm van waarheidsvinding en is feitelijk van aard. Het voorafgaand onderzoek daarentegen leidt blijkens artikel 32 tot een verklaring die uiteindelijk door de rechter kan worden getoetst.
De beoordeling of een organisatie de wettelijke voorschriften over gegevensbescherming naleeft kan een diepgaand onderzoek vergen binnen die organisatie. In 1995 is de Registratiekamer gestart met het opbouwen van deskundigheid op het gebied van de privacy-audits. Proef-audits werden onder meer verricht binnen een politie-organisatie en een instelling voor de geestelijke gezondheidszorg. Met behulp van privacy-audits is het mogelijk de reguliere handhavingstaak te intensiveren op vitale onderdelen van de privacywetgeving. Dergelijke audits kunnen met behulp van de normale onderzoeksbevoegdheden worden verrichten.

Artikel 61

Artikel 28, derde lid, van de richtlijn bepaalt over welke bevoegdheden een toezichthoudende autoriteit in ieder geval behoort te beschikken. De onderhavige bepaling geeft hieraan een nadere uitwerking. Het artikel dient steeds in samenhang te worden bezien met Afdeling 5.2 Awb.
In het eerste lid wordt geregeld welke personen zijn of kunnen worden belast met het toezicht op de naleving van hetgeen bij of krachtens dit wetsvoorstel is bepaald. Deze personen worden beschouwd als «toezichthouder» in de zin van artikel 5:11 Awb. Zij beschikken over de bevoegdheden van Afdeling 5.2 Awb. Het betreft hier onder meer het vragen van inlichtingen, het vorderen van inzage in zakelijke gegevens en bescheiden en het onderzoeken van zaken en vervoermiddelen.
In aanvulling op dit basispakket bevoegdheden is in het tweede lid de bevoegdheid opgenomen om onder bepaalde voorwaarden een woning te betreden zonder toestemming van de bewoner. Deze bevoegdheid bestaat ook thans al: zij wordt geacht besloten te liggen in het huidige artikel 45, derde lid WPR. Als extra waarborg wordt in het derde lid bepaald dat de toezichthouder voor de uitoefening van de bevoegdheid van het tweede lid de uitdrukkelijke en bijzondere volmacht van de kamer behoeft. Dit sluit aan bij het bestaande artikel 45, vierde lid, WPR. Voorts geldt op grond van artikel 5:13 Awb als beperking dat de toezichthouder de bevoegdheid slechts mag gebruiken voor zover dat redelijkerwijs nodig is voor de vervulling zijn taak.
Krachtens artikel 5:20, eerste lid, Awb is in beginsel een ieder verplicht aan de toezichthouder alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden. In het verlengde van het huidige artikel 45, vijfde lid, WPR kent het vierde lid de Registratiekamer de bevoegdheid toe om bestuursdwang toe te passen indien geen of onvoldoende medewerking als hiervoor bedoeld wordt verleend. Op de uitoefening van deze bevoegdheid is Afdeling 5.3 Awb van toepassing. Een aparte bepaling naast artikel 65, eerste lid, is nodig omdat laatstgenoemde bepaling uitsluitend ziet op schending van de verplichtingen die bij of krachtens de onderhavige wetsvoorstel zijn gesteld. In artikel 51, vierde lid, gaat het daarentegen om een medewerkingsverplichting die – afgezien van het tweede lid – geldt uit hoofde van een andere wet, nl. de Awb.
Het vijfde lid is ontleend aan het huidige artikel 45, zesde lid, WPR. De uitoefening van de aan de Kamer toekomende bevoegdheden valt onder de geheimhoudingsplicht. Artikel 2.5 van de Awb verplicht de Registratiekamer als bestuursorgaan tot geheimhouding. Afhankelijk van de omstandigheden, bij voorbeeld wanneer dit nodig is om misstanden aan de kaak te stellen, zal het echter tot haar taak behoren dat bepaalde – door haar ontdekte – zaken bekend worden gemaakt. Het is niet uitgesloten dat ook de daarbij betrokken verantwoordelijke wordt bekend gemaakt. Doorslaggevend is of een goede taakuitoefening van de Kamer daartoe noodzaakt. In andere gevallen zal bij een eventueel beroep op de Wet openbaarheid van bestuur de belangen van de verantwoordelijke zwaarder moeten worden afwogen tegen het belang van het verstrekken van informatie aan een geïnteresseerde verzoeker.
Het zesde lid ten slotte legt aan de Registratiekamer een medewerkingsplicht op jegens de toezichthoudende autoriteiten van de andere lid-staten van de Unie. De bepaling vormt de implementatie van artikel 28, zesde lid, van de richtlijn.

Artikel 62

Het Duitse recht kent vanouds binnen de private sector een toezichthouder binnen het eigen bedrijf. In de particuliere sector is het gebruikelijk dat bij bedrijven boven een bepaalde omvang het toezicht op de verwerking van persoonsgegevens plaatsvindt door een toezichthouder binnen het bedrijf. Deze bedrijven zijn dan ook uitgezonderd van een meldingsplicht, tenzij zij de verstrekking van persoonsgegevens aan derden, zoals krediet- en handelsinformatiebureaus, tot doel hebben. Dit systeem heeft ten grondslag gelegen aan het voorschrift in de richtlijn (artikel 18, tweede lid, tweede gedachtenstreepje) dat de lid-staten de mogelijkheid hebben om als alternatief voor de melding bij de van overheidswege ingestelde toezichthouder, voor te schrijven dat gemeld kan worden bij een door de verantwoordelijke aangestelde toezichthouder. Op verzoek van Nederland is tevens de mogelijkheid geopend een toezichthouder door de aangesloten verantwoordelijken te laten aanstellen op brancheniveau en bij deze te melden. De interne toezichthouder moet wel aan een aantal kwaliteitseisen voldoen. Van deze mogelijkheid wordt in de WBP gebruik gemaakt. Ingevolge artikel 27, derde lid, meldt de verantwoordelijke de gegevensverwerking bij de Registratiekamer of bij een functionaris voor de gegevensbescherming. In het wetsvoorstel en in de memorie van toelichting wordt deze interne toezichthouder aangeduid als «functionaris». Dit begrip is ook in de definitiebepaling nader omschreven. Het systeem van een interne toezichthoudende functionaris sluit eveneens aan bij de behoeften die ingevolge de juridische evaluatie in de praktijk zijn gebleken.

Artikelen 63 en 64

Deze artikelen gaan uit van een individuele functionaris. Daar waar er privacy-commissies werkzaam zijn, is het dus nodig dat één van de leden de verantwoordelijkheid op zich neemt voor het uit te oefenen toezicht. Hij kan zich laten vertegenwoordigen door anderen; bijvoorbeeld leden van een privacy-commissie. Dit laat de verantwoordelijkheid van de individueel aangewezen functionaris onverlet.
De toezichthoudende functionaris moet aan bepaalde vereisten voldoen. Hij moet bijvoorbeeld over toereikende kennis beschikken. Hieronder wordt verstaan kennis van de organisatie, de gegevensverwerkingen die zich binnen de organisatie afspelen, de belangen die daarbij betrokken zijn en uiteraard kennis van de privacywetgeving die op de verwerkingen binnen zijn organisatie van toepassing is. Ook moet hij voldoende betrouwbaar worden geacht. Deze betrouwbaarheid uit zich bijvoorbeeld in het vermogen alle bij de verwerkingen betrokken belangen op een onafhankelijke wijze tegen elkaar te kunnen afwegen. De functionaris moet in staat zijn op een juiste en zorgvuldige wijze gebruik te maken van zijn bevoegdheden zoals geregeld in afdeling 5.2 van de Algemene wet bestuursrecht.
De Registratiekamer moet op de hoogte gebracht worden van de naam van deze functionaris. De Registratiekamer moet namelijk met hem contact kunnen onderhouden in geval navraag wordt gedaan over gegevensverwerkingen die niet zijn vrijgesteld. Een melding van gegevensverwerkingen bij deze functionaris lijkt zinvol en kan in de plaats komen van die aan de Registratiekamer. Verantwoordelijken hebben daarmee de keuze, hetzij te melden bij een functionaris in eigen dienst, hetzij bij de van overheidswege benoemde functionaris: de Registratiekamer.
Overigens laat de benoeming van een toezichthouder de toezichthoudende bevoegdheden van de Registratiekamer onverlet. De toezicht-

houder vervangt de Registratiekamer slechts voor wat betreft de meldingen van de meldingsplichtige gegevensverwerkingen. Dit laat onverlet dat ook niet-meldingsplichtige gegevensverwerkingen bij de functionaris kunnen worden aangemeld. Dit ligt eerder in de rede bij een functionaris die door een individuele verantwoordelijke is aangemeld. De functionaris pleegt een overzicht te hebben van de verwerkingen binnen de organisatie of de branche. Met de melding van de niet-meldingsplichtige gegevensverwerkingen kan de functionaris een totaalbeeld van alle verwerkingen krijgen. Deze melding komt de transparantie ten goede, mede omdat vanuit een dergelijk totaalbeeld op het niveau van de individuele verantwoordelijke, makkelijk een antwoord gegeven kan worden op vragen naar de gegevensverwerkingen van de verantwoordelijke.
De richtlijn stelt twee eisen aan de functionaris: allereerst dient het toezicht op een wijze te worden uitgeoefend dat het op onafhankelijke wijze plaatsvindt en ten tweede dat de inbreuk op de rechten en vrijheden van de betrokkenen onwaarschijnlijk is. Daar de regeling is opgesteld tegen de achtergrond van de Duitse wet, zijn de waarborgen in die wet die gelden voor interne toezichthouders, grotendeels overgenomen in het onderhavige wetsvoorstel. De bepalingen in het derde tot en met vijfde lid moeten in dat licht worden gezien. Om zijn toezicht daadwerkelijk te kunnen uitoefenen, is het noodzakelijk dat de functionaris over adequate bevoegdheden beschikt, zoals bijvoorbeeld toegang tot alle systemen waar mogelijk gegevens worden verwerkt. Daartoe is in het wetsvoorstel opgenomen dat de verantwoordelijke of de organisatie door wie de functionaris is aangesteld er voor zorg dient te dragen dat hij vergelijkbare bevoegdheden heeft als de Registratiekamer op grond van Afdeling 5.2 Awb. Het ligt in de rede dat deze schriftelijk worden vastgelegd. In de gekozen constructie ligt besloten dat de functionaris voor de gegevensbescherming niet wordt beschouwd als een toezichthouder in de zin van artikel 5:11 Awb. De functionaris wordt immers niet bij of krachtens wettelijk voorschrift met het houden van toezicht belast. Het betreft hier een facultatief instituut dat wordt ingesteld door de verantwoordelijke of door een organisatie van verantwoordelijken op basis van een interne regeling. Het ligt in de rede dat in dat geval ook de bevoegdheden van de toezichthouder bij interne regeling worden vastgesteld. Artikel 64, derde lid, sluit daarbij aan.
Oefent de functionaris een van zijn bevoegdheden uit en treft hij onregelmatigheden aan, dan ligt in zijn taakopdracht en in zijn aanstelling besloten dat hij daarover verslag uitbrengt aan de verantwoordelijke of de organisatie waardoor hij is aangesteld. De functionaris heeft geen verplichting onregelmatigheden te melden bij de Registratiekamer; hij is immers niet de verlengde arm van deze kamer.
Daar staat tegenover dat de Registratiekamer te allen tijde zijn bevoegdheden kan uitoefenen, ook al is er een functionaris aangesteld binnen de organisatie of branche. Adviezen die de functionaris aan de verantwoordelijke geeft kunnen door de Registratiekamer veroordeeld worden en de verantwoordelijke kan zich dus ook niet beroepen op het opvolgen van bepaalde adviezen. Evenzeer moet rekening worden gehouden met de reële mogelijkheid dat de functionaris de verantwoordelijke aanbevelingen doet die niet voldoen aan wettelijke normeringen. Heeft een verantwoordelijke twijfels over de grondslag van een aanbeveling van de functionaris, dan kan hij de Registratiekamer een nader oordeel vragen. De bedoeling is dat een soepel samenspel zich ontwikkelt tussen functionaris, verantwoordelijke en de Registratiekamer, maar in dit spel zijn conflicten niet uit te sluiten. Het is daarbij echter te verwachten dat in gevallen van het optreden van een functionaris de bemoeienis van de Registratiekamer een meer afstandelijke kan zijn.
Er is van afgezien om voor te schrijven dat de functionaris een jaarverslag opstelt. Het is aan degene die een functionaris aanstelt dit eventueel te

eisen. Indien een functionaris werkzaam is ten behoeve van een rechtspersoon of van rechtspersonen die verplicht zijn een jaarrekening en een jaarverslag uit te brengen, ligt het in de rede dat de functionaris een eventueel jaarverslag, voor zover zijn geheimhoudingsplicht dat toelaat, afstemt met de accountant die ingevolge artikel 2:393, vierde lid, tweede volzin, BW in zijn verslag aan de raad van commissarissen en aan de raad van bestuur melding maakt van zijn bevindingen met betrekking tot de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking.

HOOFDSTUK 10 SANCTIES

PARAGRAAF 1 BESTUURSDWANG

Artikel 65

In artikel 28, derde lid, van de richtlijn wordt bepaald dat de toezichthoudende autoriteit dient te beschikken over effectieve bevoegdheden om in te grijpen. Ter uitvoering van deze bepaling wordt in artikel 65 aan de Registratiekamer de bevoegdheid toegekend om bestuursdwang toe te passen. De bevoegdheid kan worden uitgeoefend indien naar het oordeel van de kamer in strijd wordt gehandeld met de bij of krachtens dit wetsvoorstel gestelde verplichtingen. Zij kan tot dit oordeel komen naar aanleiding van een voorafgaand onderzoek als bedoeld in artikel 31, maar ook naar aanleiding van een onderzoek als bedoeld in artikel 60. Laatstbedoeld onderzoek kan zowel ambtshalve als op verzoek van de betrokkene worden verricht.
Met «effectieve bevoegdheden om in te grijpen» wordt blijkens de eerdergenoemde richtlijnbepaling onder meer gedoeld op de bevoegdheid om afscherming, uitwissing of vernietiging van gegevens te gelasten. Materieel gezien komt deze bevoegdheid neer op een bestuursdwangbevoegdheid. Het gaat immers conform de omschrijving van artikel 5:21 Awb om «het door feitelijk handelen optreden tegen hetgeen in strijd met bij of krachtens enig wettelijk voorschrift – in casu de WBP – gestelde verplichtingen is of wordt gedaan, gehouden of nagelaten». Om die reden wordt bepaald dat de Registratiekamer bevoegd is tot de toepassing van bestuursdwang. Met deze enkele bepaling kan worden volstaan. De uitoefening van bestuursdwang wordt verder geregeld in Afdeling 5.2 van de Awb. Uit deze regels volgt onder meer dat een beslissing van de kamer tot toepassing van bestuursdwang op schrift moet worden gesteld. In die schriftelijke beslissing moet een termijn worden gesteld waarbinnen de verantwoordelijke de tenuitvoerlegging kan voorkomen door zelf maatregelen te treffen. Voorts volgt uit artikel 5:32, eerste lid, Awb, dat de Registratiekamer in plaats van bestuursdwang ook een last onder dwangsom kan opleggen. Ook in dat geval dient de verantwoordelijke een termijn te worden gegund om eerst zelf de overtreding ongedaan te maken.

PARAGRAAF 2 BESTUURLIJKE BOETEN

Artikel 66

Deze bepaling kent aan de Registratiekamer in bepaalde gevallen de bevoegdheid toe om een bestuurlijke boete op te leggen. Het gaat om sanctionering van een beperkt aantal overtredingen van het wetsvoorstel die alle betrekking hebben op de verplichting om verwerkingen bij de Registratiekamer te melden. Concreet betreft het ten onrechte achterwege laten van de melding (artikel 27, eerste lid), het achterwege laten van de melding van een niet-geautomatiseerde verwerking voor zover onderworpen aan een voorafgaand onderzoek (artikel 27, tweede lid), het

starten van de verwerking alvorens de melding heeft plaatsgevonden (artikel 27, derde lid), het doen van een onvolledige melding (artikel 28, eerste lid), het achterwege laten van de melding van het doel of de doeleinden waarvoor de gegevens of de categorieën van gegevens zijn verzameld, het niet of niet tijdig doorgeven van wijzigingen van de eerder gemelde gegevens (artikel 28, derde lid) en het niet vastleggen of bewaren van een specifieke categorie van verwerkingen (artikel 28, vierde lid).
De genoemde feiten zijn geschikt te achten om door middel van een boete bestuursrechtelijk te worden afgedaan. Zij voldoen aan de voorwaarden die in het kabinetsbeleid inzake bestuurlijke boeten worden gesteld om voor bestuursrechtelijke afhandeling in aanmerking te komen (vgl. kamerstukken II 1993/94, 23 400 VI, nr. 48, blz. 8 e.v.). Het betreft hoofdzakelijk verplichtingen van administratieve aard. Het gaat derhalve niet om feiten die vanwege hun morele lading van een strafrechtelijke sanctionering moeten worden voorzien. Evenmin bestaat er een sterke behoefte aan toepassing van ingrijpende dwangmiddelen in welk geval handhaving van de bestaande strafrechtelijke sanctionering eveneens zou zijn aangewezen.
Een belangrijke overweging is voorts dat de omvang van de aanmeldingsplicht in beginsel zodanig duidelijk uit de regelgeving, dan wel de daaruit voortvloeiende toepassingspraktijk zal zijn af te leiden dat meestal gemakkelijk kan worden vastgesteld of een overtreding heeft plaatsgevonden. De verwachting is dan ook gerechtvaardigd dat in het overgrote deel van de gevallen de Registratiekamer een overtreding van de meldingsverplichting betrekkelijk eenvoudig zal kunnen constateren. Een uitgebreid onderzoek zal in een dergelijke gevallen niet nodig zijn. In sommige situaties zal evenwel twijfel kunnen bestaan over de vraag of en zo ja, op welke wijze aan de wettelijke verplichting moet worden voldaan. Dit zal zich bijvoorbeeld kunnen voordoen indien niet zeker is of sprake is van een verwerking in de zin van het wetsvoorstel of in hoeverre in het kader van een verwerking sprake is van samenhangende doeleinden. Deze omstandigheid is echter niet van overwegende betekenis. Het gaat in de eerste plaats om uitzonderingen. Verder zal de onduidelijkheid die zich op bepaalde punten kan voordoen in de praktijk in onderling overleg tussen de voor de verwerking verantwoordelijke en de Registratiekamer goeddeels kunnen worden weggenomen. Na verloop van tijd zal door het ontstaan van een binnen het kader van de wet ontstane gedragslijn eventuele onzekerheid verder worden gereduceerd.
Van belang in dit verband is dat in (artikel 66, tweede lid) wordt bepaald dat de Registratiekamer geen boete mag opleggen indien de verantwoordelijke aan wie de overtreding kan worden toegerekend aannemelijk maakt dat hem van de overtreding geen verwijt kan worden gemaakt. In het bestuursrecht geldt als algemeen uitgangspunt dat de rechter bepaalt hoe de bewijslast moet worden verdeeld (vrije bewijsleer). Bij boetebeschikkingen vloeit evenwel uit het artikel 6, tweede lid, EVRM geldende vermoeden van onschuld voort dat de bewijslast in beginsel op het bestuur moet rusten. Hierbij behoeft niet te worden aangetoond dat verwijtbaar is gehandeld. Het bestuursorgaan mag binnen redelijke grenzen uitgaan van een objectief vermoeden van schuld, mits de betrokkene de gelegenheid krijgt aannemelijk te maken dat hem van de overtreding geen verwijt kan worden gemaakt (EHRM 7-10-1988, NJ 1991, 351). Dit principe wordt wettelijk verankerd in de onderhavige bepaling. In hoeverre sprake is van verwijtbaarheid, hangt af het concrete geval. Onder bepaalde omstandigheden kan het proces van gegevensverwerking zodanig uitzonderlijk of gecompliceerd zijn dat de verantwoordelijke in redelijkheid niet kan worden tegengeworpen dat hij zijn wettelijke meldingsverplichting niet of niet volledig heeft nageleefd. Het is aan de verantwoordelijke om aannemelijk te maken dat zich een dergelijke

situatie in concreto voordoet. Het zal hier vermoedelijk gaan om uitzonderingssituaties.
In het derde lid wordt bepaald dat de Registratiekamer bij de vaststelling van de hoogte van de boete in ieder geval rekening dient te houden met de ernst en de duur van de overtreding. Op deze twee punten kunnen zich in de praktijk veel variaties voordoen. De zinsnede «in ieder geval» geeft aan dat de Registratiekamer niet uitsluitend dient te letten op deze twee factoren. Afhankelijk van de omstandigheden zullen ook andere factoren in de afweging een rol kunnen spelen. Te denken valt aan mogelijke recidive, alsmede de bereidheid van de betrokken verantwoordelijke om de overtreding ongedaan te maken.
In het vierde lid wordt bepaald dat de werkzaamheden die in het kader van de voorbereiding en vaststelling van de boetebeschikking alleen mogen worden verricht door personen die niet betrokken zijn geweest bij de opstelling van het in artikel 67, eerste lid, bedoelde rapport en het daaraan voorafgaande onderzoek. Binnen het gekozen systeem van bestuursrechtelijke handhaving is het van groot belang dat de beslissing omtrent sanctionering zo objectief en onbevooroordeeld als mogelijk plaatsvindt. In dat licht bezien is het wenselijk om te voorkomen dat de werkzaamheden die na het opstellen van het rapport moeten worden verricht – met name het horen van belanghebbenden en het concipiëren van de beschikking – door dezelfde functionarissen worden verricht als die welke eerder feitelijk bij het onderzoek naar die overtreding waren betrokken. Het verdient de voorkeur een dergelijke scheiding in de wet te verankeren. Zij is in overeenstemming met het kabinetsstandpunt over het advies van de Commissie voor de Toetsing van Wetgevingsprojecten «Handhaving door bestuurlijke boeten» (kamerstukken II 1993/94, 23 400 VI, nr. 48).
Zoals in het algemeen deel van deze memorie reeds is uiteengezet, blijft strafrechtelijke handhaving van de meldingsverplichting – conform het huidige artikel 50 WPR – mogelijk. Om die reden zijn voorzieningen nodig om samenloop van punitieve sancties te voorkomen. Het vijfde lid bevat een dergelijke voorziening. De bevoegdheid tot boeteoplegging vervalt indien terzake van hetzelfde feit in het kader van een strafvervolging het onerzoek ter terechtzitting is gestart of een transactie in strafrechtelijke zin heeft plaatsgevonden. De bepaling komt overeen met de aanbeveling ter zake van de Commissie voor de Toetsing van Wetgevingsprojecten. Een spiegelbeeldige bepaling is opgenomen in artikel 75.
Om bij de uitoefening van de diverse sanctiebevoegdheden een adequate afstemming te garanderen, dient zonodig overleg tussen OM en Registratiekamer plaats te vinden. In dit licht bezien ligt het in de rede dat de Registratiekamer gedurende de voorbereiding van een te nemen boetebeschikking, het OM over zijn voornemen informeert. Ook het omgekeerde ligt voor de hand. In het sporadische geval dat het OM zou besluiten tot vervolging, zal het OM vooraf in contact treden met de Registratiekamer.

Artikel 67

Indien de Registratiekamer een overtreding constateert als bedoeld in het eerste lid van het vorige artikel, dient op grond van de zich voordoende omstandigheden te worden bezien of het in de rede ligt om een boete op te leggen. Is dat inderdaad het geval dan dient een rapport te worden opgemaakt. Het rapport markeert het formele begin van de daarop volgende fase van de procedure, te weten het horen van de belanghebbenden. Het begrip «rapport» is ontleend aan het advies van de Commissie voor de Toetsing van Wetgevingsprojecten «Handhaving door bestuurlijke boeten» (hierna: CTW-advies). De in het tweede lid voorgestelde inhoud van het rapport is grotendeels eveneens uit dit advies overgenomen.

Ingevolge artikel 6, derde lid, onder a, EVRM heeft een ieder het recht om onverwijld op de hoogte te worden gebracht van de aard en de reden van de tegen hem ingebrachte beschuldiging in een taal die hij verstaat. In de regel zal geen taalvoorziening nodig zijn: aangenomen mag worden dat binnen de organisatie van de verantwoordelijke altijd wel iemand beschikbaar is die het Nederlands beheerst en bevoegd is namens de verantwoordelijke op te treden. Ten einde zeker te stellen dat de waarborgen van het EVRM in acht worden genomen, is evenwel in het vierde lid toch een taalvoorziening opgenomen, indien dat onverhoopt niet het geval zou zijn.

Artikel 68

Dit artikel treft een voorziening voor het zwijgrecht en de cautieplicht. De eerste volzin regelt het zwijgrecht ofwel het recht om geen belastende verklaring tegen zichzelf af te hoeven leggen ter zake van de in onderzoek zijnde overtreding. De toezichthoudende ambtenaren van de Registratiekamer hebben op grond van de Awb de bevoegdheid om inlichtingen te vorderen. Degene tot wie een zodanig verzoek wordt gericht, is in beginsel verplicht die inlichtingen te verstrekken. Deze verplichting kan evenwel niet onverkort gehandhaafd blijven ingeval de betreffende ambtenaren een onderzoek verrichten naar een mogelijke overtreding. Op grond van artikel 14, derde lid, onder g, IVBPR mag niemand bij het bepalen van de gegrondheid van een tegen hem ingestelde strafvervolging worden gedwongen tegen zichzelf te getuigen of een bekentenis af te leggen. Het zwijgrecht wordt ook via de jurisprudentie gewaarborgd in artikel 6, eerste lid, EVRM (EHRM 25-2-1993, NJ 1993, 485 m.n. Kn. (Funke)). Dit zwijgrecht gaat niet zover dat iedere vorm van medewerking aan het verzamelen van belastend materiaal kan worden geweigerd. De Hoge Raad heeft in een reeks van uitspraken op het gebied van het strafrecht geoordeeld dat «in het Nederlandse recht niet een onvoorwaardelijk recht of beginsel is verankerd, volgens hetwel een verdachte op generlei wijze kan worden verplicht tot het verlenen van medewerking aan het verkrijgen van voor hem belastend materiaal» (bijv. HR 15-2-1977, NJ 1977, 557 en HR 5-1-1982, NJ 1982, 308). Deze lijn is onlangs door het EHRM bevestigd in de Saunders-zaak (EHRM 17 december 1996, NJCM-Bull. 22-3 (1997), p. 298 e.v.). Volgens dit arrest gaat het zwijgrecht niet zover dat de verdachte niet zou kunnen worden verplicht tot het afgeven van materiaal dat bestaat onafhankelijk van de wil van de betrokkene, zoals schriftelijke documenten en lichaamsmateriaal.
Het CTW-advies en het kabinetsstandpunt ter zake onderschrijven de aldus weergegeven inhoud van het zwijgrecht in relatie tot de oplegging van bestuurlijke boeten. Hierbij wordt voorts aandacht besteed aan de vraag vanaf welk moment het zwijgrecht moet gelden. Naar de mening van het kabinet vloeit uit artikel 6 EVRM voort dat het zwijgrecht moet worden gerespecteerd vanaf het moment dat van een «criminal charge» in de zin van voormelde bepaling sprake is. Volgens de fiscaalrechtelijke jurisprudentie van de Hoge Raad is van «criminal charge» eerst sprake op het moment waarop jegens een persoon vanwege de Staat een handeling is verricht waaraan deze persoon in redelijkheid de gevolgtrekking heeft kunnen verbinden dat aan hem een boete zal worden opgelegd (vgl. HR 17-2-1987, NJ 1987, 951, HR 23-6-1993, BNB 1993, 271). Het zwijgrecht geldt volgens dit criterium dus niet in de controlefase waarin nog geen sprake is van een «criminal charge». Wel gelden blijkens het eerder genoemde Saunders-arrest beperkingen als het gaat om het gebruik van het in de controlefase verzamelde materiaal in een latere fase, indien dat materiaal onder dwang is verkregen.
In het onderhavige artikel is nauw aangesloten bij de zojuist vermelde jurisprudentie van de Hoge Raad. Overeenkomstig de door de Hoge Raad aangelegde maatstaf is de verantwoordelijke jegens wie een handeling is

verricht waaraan hij in redelijkheid de gevolgtrekking kan verbinden dat hem wegens een overtreding als bedoeld in artikel 66, eerste lid, een boete zal worden opgelegd, niet verplicht ter zake een verklaring af te leggen. Wanneer dat moment zich voordoet zal aan de hand van de feiten en omstandigheden van het concrete geval moeten worden beoordeeld. In de regel zal sprake zijn van een «criminal charge» vanaf het moment waarop conform artikel 67, vierde lid, een afschrift van het rapport aan de verantwoordelijke wordt toegestuurd. Aan dat rapport kan de verantwoordelijke kan de verantwoordelijke in redelijkheid de gevolgtrekking verbinden dat hem een boete zal worden opgelegd.
De tweede volzin bevat een cautieplicht. Noch artikel 6 EVRM, noch artikel 14 IVBPR schrijven een zodanige plicht voor. Niettemin wordt zowel in het CTW-advies als in het kabinetsstandpunt ter zake gesteld dat het wenselijk is in procedures inzake bestuurlijke boeten – analoog aan artikel 29 Sv. – in een cautieplicht te voorzien. De cautie moet worden gegeven voordat vragen worden gesteld die zouden kunnen leiden tot een verklaring.

Artikel 69

Afdeling 4.1.2 Awb geeft voorschriften voor de voorbereiding van een beschikking. Uit deze bepalingen vloeit voort dat toepassing van de hoorplicht alvorens een beschikking wordt genomen, in bepaalde gevallen achterwege kan blijven. Het kabinet meent echter dat bij boete-beschikkingen – als zijnde punitieve sancties – in beginsel voorzien dient te worden in een hoorplicht voordat de boete wordt opgelegd. De Registratiekamer kan zelf bepalen op welke wijze desgewenst mondeling gehoord kan worden.
Op grond van artikel 6, derde lid, onder e, EVRM heeft een ieder tegen wie een vervolging is ingesteld, het recht zich kosteloos doen bijstaan door een tolk, indien hij de taal die ter terechtzitting wordt gebezigd niet verstaat of niet spreekt. Hoewel dit recht zich strikt genomen niet uitstrekt tot de bestuurlijke fase, ligt het in de rede in voorkomende gevallen dit recht ook toe te kennen met het oog op het horen voorafgaande aan de boeteoplegging. Zoals ook uiteengezet is bij artikel 67, vierde lid, zal slechts sporadisch behoefte zijn aan een dergelijke voorziening.

Artikel 70

Indien de voorbereidende procedure zoals beschreven in voorgaannde artikelen is doorlopen, dient de Registratiekamer te beslissen of al dan niet een boete wordt opgelegd. Het eerste lid bepaalt dat dit bij beschikking geschiedt. Hiertegen staat bezwaar en beroep open op grond van de Awb. Voorts wordt in het tweede lid overeenkomstig het CTW-advies een nadere invulling gegeven aan de reeds uit de Awb voortvloeiende motiveringsvoorschriften. Ten slotte bevat ook dit artikel een taalvoorziening voor degenen die de Nederlandse taal onvoldoende begrijpt. Verwezen zij naar de toelichting op artikel 3.9, vierde lid waar voor het rapport eenzelfde voorziening is opgenomen.

Artikel 71

In het bestuursrecht geldt als hoofdregel dat het maken van bezwaar of het instellen van beroep geen schorsing van het omstreden besluit met zich meebrengt (artikel 6.16 Awb). De CTW heeft evenwel geadviseerd bij de bestuurlijke boete als specifieke sanctiebeschikking aan bezwaar schorsende werking toe te kennen. In het onderhavige artikel hebben wij dit advies gevolgd.

Artikel 72

Dit artikel bepaalt dat de bevoegdheid tot het opleggen van een boete vervalt vijf jaar nadat de overtreding is begaan. Omwille van de rechtszekerheid behoort de periode waarover de bevoegdheid tot oplegging van een boete bestaat, duidelijk worden begrensd. Gekozen is voor een termijn van vijf jaar mede omdat een overtreding eerst na verloop van tijd aan het licht kan komen. In enkele andere wetsvoorstellen is voor eenzelfde termijn gekozen. De termijn van vijf jaar heeft betrekking op het tijdvak tussen de overtreding en de boetebeschikking van de Registratiekamer. De duur benodigd voor de afwikkeling van een eventuele bezwaarschrift- of beroepsprocedure en voor de tenuitvoerlegging van de boetebeschikking ligt niet in deze periode besloten.

Artikel 73

Dit artikel bevat een aantal standaardregels voor de aanmaning en invordering van de boete. De voorstellen van de CTW zijn op dit punt gevolgd. Het komt er op neer dat de boete binnen zes weken moet worden betaald nadat de boete is opgelegd. Wordt niet binnen deze termijn betaald, dan wordt de betrokkene aangemaand om alsnog binnen twee weken zijn schuld te voldoen. Indien dan nog niet wordt betaald dan is er de bevoegdheid om bij dwangbevel in te vorderen. Een dwangbevel is een executoriale titel in de zin van het Wetboek van Burgerlijke Rechtsvordering. Op de verdere tenuitvoerlegging zijn de in dit wetboek opgenomen regels van toepassing.

Artikel 74

De Registratiekamer heeft conform de EU-richtlijn een toezichthoudende taak die hij op onafhankelijke wijze uitoefent. De aldus gekenschetste positie van de Kamer verdraagt zich niet met een algemene bevoegdheid van de minister van Justitie tot het geven van algemene aanwijzingen. Een dergelijke algemene bevoegdheid is dan ook niet in het wetsvoorstel opgenomen. In het onderhavige artikel is evenwel een uitzondering daarop gemaakt specifiek gericht op de oplegging van bestuurlijke boeten. De minister van Justitie heeft een bijzondere verantwoordelijkheid met betrekking tot de eenheid van de rechtshandhaving. Dit geldt in het bijzonder als het gaat om punitieve sancties zoals de bestuurlijke boete. Vanuit dit oogpunt achten wij het gewenst dat de minister van Justitie ter zake algemene aanwijzingen kan geven. De bevoegdheid tot het opleggen van boeten in concrete gevallen behoort evenwel tot de exclusieve verantwoordelijkheid van de Registratiekamer. Daarop heeft de bevoegdheid van de minister geen betrekking.
De algemene aanwijzingen zijn gegoten in de vorm van beleidsregels als bedoeld in artikel 1:3, vierde lid, Awb. In de formulering van de bepaling is daarop aangesloten. Een uitdrukkelijke bepaling is nodig omdat de bevoegdheid van de minister van Justitie niet rechtstreeks op artikel 4:81, eerste lid, Awb kan worden gebaseerd. Bij de vaststelling van beleidsregels op grond van de onderhavige bepaling zal de minister moeten voldoen aan de verplichtingen die voortvloeien uit hoofdstuk 3 en titel 4.3 van de Awb. Gekozen is voor beleidsregels in de plaats van algemeen verbindende voorschriften, omdat bij de te stellen regels inzake bestuurlijke boeten er uit een oogpunt van rechtsbescherming wellicht behoefte zal kunnen bestaan om in individuele gevallen af te wijken van de algemene regels.

Artikel 75

In het algemeen deel van de toelichting is reeds uiteengezet dat in uitzonderingsgevallen strafrechtelijke handhaving van de meldingsverplichting mogelijk moet blijven. In artikel 75, eerste lid, worden dezelfde feiten strafbaar gesteld waarvoor ook een bestuurlijke boete kan worden opgelegd. Om ongewenste samenloop te voorkomen wordt in het vijfde lid gergeld dat het recht tot strafvervolging vervalt indien de Registratiekamer reeds voor hetzelfde feit een boete heeft opgelegd. Voor de omgekeerde situatie bevat artikel 66, vijfde lid, een vergelijkbare voorziening. Om een adequate afstemming op dit terrein te garanderen, dient zonodig overleg tussen OM en Registratiekamer plaats te vinden. Verwezen zij naar de toelichting op artikel 66. Het tweede tot en met het vierde lid komen overeen met het tweede tot en met vierde lid van het huidige artikel 50 WPR.
In het algemeen deel van de toelichting is reeds aangegeven dat naast de meldingsplicht ook een beperkt aantal overtredingen strafbaar blijven die samenhangen met het internationale gegevensverkeer. Naast de meldingsplicht blijven ook een beperkt aantal overtredingen strafbaar die samenhangen met het internationale gegevensverkeer. Het betreft in de eerste plaats het verbod gericht tot een verantwoordelijke die buiten de Unie is gevestigd, om in Nederland gegevens te verwerken zonder een vertegenwoordiger aan te wijzen. Het betreffende voorschrift is vastgelegd in artikel 4, derde lid. Daarnaast is strafbaar de doorgifte van gegevens naar landen buiten de Unie waarvan op Europees niveau is bepaald dat geen passend beschermingsniveau aanwezig is. Een dergelijk besluit moet op grond van artikel 78, tweede lid, worden omgezet in een ministeriële regeling of beschikking. Overtreding van een zodanige regeling of beschikking wordt in artikel 75, eerste lid, strafbaar gesteld. Deze strafbaarstelling komt in grote lijnen overeen met het huidige artikel 50, eerste lid, onderdeel c, WPR.

HOOFDSTUK 11 GEGEVENSVERKEER MET LANDEN BUITEN DE EUROPESE UNIE

De bepalingen van het wetsvoorstel zijn van toepassing op de verwerking en bewerking van persoonsgegevens, ongeacht of deze gegevens in Nederland blijven of ook daarbuiten komen. De vraag rijst of aanvullende bepalingen nodig zijn voor de doorgifte van persoonsgegevens aan andere landen om te voorkomen dat het niveau van bescherming wordt omzeild door bepaalde vormen van verwerking of bewerking in het buitenland te verrichten. De WPR bevatte in dit opzicht in artikel 49, tweede lid, slechts de mogelijkheid bij algemene maatregel van bestuur de verstrekking aan het buitenland te verbieden. Van deze mogelijkheid is tot dusverre geen gebruik gemaakt. Met de toenemende technische mogelijkheden om gegevens massaal uit te wisselen, wordt het noodzakelijk in een aanvullend regime voor het internationale gegevensverkeer te voorzien.
In het algemeen deel van deze toelichting is uiteengezet dat de richtlijn gericht is op de voltooiing van de interne markt binnen de Europese Unie. Dit komt tot uitdrukking in artikel 1, tweede lid, van de richtlijn dat enige belemmering van het vrije verkeer van persoonsgegevens uit hoofde van bescherming van de persoonlijke levenssfeer verbiedt. Daarentegen wordt ten opzichte van landen buiten de Unie wel voorzien in een aanvullend regime in de artikelen 25 en 26 van de richtlijn.
De Unie is geen eiland in de wereld. Moderne informatietechnologische middelen maken de plaatsbepaling van gegevens steeds abstracter. Enerzijds werkt dit de mogelijkheden tot misbruik in de hand. De

regelgeving dient handvatten te bieden hiertegen te kunnen optreden. Anderzijds kan het verkeer van persoonsgegevens in contacten met landen buiten de Unie niet aan zodanige beperkingen worden onderworpen dat daardoor bij voorbeeld het reguliere handelsverkeer onnodig zou worden belemmerd. De vastgestelde bepalingen beogen deze belangentegenstelling in evenwicht te brengen, althans het instrumentarium aan te reiken om dit in voorkomend geval te bewerkstelligen.

Artikel 76

Met het begrip «doorgifte» in dit artikel wordt gedoeld op het ter kennis brengen van de gegevens aan een persoon die zich bevindt buiten de rechtsmacht van één van de landen van de Unie. Het gaat daarbij zowel om het gebruik van gegevens binnen concernverband, indien onderdelen van een concern zich binnen en buiten de Unie bevinden, de verstrekking aan derden die zich buiten de Unie bevinden, als om het ter beschikking stellen van de gegevens met het oog de bewerking daarvan. De bepaling is, evenals de bepaling in de richtlijn, in de lijdende vorm gesteld teneinde aan te geven dat deze zich richt tot een ieder. Dit betekent dat zowel verantwoordelijke als bewerker de geadresseerde zijn van het verbod tot doorgifte indien niet is voldaan aan de voorwaarden van dit hoofdstuk. Zie ook de toelichting op artikel 15.
Het uitgangspunt is dat de doorgifte van persoonsgegevens naar een land buiten de Unie slechts mogelijk is, indien dat andere land voldoende bescherming biedt. De beoordeling of hiervan sprake is, is allereerst opgedragen aan de verantwoordelijke. Het tweede lid van artikel 76 noemt een aantal criteria die bij de beoordeling in ieder geval in aanmerking moeten worden genomen. Het gaat daarbij niet om een beoordeling van de wetgeving in een ander land in het algemeen, doch om de vraag of met betrekking tot de doorgifte van de desbetreffende gegevens een passend beschermingsniveau kan worden geboden. In geval van twijfel zal de Registratiekamer nadere informatie kunnen verstrekken.
Denkbaar is bijvoorbeeld dat de vraag rijst of medische gegevens kunnen worden uitgewisseld voor wetenschappelijk onderzoek met een land gelegen buiten de Unie. Is er in dat land sprake van een deugdelijke wetgeving inzake medische gegevens, of is er anderszins een praktijk die een zorgvuldige omgang met dergelijke gegevens waarborgt, dan kunnen deze gegevens, ongeacht de overige wetgeving in dat land, worden verstrekt.
De Registratiekamer heeft de vraag geopperd of de bepaling ook van toepassing is op het verzamelen van persoonsgegevens met het oog op doorgifte naar een derde land. Wanneer de doorgifte niet is toegestaan, is, zo vloeit voort uit de algemene bepalingen, ook de verzameling van gegevens niet rechtmatig.
Verder wijst de Registratiekamer op de situatie dat een verantwoordelijke bijvoorbeeld via Internet persoonsgegevens uit een derde land verzamelt. Zodra de verantwoordelijke over persoonsgegevens macht kan uitoefenen omdat hij deze voor zich heeft opgeslagen, is de wet van toepassing. Het is niet van belang van op welke wijze hij deze persoonsgegevens heeft verkregen. Dat betekent dat ook aan betrokkenen die zich bijvoorbeeld bevinden in de Verenigde Staten, wanneer hun persoonsgegevens worden vergaard, zij daarover behoren te worden geïnformeerd in de zin van de artikelen 33 en 34 van het wetsvoorstel. Zou zo iemand op enigerlei wijze bemerken dat met overtreding van dit voorschrift persoonsgegevens over hem zijn verwerkt, bijvoorbeeld doordat hij specifiek op hem gerichte reclame ontvangt, dan kan hij in Nederland de rechtsmiddelen aanwenden die deze wet hem toekent.

Artikel 77

Eerste lid

Wanneer een land buiten de Unie onvoldoende bescherming van persoonsgegevens biedt, is verkeer van persoonsgegevens niet uitgesloten, doch onderworpen aan aanvullende regels. De bepaling bevat een aantal alternatieve criteria. Indien aan één daarvan is voldaan, kan de doorgifte aan dat land plaatsvinden, mits uiteraard ook overigens is voldaan aan alle criteria die reeds voor het verkeer binnen de Unie gelden.
Onderdeel a eist dat de toestemming betrekking heeft op de doorgifte naar het derde land. Artikel 1 onder h, vereist dat het moet gaan om een «vrije, specifieke en op informatie berustende wilsuiting». Dat betekent dat betrokkene op de hoogte moet zijn, zonodig op de hoogte moet worden gebracht, van het niveau van gegevensbescherming in het land waarnaar de gegevens zullen worden overgedragen, en zijn toestemming ondubbelzinnig op die overdracht betrekking moet hebben.
Onderdeel b opent de mogelijkheid dat bij de uitvoering of de voorbereiding van overeenkomsten ook doorgifte van persoonsgegevens plaatsvindt. Dit onderdeel heeft betrekking op de uitvoering van overeenkomsten waarbij de betrokkene partij is. Het kan bij voorbeeld nodig zijn dat voor de uitvoering van een overeenkomst een betaling plaatsvindt, welke betaling in het bancaire verkeer via een niet steeds te voorzien aantal landen verloopt. Het is dan niet nodig, zelfs niet altijd mogelijk om de betrokkene toestemming voor een dergelijke doorgifte te vragen. De betrokkene is dan degene die in het kader van een rekening-courantverhouding een betalingsopdracht doet, waarbij zijn gegevens worden doorgegeven.
Onderdeel c heeft betrekking op de uitvoering van een overeenkomst waarbij de betrokkene geen partij is, doch waarbij hij belang heeft. Zo kan bij herverzekering van een in Nederland gesloten verzekering het onder omstandigheden noodzakelijk zijn de persoonsgegevens van de verzekerde door te geven aan een land buiten de Unie in het kader van een overeenkomst tussen een Nederlandse verzekeraar en een herverzekeraar, gevestigd buiten de Unie. Een dergelijke herverzekering is mede in het belang van de betrokkene. Ook een bank die in een betalingsopdracht opgenomen persoonsgegevens doorgeeft van een ander dan degene die de opdracht gaf, kan dit doen indien die doorgifte plaatsvindt in het kader van een overeenkomst tussen de opdrachtgever en een derde voor zover die overeenkomst is gesloten in het belang van de betrokkene. Deze bepaling legt een bank geen actieve plicht op om de persoonsgegevens die onder verantwoordelijkheid van een opdrachtgever worden verwerkt, als bewerker te controleren op overeenstemming met deze bepaling. Mogelijke schade wegens niet-naleving van dit voorschrift komt blijkens artikel 49, vierde lid, slechts voor rekening van de bewerker voor zover hem deze kan worden toegerekend. Dit is slechts het geval indien zonder bijzondere controle het de bank als bewerker onmiskenbaar duidelijk is, dat doorgifte in strijd zou komen met deze bepalingen. Dit onderdeel kan geen basis vormen voor de doorgifte van persoonsgegevens met het oog op direct marketing. Een dergelijke doorgifte vindt immers niet plaats met het oog op het belang van de betrokkene, doch slechts in het belang van degene die de betrokkene met behulp van de persoonsgegevens benadert.
Onderdeel d omschrijft de gevallen waarin zonder dat het belang van de betrokkene daarmee is gediend, desondanks de overdracht van gegevens is aangewezen. Dan moet een zwaarwegend algemeen belang in het geding zijn. Ook is doorgifte toegestaan wanneer dat nodig is voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht. Dit omvat mede de doorgifte van persoonsgegevens aan bij voorbeeld een

incassobureau gevestigd buiten de Unie voorafgaand aan een mogelijke gerechtelijke procedure.
Onderdeel e maakt de doorgifte mogelijk van persoonsgegevens wanneer vitale belangen van de betrokkene in het geding zijn. Voor een uitleg van dit begrip verwijzen wij naar de toelichting op artikel 77, eerste lid, onder e.
Onderdeel f ziet op openbare registers. De richtlijn spreekt van registers die bedoeld zijn om het publiek voor te lichten. Een ieder kan het kadaster, het handelsregister e.d. ongeacht of hij binnen of buiten de Unie zich bevindt of is gevestigd. Hetzelfde geldt voor registers die in de Nederlandse wetgeving weliswaar niet als openbaar register bij wet is ingesteld, maar waaruit belanghebbenden, wanneer aan bepaalde voorwaarden is voldaan, persoonsgegevens kunnen verkrijgen. Een voorbeeld is de kentekenregistratie. Beiden varianten wordendoor de richtlijn gedekt.

Tweede lid

Deze bepaling bevat een noodklep indien de toegestane uitzonderingsgronden ontoereikend blijken. De Minister van Justitie kan in dat geval vergunning voor doorgifte verlenen. Aan de vergunning dienen nadere voorschriften te worden verbonden ter bescherming van de persoonlijke levenssfeer of de fundamentele rechten en vrijheden van personen.[1] Deze voorschriften kunnen betrekking hebben op contractuele bepalingen die de verantwoordelijke in een overeenkomst met degene aan wie de gegevens worden doorgegeven, opneemt.
Over de inhoud van een vergunning zal het advies van de Registratiekamer worden ingewonnen. De verplichting daartoe is opgenomen omdat bij de Registratiekamer op dit terrein veel expertise aanwezig is. De inbreng van de Kamer zal aldus een belangrijke bijdrage kunnen leveren aan de kwaliteit van de beslissing. Toekenning van de bevoegdheid aan de Registratiekamer zou evenwel te ver gaan. Gelet op het weinig gebonden karakter van de bevoegdheid om de vergunning te verlenen en de abstracte materiële normen waarna wordt getoetst, zou een overdracht van de bevoegdheid tot het afgeven van de vergunning aan de Registratiekamer als zelfstandig bestuursorgaan op gespannen voet komen met de daarop betrekking hebbende Aanwijzingen inzake zelfstandig bestuursorganen. Voorts kunnen in de relatie tot derde landen aspecten een rol spelen die primair tot de verantwoordelijkheid van de regering moeten worden gerekend. Om deze redenen komen de vergunning en de daarin opgenomen voorwaarden uiteindelijk voor de verantwoordelijkheid van de Minister.

Artikel 78

Artikel 25, derde lid, van de richtlijn verplicht Nederland als lid-staat van de Unie de Commissie op de hoogte te brengen van de gevallen waarin naar het oordeel van de regering een derde land geen passend niveau van bescherming biedt. De bepaling legt deze verplichting op aan de Minister van Justitie. Er is een overeenkomstige verplichting indien een vergunning wordt afgegeven als bedoeld in artikel 77, tweede lid. Dit is opgenomen in onderdeel b van het eerste lid. Naar aanleiding van deze melding kan de Commissie verzet aantekenen en maatregelen nemen overeenkomstig de procedure, beschreven in artikel 31, tweede lid, van de richtlijn (artikel 26, derde en vierde lid).
Artikel 25, vierde tot en met zesde lid, geven de Europese Commissie de bevoegdheid interpretatieve verklaringen met bindende kracht te doen omtrent het beschermingsniveau van derde landen, zowel in positieve als in negatieve zin. Hetzelfde kan ingevolge artikel 26, derde lid, van de richtlijn geschieden naar aanleiding van een melding van een door een van de lidstaten bedoelde toestemming als bedoeld in artikel 26, tweede

[1] Zie voor de betekenis van fundamentele rechten en vrijheden ook 4 van het Algemeen deel van de toelichting.

lid, van de richtlijn. Aldus zijn instrumenten gegeven om een geharmoniseerd beleid van de Unie tegenover derde landen te bewerkstelligen. Het tweede lid van artikel 78 biedt de mogelijkheid dergelijke verklaringen om te zetten in het nationale recht. Gaat het om verklaringen van algemene strekking dan vindt de omzetting plaats bij ministeriële regeling. In andere gevallen vindt de omzetting plaats middels bij beschikking. Titel 1.2 Awb ontheft de Minister van een aantal procedureverplichtingen wanneer het gaat om de uitvoering van bindende besluiten van organen van de Europese Gemeenschappen. Een spoedige omzetting is aldus gewaarborgd.
Daarnaast kan het ten behoeve van een juiste implemenatie in het Nederlandse recht nodig zijn om een eerder verleende vergunning als bedoeld in artikel 77, tweede lid, te herzien. Een verklaring van de Commissie kan aanleiding zijn om een dergelijke vergunning in te trekken of te wijzigen. In het tweede lid, onderdeel c, wordt hierin voorzien.

HOOFDSTUK 12 OVERGANGSBEPALINGEN

Artikel 79

eerste lid

Artikel 32 van de richtlijn schrijft voor dat bestaande gegevensverwerking binnen uiterlijk drie jaren in overeenstemming moeten zijn gebracht met de nationale bepalingen ter implementatie van de richtlijn. Daarbij had men in het bijzonder die lid-staten in het oog voor welke de nieuwe bepalingen een geheel nieuw regime tot gevolg zouden hebben.
In het wetsvoorstel is voor Nederland een onderscheid gemaakt tussen de verwerking van niet-gevoelige gegevens en die van de wel gevoelige gegevens. Met dat laatste wordt gedoeld op alle gegevens voor welke een bijzondere regeling geldt ingevolge paragraaf 2 van Hoofdstuk 2. Voor de niet-gevoelige gegevens verandert er slechts in mindere mate iets dan voor de overige.
Voor de niet-gevoelige gegevens geldt dat zowel voor de private als voor de publieke sector de normen in beginsel dezelfde uitwerking zullen hebben. Weliswaar gold onder de WPR voor persoonsregistraties in de private sector een zwakker regime dan voor de publieke sector. Voor de private sector gold dat een persoonsregistratie mocht worden aangelegd voor een doel waartoe het belang van de houder redelijkerwijs aanleiding gaf. Voor de publieke sector gold het noodzakelijkheidsvereiste. In de praktijk is dit verschil niet tot wasdom gekomen en werden feitelijk dezelfde eisen gesteld. In haar advisering heeft de Registratiekamer al enige tijd geanticipeerd op de richtlijn. Voor private registraties zal er daarom van kunnen worden uitgegaan dat wanneer een registratie toelaatbaar was onder de WPR, dit ook het geval is onder de WBP. Tegen deze achtergrond is het verantwoord hier te kiezen voor een kortere overgangstermijn, nl. een half jaar. Uiteraard geldt deze termijn slechts voor verwerkingen die voorafgaande aan de inwerkingtreding hebben plaatsgevonden. Gegevensverwerking van na dat tijdstip dienen per onmiddellijke ingang aan de eisen van de wet te voldoen. De werklast ligt in de gegevensverwerking die niet onder het bereik van de WPR vielen, doch wel onder dat van de WBP. Via de vrijstellingsregeling zal echter worden getracht zoveel mogelijk alle standaardverwerkingen van de melding vrij te stellen. Met betrekking tot de meldingsverplichting, bedoeld in artikel 27, is de mogelijk geschapen bij algemene maatregel van bestuur de termijn van een half jaar te verlengen tot drie jaren. Daarmee kan rekening worden gehouden met de behoefte in de praktijk een zekere overgangsfase te hebben ten einde de bestaande

aanmeldingsformulieren en reglementen te kunnen aanpassen aan de nieuwe wetgeving alsmede met de werklast van de Registratiekamer in deze.

tweede lid

Voor de gevoelige gegevens geldt daarentegen ook voor de inhoudelijke normering een strikter regime dan onder de WPR. Het ligt daarom in de rede daarvoor de volle termijn die de richtlijn toelaat ook te benutten. Aldus wordt ook enige fasering in de aanpassing bewerkstelligd. De langere termijn geldt uitsluitend voor de benodigde aanpassing aan paragraaf 2 van hoofdstuk 2, waarin het striktere regime is opgenomen. Voor de aanpassing van de verwerking van bijzondere gegevens aan de overige bepalingen van het wetsvoorstel geldt gewoon de termijn van het eerste lid.
Wat betreft de gevoelige gegevens kan de vraag worden gesteld of een toestemming die gegeven is voor een gegevensverwerking voorafgaand aan de datum van inwerkingtreding, moet worden hernieuwd, of dat de indertijd gegeven toestemming, wanneer deze voldoet aan de vereisten, bedoeld in artikel 1, onderdeel i, en dus vrij, specifiek en op afdoende informatie berust, onder de nieuwe regeling gelding behoudt. Gelet op overweging 70 van de richtlijn, moet het laatste worden aangenomen. Deze overweging bepaalt expliciet dat verwerkingen die noodzakelijk zijn voor de uitvoering van op het moment van het van kracht worden van de implementatiewetgeving bestaande overeenkomsten die op basis van vrije en geïnformeerde toestemming zijn gesloten, vrijgesteld zijn van het vereiste van uitdrukkelijke toestemming voor het verwerken van gevoelige gegevens (De Engelse tekst spreekt van «whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process....»). Zo blijft het mogelijk voor de verantwoordelijke gevoelige gegevens te verwerken indien dit nodig is voor de uitvoering van een overeenkomst, bijvoorbeeld een levensverzekerings-overeenkomst, die op basis van vrije en geïnformeerde toestemming is gesloten vóór de inwerkingtreding van dit wetsvoorstel.

Artikel 80

Gelet op de snelle informatietechnologische ontwikkelingen is het dienstig een evaluatiebepaling in het wetsvoorstel op te nemen. Bezien zal moeten worden of bepalingen wellicht knelpunten opleveren, dan wel de bescherming van de persoonlijke levenssfeer ontoereikend garanderen.

De Minister van Justitie,
W. Sorgdrager

De Staatssecretaris van Binnenlandse Zaken,
J. Kohnstamm

BIJLAGE

Transponeringstabel

Artikel WBP	Artikel richtlijn
artikel 1	
onderdeel a	artikel 2 sub a
onderdeel b	artikel 2 sub b
onderdeel c	artikel 2 sub c
onderdeel d	artikel 2 sub d
onderdeel e	artikel 2 sub e
onderdeel f	artikel 2 sub f
onderdeel g	artikel 2 sub g
onderdeel h	artikel 2 sub h
onderdeel i	
artikel 2	
lid 1	artikel 3 lid 1
lid 2	artikel 3 lid 2
artikel 3	
lid 1	artikel 9
lid 2	artikel 8 lid 4
artikel 4	artikel 4
artikel 5	
artikel 6	artikel 6 lid 1 sub a
artikel 7	artikel 6 lid 1 sub b
artikel 8	artikel 7
artikel 9	
lid 1	artikel 6 lid 1 sub b
lid 2	
lid 3	artikel 6 lid 1 sub b
artikel 9a	
artikel 10	artikel 6 lid 1 sub e
artikel 11	
lid 1	artikel 6 lid 1 sub c
lid 2	artikel 6 lid 1 sub d
artikel 12	artikel 16
artikel 13	artikel 17 lid 1
artikel 14	
lid 1	artikel 17 lid 2
lid 2	artikel 17 lid 3
lid 3	artikel 17 lid 4
artikel 15	artikel 6 lid 2
artikel 16	artikel 8 lid 1
artikel 17	artikel 8 lid 2 sub d
artikel 18	artikel 8 lid 4
artikel 19	
lid 1 sub b	artikel 8 lid 2 sub d
lid 1 sub b	artikel 8 lid 4
artikel 20	artikel 8 lid 2 sub d
artikel 21	artikel 8 leden 3 en 4
artikel 22	artikel 8 lid 5

Artikel WBP	Artikel richtlijn
artikel 23	
lid 1 sub a	artikel 8 lid 2 sub a
lid 1 sub b	artikel 8 lid 2 sub e
lid 1 sub c	artikel 8 lid 2 sub e
lid 1 sub d	artikel 8 lid 4
lid 1 sub e	artikel 8 lid 4
lid 2	artikel 8 lid 4
artikel 24	artikel 8 lid 7
artikel 25	artikel 27 lid 2
artikel 26	
artikel 27	
lid 1	artikel 18 lid 1
lid 2	artikel 18 lid 5
lid 3	artikel 18 lid 1
artikel 28	
leden 1 en 2	artikel 19 lid 1
lid 3	artikel 19 lid 2
leden 4 en 5	
artikel 29	
leden 1 en 2	artikel 18 lid 2
lid 3	artikelen 18 lid 3 en 1
lid 4	sub g
artikel 30	
lid 1	artikel 21 lid 2
lid 2	artikel 21 lid 1
lid 3	artikel 21 lid 3
lid 4 sub a	artikel 13
lid 4 sub b	artikel 21 lid 3
artikel 31	artikel 20 leden 1 en 2
artikel 32	artikel 20 lid 2
artikel 33	artikel 10
artikel 34	artikel 11
artikel 35	artikel 12 lid 1
artikel 36	artikel 12 lid 2
artikel 37	
artikel 38	artikel 12 lid 3
artikel 39	
artikel 40	artikel 14 sub a
artikel 41	artikel 14 sub b
artikel 42	artikel 15
artikel 43	artikel 13 lid 1
artikel 44	artikel 13 lid 2
artikelen 45 t/m 48	artikel 22
artikelen 49 en 50	artikelen 23 en 24
artikel 51	
lid 1	artikel 28 lid 1

Artikel WBP	Artikel richtlijn
lid 2	artikel 28 lid 2
artikel 52	artikel 28 lid 1
artikel 53 t/m 57	
artikel 58	artikel 28 lid 5
artikel 59	
artikel 60	artikel 28 lid 4
artikel 61	artikel 28 lid 3
artikel 62 t/m 64	artikel 18 lid 2, tweede gedachtenstreepje
artikel 65	artikel 28 lid 3
artikelen 66 t/m 75	artikel 24
artikel 76	artikel 25 leden 1 en 2
artikel 77	artikel 26 lid 1
artikel 78	artikel 25 leden 3 t/m 6
artikel 79	artikel 32

* De meegezonden adviezen zijn ter inzage gelegd bij de afdeling Parlementaire Documentatie.