

# Nader onderzocht: het voorafgaand onderzoek door het CBP

4

## Trefwoorden:

voorafgaand onderzoek, samenwerkingsverbanden, Wet toezicht accountantsorganisaties (Wta), Besluit toezicht accountantsorganisaties (Bta), art. 31 WBP

**Art. 31 Wet bescherming persoonsgegevens somt een drietal gronden op voor een zogenaamd 'voorafgaand onderzoek' door het College bescherming persoonsgegevens. Onder andere de telecommunicatiesector, samenwerkingsverbanden en accountantsorganisaties zien zich geconfronteerd met deze onderzoeksbevoegdheid van de toezichthouder. De gronden voor het voorafgaand onderzoek zijn echter zeer algemeen geformuleerd. Dit werpt in de dagelijkse praktijk belemmeringen op voor de toezichthouder en zorgt ook voor onzekerheid bij verantwoordelijken. De Minister van Justitie bestudeert inmiddels de mogelijkheden voor het wegnemen van de belemmeringen.**

## 1 Inleiding

In de Wet bescherming persoonsgegevens (WBP) is vastgelegd dat er toezicht op verwerkingen van persoonsgegevens wordt gehouden door het College bescherming persoonsgegevens (CBP). Ten behoeve van de uitoefening van dit toezicht is een aantal onderzoeksbevoegdheden aan het CBP toegekend. Eén van die onderzoeksbevoegdheden is gebaseerd op art. 31 WBP en betreft het zogeheten 'voorafgaand onderzoek' (VO).

Het VO kan verstrekken gevolgen hebben voor organisaties die persoonsgegevens willen verwerken. Zo mogen bepaalde verwerkingen pas plaatsvinden nádat het CBP heeft besloten dat de voorgenomen verwerking van persoonsgegevens rechtmatig is. In dit artikel wordt nader stilgestaan bij het VO ten aanzien van drie soorten van gegevensverwerkingen: verwerkingen in de telecommunicatiesector, verwerkingen in samenwerkingsverbanden en verwerkingen in de accountancy. Beschreven zal worden wat een VO is, wat dit betekent voor de drie sectoren en waarom niet alleen het CBP van mening is dat de toepassing van het VO dient te veranderen.

## 2 Art. 31 WBP

### 2.1 Wet(s)geschiedenis

Met de inwerkingtreding van de WBP per 1 september 2001 is aan de toezichthouder, het CBP, de bevoegdheid toegekend tot het instellen van een VO.

Art. 31 WBP is gebaseerd op art. 20 van Richtlijn nr. 95/46/EG. De wetsgeschiedenis bij art. 31 WBP vermeldt hierover:

Volgens art. 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.<sup>2</sup>

Het VO is onderdeel van de melding van verwerkingen van persoonsgegevens bij het CBP.<sup>3</sup> De meldingsplicht geldt voor alle geautomatiseerde verwerkingen van persoonsgegevens, tenzij er sprake is van een vrijstelling op grond van het Vrijstellingsbesluit.<sup>4</sup> In de melding moet worden aangegeven of deze (gedeeltelijk) betrekking heeft op een verwerking waarvoor een VO nodig is.

Het niet nakomen van de meldingsplicht kan leiden tot het opleggen van een boete door het CBP of het doen van aangifte door het CPB.<sup>5</sup> Het CPB stelt alleen een VO in als verantwoordelijken<sup>6</sup> daar zelf om vragen in de melding. Men zou hierdoor in de verleiding kunnen komen om in VO-situaties geen aanvraag te doen, maar het CPB neemt elke melding handmatig door. Een discrepantie tussen het wel aanwezig zijn van een VO-plichtige verwerking en het niet aanvragen van een VO, zal in de meeste gevallen direct opvallen. Het CPB zal de melding 'onaanmemelijk' verklaren zolang niet ook om een VO is verzocht. Aan deze werkwijze wordt strikt de hand gehouden. Ook bij gegronde twijfel over de aanwezigheid van een VO-plicht of een noodzaak tot het aanvragen van een VO, dient naar de mening van het CPB een VO te worden aangevraagd.

De tekst van art. 31 WBP luidt:

- 1 Het College stelt voorafgaand aan een verwerking een onderzoek in indien de verantwoordelijke:
  - a. een nummer ter identificatie van personen voornemens is te verwerken voor een ander doeleinde dan

1 Jean Paul van Schoonhoven is als adviseur Bestuur, ICT en Recht werkzaam bij Duthler Associates in Den Haag. Daarvoor werkte hij als beleidsmedewerker bij het College bescherming persoonsgegevens.

2 Kamerstukken II 1997/98, 25 892, nr. 3 (MvT), p. 17 en p. 144-147.

3 Art. 27 WBP.

4 Besluit van 7 mei 2001, *Stb.* 250. Laatstelijk gewijzigd bij Besluit van 16 juni 2004, *Stb.* 261.

5 Art. 75 lid 1 WBP.

6 Art. 1 sub d WBP: 'verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.'

- waarvoor het nummer specifiek bestemd is teneinde gegevens in verband te kunnen brengen met gegevens die worden verwerkt door een andere verantwoordelijke, tenzij het gebruik van het nummer geschiedt voor de gevallen als omschreven in art. 24;
- b. voornemens is gegevens vast te leggen op grond van eigen waarneming zonder de betrokkene daarvan op de hoogte te stellen, of
  - c. anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus voornemens is strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag te verwerken ten behoeve van derden.
2. Het eerste lid, onder b, is niet van toepassing op openbare registers die bij de wet zijn ingesteld.
  3. Bij wet of algemene maatregel van bestuur kunnen andere gegevensverwerkingen die een bijzonder risico inhouden voor de persoonlijke rechten en vrijheden van de betrokkene worden aangewezen waarop het eerste lid van toepassing is. Het College geeft in zijn jaarverslag aan in hoeverre naar zijn oordeel een dergelijke aanwijzing wenselijk is.
  4. Het College meldt een verwerking als bedoeld in het eerste lid, onder c, bij de Europese Commissie.

Volgens de wetsgeschiedenis heeft het VO in beginsel alleen betrekking op een geheel van verwerkingen en niet op een individuele beslissing om een gegeven te verwerken in de zin dat het zal worden verstrekt aan een ontvanger.<sup>7</sup> De toets door het CPB betreft een rechtmatigheidstoets. Het VO leidt tot een *niet-bindende* verklaring over de rechtmatigheid van de verwerking door het CPB, maar ontslaat de verantwoordelijke dus niet van de verplichting om zijn eigen afweging te maken. De verklaring van het CPB zal echter in de afweging door de verantwoordelijke een belangrijke rol spelen. Omdat het belang van de verklaring van het CPB voor de verantwoordelijke groot kan zijn, is het mogelijk rechtstreeks beroep bij de bestuursrechter tegen het oordeel van het CPB in te stellen.

Bepaalde lidstaten van de Europese Unie kenden voor de inwerkingtreding van de WBP al een systeem van voorafgaande toetsing in de vorm van een vergunningverlening. Dit systeem werd ook in Nederland geïntroduceerd en wel 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 persoonsregistraties, de voorloper van de WBP. Dit voorstel is later uit dereguleringsoogpunt ingetrokken.<sup>8</sup>

Met aan een VO onderworpen verwerking mag niet worden begonnen voordat het CPB uitspraak heeft gedaan over de rechtmatigheid van de verwerking. Het CPB kan drie soorten uitspraken doen:

- de verwerking is onrechtmatig;
- de verwerking is rechtmatig mits met een aantal voorwaarden rekening wordt gehouden en
- de verwerking is rechtmatig.

Op 1 juli 2005 is de uniforme openbare voorbereidingsprocedure van de Algemene wet bestuursrecht (Awb) gewijzigd. Daar waar voorheen een VO maximaal 17 weken kon duren, zijn er nu 6 weken (plus een extra behandelweek) bijgekomen. Niet langer hoeft het CPB bij de start van een VO, mededeling hiervan te doen in de Staatscourant. Deze mededelingsplicht is verschoven naar het moment waarop het CPB een conceptbesluit heeft geformuleerd. Dat conceptbesluit moet thans gepubliceerd worden in de Staatscourant op grond van art. 3:11 lid 1 Awb. Vervolgens kan een belanghebbende hiertegen binnen 6 weken rechtstreeks beroep instellen bij de rechtbank op grond van art. 7:1 lid 1, onder d jo. 8:1 lid 1 Awb.

Na verloop van tijd zal het CPB bij de verantwoordelijke informeren welke maatregelen inmiddels zijn getroffen naar aanleiding van een weigering van een verklaring van rechtmatigheid of naar aanleiding van de gestelde voorwaarden bij een verklaring van rechtmatigheid. Na deze informatieronde volgt eventueel een ambtshalve onderzoek en zonodig kan het CPB besluiten tot toepassing van bestuursdwang of het opleggen van een last onder dwangsom.

## 2.2 Rol CPB

Het CPB heeft in september 2001 een informatieblad uitgegeven waarin het aan verantwoordelijken informatie verschaft over het VO en tevens antwoord geeft op een aantal van de belangrijkste en meest gestelde vragen.<sup>9</sup> Dit is nagenoeg alle algemene informatie die het CPB naar buiten heeft gebracht rondom het VO. Dat is niet veel. Zeker niet als je de tekst van art. 31 leest. De onderzoeksgronden zijn bepaald algemeen geformuleerd en niet direct te doorgronden. Daarnaast heeft het CPB ook geen beleidsregels gepubliceerd. Het VO ontbeert hierdoor voor veel verantwoordelijken in de praktijk, heldere en kenbare criteria over de uitoefening van het onderzoek door het CPB. Voor verantwoordelijken is het daarom van belang om naast de wetsgeschiedenis, rechtsontwikkelingen bij te houden aan de hand van gepubliceerde uitspraken van het CPB.

Belangrijk om niet onvermeld te laten is dat ondanks de 'harde' formulering in de WBP, de bevoegdheid van het CPB om een VO in te stellen een discretionaire bevoegdheid is volgens de wetsgeschiedenis. Het CPB is dus niet verplicht onderzoek te doen in de situaties genoemd in art. 31 WBP.<sup>10</sup>

## 2.3 Rol functionaris voor de gegevensbescherming

Verantwoordelijken kunnen een eigen interne 'toezichthouder' benoemen. Dit is de zogenaamde functionaris voor de

7 Zie de toelichting op art. 1, onderdeel b, en art. 27 lid 1 in *Kamerstukken II 1997/98, 25 892, nr. 3.*

8 *Kamerstukken II 1981/82, 17 207, nr. 1-2.*

9 Informatieblad 'Voorafgaand onderzoek' nummer 15, september 2001 <[www.Cbpweb.nl](http://www.Cbpweb.nl)>.

10 *Kamerstukken II 1997/98, 25 892, nr. 3, p. 144-145.*

gegevensbescherming (FG).<sup>11</sup> Bepaalde verwerkingen van persoonsgegevens die anders op grond van art. 27 WBP bij het CPB gemeld moeten worden, kunnen dan gemeld worden bij de FG. De FG is echter niet bevoegd een VO in te stellen, die bevoegdheid is aan het CBP voorbehouden.<sup>12</sup>

### 3 Het VO in de praktijk

#### 3.1 Consultatie in de telecommunicatiesector

Verwerkingen van verantwoordelijken in de telecommunicatiesector (zoals internet service providers, internet access providers, telefoonproviders) kunnen in bepaalde gevallen onderworpen zijn aan een VO. Om welke gevallen het gaat, is niet altijd zonder meer duidelijk. Zoals al eerder opgemerkt, de grondslagen voor een VO zijn algemeen geformuleerd en niet eenvoudig te doorgronden. In een VO bleek het CPB dat een 'niet nader te noemen telecommunicatieaanbieder' onvoldoende uitwerking had gegeven aan de WPB en diens tengevolge onrechtmatig persoonsgegevens verwerkte.<sup>13</sup> Op grond van deze opgedane ervaringen is het CPB in juni 2003 een consultatie in de telecommunicatiesector gestart. Door de sector te consulteren alvorens het consultatiedocument als beleidskader te aanvaarden, beoogde het CPB meer houvast te bieden voor partijen in de telecommunicatiesector die mogelijk met voorafgaande onderzoeken te maken hebben.<sup>14</sup> Tegelijkertijd diende deze consultatie nog twee andere doelen. De eerste is dat het CPB meer informatie krijgt over verwerkingen van persoonsgegevens in deze sector. Daarnaast is het CPB daardoor in staat een duidelijker en kenbaarder normenkader te scheppen, waardoor het CPB te zijner tijd eenvoudiger handhavende onderzoeken in de telecommunicatiesector kan uitvoeren.

Een voordeel van de consultatie is dat de telecommunicatiesector iets meer duidelijkheid heeft over de uitoefening van de onderzoeksbevoegdheid door het CPB. In het consultatiedocument heeft het CPB ten aanzien van twee van de drie onderzoeksgronden een gedragslijn geformuleerd. Deze gedragslijn heeft betrekking op heimelijke waarnemingen in de zin van art. 31 lid 1, onder b WBP, en op de verwerkingen van strafrechtelijke persoonsgegevens ten behoeve van derden in de zin van art. 31 lid 1, onder c WBP.

De gedragslijnen zijn:<sup>15</sup>

#### 'Gedragslijn voor heimelijke waarnemingen

Voor heimelijke waarnemingen geldt dat de betrokken abonnees en/of gebruikers vóór af dienen te worden geïnformeerd over de mogelijke toepassing van de waarnemingsmethode, via daarvoor geëigende communicatiekanalen. Daarnaast moet zo veel mogelijk worden voorzien in de mogelijkheid om achteraf kennis te nemen van de uit de heimelijke waarneming verkregen gegevens.

Voor sommige vormen van heimelijke waarnemingen zijn daarnaast nog de volgende gedragslijnen van toepassing:

#### Gespreksopnames

- Het opnemen van gesprekken of het bewaren van elektronische berichten dient in elk geval beperkt te zijn tot gesprekken die afkomstig zijn van, dan wel bestemd zijn voor het eigen bedrijf.
- Het opnemen van gesprekken voor training van het personeel behoeft de instemming van de ondernemingsraad, terwijl het personeel over het gebruik van deze waarnemingsmethode dient te zijn geïnformeerd.<sup>16</sup>
- Over het opnemen van gesprekken of het bewaren van elektronische berichten voor klachtafhandeling en bewijsvoering dienen de klanten vooraf te worden geïnformeerd. Het opnemen van *alle* gesprekken voor incidenteel gebruik in de klantrelatie wordt doorgaans disproportioneel geacht.

#### Bewaren van gegevens over het telecommunicatieverkeer (verkeersgegevens)

- Verkeersgegevens dienen bij het beëindigen van oproepen te worden verwijderd of geanonimiseerd, afgezien van het bepaalde in art. 13.4 Telecommunicatiewet. De verkeersgegevens die noodzakelijk zijn voor rekeningdoeleinden mogen wel worden bewaard. Er dient dan wel een redelijke termijn te worden bepaald voor de periode waarin de rekening kan worden betwist door de klant. Bij niet betwiste rekeningen dienen de achterliggende verkeersgegevens na afloop van de gestelde termijn alsnog te worden gewist. Bij wel betwiste rekeningen kunnen ze langer worden bewaard (uiterlijk tot de wettelijke verjaringstermijn).
- Verkeersgegevens mogen worden verwerkt voor de marketing van eigen telecommunicatiediensten, indien de abonnee daarmee heeft ingestemd. De abonnee dient een reële mogelijkheid te worden geboden zich over het specifieke gebruik van verkeersgegevens voor marketingdoeleinden met inbegrip van de beëindiging daarvan uit te spreken.

#### Gedragsregels voor het verwerken van strafrechtelijke persoonsgegevens ten behoeve van derden

Voor het verwerken van strafrechtelijke gegevens ten behoeve van derden dient een procedure te zijn vastgesteld die voorziet in passende en specifieke waarborgen. Voor zover de te verwerken gegevens (tevens) betrekking kunnen hebben op het eigen personeel dient de ondernemingsraad met de daarvoor geldende procedure te hebben ingestemd, een en ander in overeenstemming met het bepaalde in art. 22 lid 3 WBP.

11 Art. 62-64 WBP.

12 Kamerstukken II 1997/98, 25 892, nr. 3, p. 145.

13 CPB 3 juli 2002, z2002-0597 en CPB z2001-1395.

14 Consultatiedocument 'Uitgangspunten voorafgaand onderzoek in

de telecommunicatiesector', versie 1.0 juni 2003 <www.Cbpweb.nl>.

15 Zie 'Uitgangspunten voorafgaand onderzoek in de telecommunicatiesector', versie 1.0 juni 2003, p. 8-10.

16 Art. 27 lid 1, onder k WOR.

**Internetmisbruik en plaaggevallen**

Aannemelijk moet worden gemaakt dat de verwerking van gegevens naar aanleiding van een opgelegd verbod voor een bepaalde vorm van internetmisbruik of telefoonhinder voldoende zorgvuldig geschiedt, bijvoorbeeld blijkend uit een daarvoor vastgestelde procedure en de daarover beschikbare informatie voor de klant. Als de verwerking ook het eigen personeel betreft, dient ook de ondernemingsraad met die procedure te hebben ingestemd.

**Slotsom**

De verplichting voor de telecommunicatiesector tot het aanvragen van een voorafgaand onderzoek bij het CPB doet zich voor:

- in situaties van heimelijke waarneming, ofwel bij gegevensverwerkingen die voor de betrokkene onopgemerkt blijven en ook moeten blijven;
- bij uitwisseling van strafrechtelijke gegevens met derden;
- bij optreden tegen internetgebruik volgend op een daarvoor door de rechter opgelegd verbod.

Het meewerken aan de opsporing van strafbare feiten door politie en justitie valt doorgaans niet onder de plicht tot het aanvragen van een voorafgaand onderzoek.'

Voor zover bekend heeft de consultatie nog niet tot een definitief einddocument geleid. De door het CPB geschetste gedragslijnen zijn dus nog vatbaar voor 'voortschrijdende inzichten.'

**3.2 OPTA**

De Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) is toezichthouder in de telecommunicatiesector. In die hoedanigheid kan de OPTA in sommige gevallen en bij de uitoefening van haar wettelijke taken, persoonsgegevens verwerken.

Op 18 april 2005 heeft de OPTA melding gedaan bij het CPB van een verwerking van persoonsgegevens met de naam 'spamtoezicht'. In deze melding heeft de OPTA het CPB op twee gronden verzocht om een VO. De eerste grond is dat de OPTA voornemens zou zijn gegevens vast te leggen zonder de betrokkenen daarvan op de hoogte te stellen. De tweede grond is dat de OPTA voornemens zou zijn om voor derden strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag te verwerken.

Het CPB kwam in het VO uiteindelijk tot de conclusie dat de gemelde verwerking 'spamtoezicht' niet onderworpen was aan een VO. De OPTA verzamelt persoonsgegevens die niet door eigen waarneming zijn verkregen. De OPTA verzamelt deze gegevens via <www.spamklacht.nl>, welke persoonsgegevens daar door derden zijn gemeld. In deze gevallen is de verantwoordelijke, de OPTA, op grond van art. 34 WBP ver-

plicht de betrokkene te informeren over zijn identiteit en de doeleinden van verwerking. Als dit laatste niet mogelijk blijkt, bijvoorbeeld omdat dit onmogelijk blijkt of onevenredige inspanning kost, is de OPTA verplicht de herkomst van de gegevens vast te leggen. Dit biedt volgens de wetgever voor deze gevallen voldoende compenserende waarborg voor het feit dat de betrokkene niet op de hoogte wordt gesteld.

Verder bleek dat de OPTA strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag alleen verwerkt ten behoeve van de uitvoering van de aan haar wettelijk opgedragen taken en het toegekende wettelijk instrumentarium. De uitvoering van haar wettelijke taken zou er onder omstandigheden toe kunnen leiden dat deze bijzondere persoonsgegevens aan derden kunnen worden verstrekt, maar dat zou slechts in incidentele en niet voorzienbare gevallen aan de orde kunnen komen. Zoals ik in paragraaf 2.1 opmerkte, ziet het VO alleen op gevallen waarin sprake is van een 'geheel van verwerkingen' en niet op elke 'individuele beslissing'.<sup>17</sup> Ook dit had tot gevolg dat geen VO noodzakelijk was.

**3.3 Stichting Brein**

Stichting Brein (Brein) is een particuliere stichting die zowel in als buiten rechte optreedt tegen onrechtmatige exploitatie van mediadragers en de daarop vervatte informatie.

Op 22 december 2003 heeft Brein melding gedaan bij het CPB van de verwerking van persoonsgegevens in het kader van het 'antipiraterij databestand'. In deze melding heeft Brein het CPB op twee gronden verzocht om een VO. Brein was voornemens gegevens vast te leggen zonder de betrokkenen daarvan op de hoogte te stellen én Brein was voornemens om voor derden strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag te verwerken.

Het CPB oordeelde dat de gemelde verwerking door Brein rechtmatig was, mits met een aantal voorwaarden rekening werd gehouden zoals het naleven van de informatieplicht en het waarborgen van de rechten van betrokkenen.<sup>18</sup>

De uitspraak van het CPB is naderhand aangehaald in een voorlopige voorzieningprocedure bij de Rechtbank Utrecht. Brein vorderde afgifte van persoonsgegevens bij een aantal internet service providers en internet access providers. Deze weigerden dat, mede door te stellen dat Brein in strijd handelde met de door het CPB afgegeven verklaring van rechtmatigheid. De rechter oordeelde dat hier inderdaad sprake van was en oordeelde dat persoonsgegevens niet aan Brein mochten worden afgestaan.<sup>19</sup> Het oordeel van de voorzieningenrechter heeft het CPB overigens nog geen aanleiding gegeven de aan Brein afgegeven verklaring van rechtmatigheid te herzien.

**3.4 Samenwerkingsverbanden**

Samenwerkingsverbanden tussen organisaties in de publieke sector en/of private sector komen veelvuldig voor. Vaak is deze samenwerking noodzakelijk om maatschappelijke pro-

<sup>17</sup> CPB 20 juni 2005, z2005-0409.

<sup>18</sup> CPB 16 april 2004, z2003-1660.

<sup>19</sup> Pres. Rb. Utrecht, 12 juli 2005, LjN AT9073 <www.rechtspraak.nl>.

blemen aan te pakken. Hierbij worden persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Bijzondere persoonsgegevens kunnen bijvoorbeeld strafrechtelijke gegevens zijn of gegevens over iemands gezondheid.

Bij het aanpakken van maatschappelijke problemen wordt er vaak nauw samengewerkt tussen instanties zoals de GGD, de thuiszorg, maatschappelijk werk, GGZ, gemeenten, politie, woningbouwcorporaties en energieleveranciers. Doel daarvan is bepaalde basisbehoeften of hulp- en zorgverlening binnen het bereik van mensen te brengen (bemoeizorg).<sup>20</sup> Ook wordt er vaak nauw samengewerkt tussen organisaties in het kader van een bestuursrechtelijke aanpak van bepaalde vormen van overlast. Bij dit laatste valt te denken aan criminaliteitsbestrijding in een bepaalde regio in brede zin, maar ook aan het doelgericht aanpakken van illegale hennepcult.

Het delen van informatie binnen dergelijke samenwerkingsverbanden valt meestal onder art. 31 WBP. Veelal is dit omdat strafrechtelijke gegevens ten behoeve van derden worden verwerkt, hetgeen één van de drie grondslagen is voor een VO (denk aan een verslag van het politieverhoor die door de politie aan een burgemeester mag worden verstrekt<sup>21</sup> of feitenrapportages ontmantelbedrijven).

Het doorlopen van een procedure van het VO is wettelijk noodzakelijk, maar kan een vertragende werking hebben op het voortvarend kunnen oppakken van werkzaamheden door het samenwerkingsverband. Wettelijk gezien mag er namelijk pas bepaalde informatie gedeeld worden als het CPB heeft verklaard dat deze verstrekking rechtmatig is. Een VO door het CPB kan echter gelet op de eerder vermelde wettelijke termijnen, 24(!) weken duren.<sup>22</sup>

Ondanks deze vertragende werking is er een groot pluspunt. Verwerkingen die binnen een samenwerkingsverband (kunnen) plaatsvinden, zullen veelal een bijzonder risico voor de persoonlijke levenssfeer van de betrokkene inhouden. Een betrokkene zal bijvoorbeeld niet altijd zelf om hulp bij een organisatie aankloppen, maar zal (ongevraagd, maar misschien wel gewenst) door de organisatie worden opgezocht. Het pluspunt is dat samenwerkingsverbanden als het ware 'gedwongen' worden zich te bezinnen op hun omgang met persoonsgegevens. Wie doet wat, wanneer, waarmee en naar wie, zijn vragen die antwoord vergen. Ook zal er aandacht besteed moeten worden aan de vaak aanwezige wettelijke geheimhoudingsplicht die aan bepaalde hulpverleners of ambtenaren is opgelegd. Wat mogen zij wel, onder welke voorwaarden, maar ook: wat mogen zij niet met persoonsgegevens doen.

Samenwerkingsverbanden hebben een maatschappelijke functie en dienen een maatschappelijk nut. Tegen deze ach-

tergrond zal de bereidheid om in overeenstemming met wet- en regelgeving te werken vaak aanwezig zijn. Immers, veel van de samenwerkingspartners zijn zelf (onderdeel van de) 'overheid' en dienen het vertrouwen van de burger te hebben.<sup>23</sup> Deze bereidheid om 'goed te doen' betekent ook dat er aandacht wordt geschonken aan wetten waarin normen staan voor de omgang met persoonsgegevens. Voorbeelden zijn de WBP, maar ook de Wet politieregisters, de Wet gemeentelijke basisadministratie persoonsgegevens, de Wet werk en bijstand, de Wet structuur uitvoeringsorganisatie werk en inkomen, de Wet justitiële en strafvorderlijke gegevens, de Wet geneeskundige behandelovereenkomst.

Samenwerkingsverbanden die zich adequaat rekenschap geven van het toepasselijke wettelijk kader, zouden een eventueel VO door het CPB met vertrouwen tegemoet moeten kunnen zien. De mogelijk lange doorlooptijd van het VO kan echter een knelpunt opleveren. Een oplossing voor dit knelpunt kan zijn om een beroep te doen op de discretionaire onderzoeksbevoegdheid van het CPB. Indien verwerkingen van persoonsgegevens inzichtelijk zijn gemaakt (welke gegevens gaan waar naartoe), er een privacyreglement is, een convenant van samenwerking en er niet meer dan noodzakelijk persoonsgegevens worden verwerkt,<sup>24</sup> dan zou dit als het ware tot de aannahme moeten leiden dat het 'bijzondere risico voor de persoonlijke levenssfeer' niet langer aanwezig is.<sup>25</sup> Mijns inziens zou het CPB met een dergelijke overweging gerechtvaardigd kunnen afzien van het instellen van een VO. Dit zou ook recht doen aan het nemen van de eigen verantwoordelijkheid van de verantwoordelijke, een van de niet onbelangrijke uitgangspunten van de WBP.

Naar mijn mening kan ditzelfde argument ook aangewend worden om in het geheel geen VO meer te hoeven aanvragen. Immers, wat zou vanuit het oogpunt van de verantwoordelijke in een dergelijke situatie de toegevoegde waarde voor hem zijn om een onderzoek met opschortende werking te moeten ondergaan, terwijl een verklaring van rechtmatigheid van het CPB onverbindend is?

Als het CPB geen VO instelt, dan zal geen verklaring van rechtmatigheid aan het samenwerkingsverband worden afgegeven. Het is aan het samenwerkingsverband om te overwegen of men op het verkrijgen van deze verklaring inzet. Zonder verklaring van het CPB kunnen de gegevensverwerkingen evenwel nog steeds rechtmatig zijn. Zoals zojuist en in paragraaf 2.1 is opgemerkt, ontslaat het al dan niet instellen van een VO de verantwoordelijke niet van de verplichting om zijn eigen afweging te maken.

Een voorbeeld waarin het CPB op grond van zijn discretionaire bevoegdheid besloot om niet op een VO aan te sturen

20 Informatieblad 'Informatie delen in samenwerkingsverbanden', nr. 31A, januari 2005 <www.Cbpweb.nl>.

21 Art. 15 lid 1, onder b, jo. 30 Wet politieregisters.

22 Art. 32 lid 3 en 4 WBP tezamen.

23 Zie over vertrouwen ook CPB 1 maart 2006, z2005-0139.

24 Zie ook CPB 17 juni 2004, z2004-0253 en CPB 4 oktober 2004, z2004-0583.

25 Zie bijvoorbeeld ook CPB 14 juli 2005, z2005-0074.

betrof het zogenaamde 'Alijda project' van de gemeente Rotterdam. Het CPB vond dat er een redelijk belang voor het project aanwezig was, de procedures en reglementen er 'goed' uitzagen en er binnen het project zorgvuldig leek te worden gewerkt.<sup>26</sup>

#### 4 Wet en Besluit toezicht accountantsorganisaties

Art. 31 WBP loopt samen met art. 32 Besluit toezicht accountantsorganisaties (Bta). Het Bta<sup>27</sup> is een uitwerking van art. 21 lid 2, onder *b* van de Wet toezicht accountantsorganisaties (Wta). Zowel de Wta als het Bta zijn per 1 oktober 2006 in werking getreden.<sup>28</sup> Art. 32 Bta bevat een wettelijke plicht voor een accountantsorganisatie om een zwarte lijst in te stellen<sup>29</sup> en vastgelegde incidenten te melden bij de Autoriteit Financiële Markten (AFM).<sup>30</sup> De nadere invulling en verdere uitwerking van de normen in het Bta dient te gebeuren via zelfregulering.<sup>31</sup> Voor accountantsorganisaties betekent dit dat zelfregulering kan geschieden door beroepsorganisaties zoals de NIVRA en NOVAA.

De verwerking van de gegevens als gevolg van art. 32 lid 2 Bta kan strafrechtelijke persoonsgegevens bevatten. Het begrip 'strafrechtelijke gegevens' heeft namelijk zowel betrekking op veroordelingen (gegevens waarbij de rechter, al dan niet onherroepelijk, strafrechtelijk gedrag heeft vastgesteld) als op min of meer gegronde verdenkingen (concrete aanwijzingen jegens een bepaalde persoon). De wettelijke verplichting van een waarschuwingslijst waarbij strafrechtelijke gegevens kunnen worden verwerkt, acht de wetgever noodzakelijk omdat dit vooral de AFM een snel en efficiënt inzicht biedt in de werking en in de mate van naleving van het stelsel van kwaliteitsbeheersing. Ook wordt de wijze zichtbaar waarop de accountantsorganisatie daarmee omgaat.

Strafrechtelijke gegevens kunnen als gevolg van art. 22 lid 4, onder *c* WBP worden verwerkt wanneer accountantsorganisaties passende en specifieke waarborgen hebben getroffen. De verwerkingen die voortvloeien uit het Bta zullen daarom moeten worden gemeld bij het CPB.<sup>32</sup>

Het CPB heeft in zijn wetgevingsadvies aan het ministerie van Financiën uitdrukkelijk laten weten dat de verwerking van persoonsgegevens ex art. 32 Bta onderworpen is aan een voorafgaand onderzoek door het CPB.<sup>33</sup> Het CPB heeft ook in dat advies laten weten het wenselijk te vinden dat alle accountantsorganisaties de verwerking en de melding daarvan bij het CPB op dezelfde wijze regelen.<sup>34</sup> Dit met het oog op een snelle en inhoudelijk verantwoorde afhandeling van de onderzoeken. Het standpunt van het CPB wordt niet alleen

ingegeven door eigenbelang, waarbij de beschikbare personele capaciteit alleen aan VO's wordt besteed waar sprake is van verwerkingen met de grootste risico's voor de persoonlijke levenssfeer. Het standpunt van het CPB sluit ook aan bij het brede kabinetsstreven om te komen tot administratieve lastenverlichting voor het bedrijfsleven.<sup>35</sup>

Omdat de Bta inmiddels in werking is getreden, is het voor accountantsorganisaties en hun beroepsverenigingen van belang de signalering van het CPB en de wetgever ter hand te nemen en te komen tot een modelmelding en tot modelprocedures. Het CPB kan dan, op grond van zijn discretionaire bevoegdheid, een gestandaardiseerde afdoening van het VO realiseren, waardoor de drempel die door een VO wordt opgeworpen, geruisloos en met minimale nalevingskosten kan worden genomen. Hierin kan een belangrijke rol zijn weggelegd voor de beroeps- en serviceorganisaties van accountants (NIVRA, NOVAA, SRA, NOVAK en NOAB), die hun krachten dienen te bundelen. Dit kan betekenen dat zij ten minste één van de verregaande en kostenverhogende implicaties van inwerkingtreding van de Wta en Bta voor hun leden tot een minimum kunnen beperken. In een tijdgeest waarin aanzienlijke vermindering van administratieve lasten voor ondernemers een belangrijk item is voor zowel de overheid als het bedrijfsleven, komt mij dit voor als een uitgelezen kans hierin proactief op te treden!

#### 5 Voorstellen tot aanpassing van het VO

De grote hoeveelheid en de grote verscheidenheid aan verwerkingen die voor een VO in aanmerking komen alsmede de administratieve lasten die het VO met zich meebrengt, heeft het CPB genoodzaakt een signaal hierover aan de Minister van Justitie af te geven.

In het kader van de vermindering van de administratieve lasten van de WBP heeft het CPB op 7 december 2004 tien voorstellen aan de Minister van Justitie gestuurd.<sup>36</sup> Aanpassing van het VO betrof één van die voorstellen. Ook in het kader van een breder voorgenomen wijziging van de WBP heeft het CPB voorstellen tot aanpassing van het VO naar de Minister van Justitie gestuurd.<sup>37</sup>

Zo schrijft het CPB dat het afspraken met een branche kan maken over de behandeling van voorafgaande onderzoeken als veel verantwoordelijken uit die branche voor een voorafgaand onderzoek in aanmerking komen (zoals de hiervoor genoemde telecommunicatiesector). De branche schrijft een protocol of gedragscode waarin de spelregels voor de gegevensverwerking worden vastgelegd en legt deze ter goedkeuring aan het CPB voor. Als het CPB het protocol heeft

26 Zie eerder nog in negatieve zin: CPB 21 november 2002, z2002-1335, en later ten positieve in het jaarverslag 2003 van het CPB, p. 32-33.

27 *Stb.* 2006, 380.

28 *Stb.* 2006, 404.

29 Art. 32 lid 2 Bta.

30 Art. 32 lid 4 Bta.

31 >*Stb.* 2006, 380, p. 17.

32 *Stb.* 2006, 380, p. 36-37, 45-46.

33 Wetgevingsadvies Cbp, december 2005, z2005-1239 (niet gepubliceerd).

34 Het CPB verwijst naar een eerdere uitspraak van 27 maart 2003, p. 4 en 5 (z2003-0168) en van 8 maart 2001 (z2000-1305).

35 CPB 7 december 2004, z2004-1086.

36 CPB 7 december 2004, z2004-1086.

37 CPB 12 juli 2005, z2004-1494.

goedgekeurd voert het in beginsel geen nader onderzoek meer uit als verantwoordelijken aangeven dat ze de goedgekeurde werkwijze onderschrijven. De voorafgaande onderzoeken worden in deze situatie gestandaardiseerd afgedaan zonder dat de verantwoordelijke aanvullende informatie hoeft te verschaffen.

Ten aanzien van de verwerking van strafrechtelijke gegevens ten behoeve van derden merkt het CPB op dat uit art. 22 WBP en de memorie van toelichting bij de WPB blijkt dat de wetgever heeft beoogd om een voorafgaand onderzoek, in het geval dat strafrechtelijke gegevens ten behoeve van derden worden verwerkt, alleen verplicht te stellen als geen van de andere uitzonderingen op het verbod om strafrechtelijke gegevens te verwerken ten behoeve van derden van toepassing is (art. 22 en 23 WBP). Het CPB adviseert de minister daarom om art. 31 lid 1, onder c WBP gelijk te laten zijn aan art. 22 lid 4, onder c WBP.

Verder schreef het CPB dat het de afgelopen jaren is gebleken dat er meer dan wenselijk een beroep gedaan wordt op de open uitzondering van art. 22 lid 4, onder c WBP. Het CPB meent dat nader onderzoek gewenst is naar de mogelijkheid en wenselijkheid de uitzonderingen op het verbod van de verwerking van strafrechtelijke gegevens fijnmaziger in te vullen. Hierdoor zouden namelijk veel voorkomende en maatschappelijk geaccepteerde verwerkingen van deze gegevens die geen onaanvaardbare risico's met zich meebrengen voor de rechten en vrijheden van de betrokkenen, niet langer vallen onder de uitzondering van het voorafgaand onderzoek door het CPB.

Enkele voorbeelden voor verwerkingen van strafrechtelijke gegevens ten behoeve van derden waar formeel gezien nu een voorafgaand onderzoek voor aangevraagd zou moeten worden, maar die naar het oordeel van het CPB wellicht niet onder het voorafgaand onderzoek zouden moeten vallen zijn:

- het verstrekken van strafrechtelijke gegevens aan de politie ten behoeve van de aangifte van een strafbaar feit;
- het verstrekken van strafrechtelijke gegevens aan inspecties en toezichthouders voor zover dit nodig is voor de uitoefening van hun taak en
- het uitwisselen van strafrechtelijke gegevens tussen partijen in samenwerkingsverbanden voor zover betrokken partijen alle op grond van hun eigen taken en bevoegdheden over deze gegevens mogen beschikken.

De uitleg van wat er bedoeld wordt met strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag leidt in de praktijk nog al eens tot verwarring. Het CPB beveelt de minister aan deze bepaling zo aan te passen dat de reikwijdte hiervan verhelderd wordt. Hierbij adviseert het CPB onder meer expliciet te maken dat ook tuchtrechtelijke maatregelen hieronder vallen. Tuchtrechtelijke maatregelen moeten worden beschouwd als bijzondere gegevens in de zin van art. 16 WBP.

38 Zie ook CPB 20 juni 2005, z2005-0409.

Daarnaast is het CPB van oordeel dat een verwerking alleen voor een voorafgaand onderzoek in aanmerking komt als de verantwoordelijke van plan is deze verwerkingen structureel toe te passen. Het gaat daarmee niet om incidentele verwerkingen en verwerkingen in incidentele situaties. Het CPB toetst in een voorafgaand onderzoek het systeem van de verwerking, geen eenmalige verwerkingen. Het woord voornemens in alledrie de gronden geeft hier enige indicatie voor, maar in de praktijk blijkt de WBP en de toelichting hier te weinig helder op zijn. Het CPB adviseert de minister de formulering van art. 31 WBP zodanig aan te passen dat duidelijk wordt dat het voorafgaand onderzoek alleen aan de orde is als het gaat om een structurele gegevensverwerking door een verantwoordelijke.<sup>38</sup>

Bovendien is het CPB van mening dat het begrip 'eigen waarneming' van art. 31 lid 1, onder b WBP, in de praktijk tot verwarring leidt omdat vaak onduidelijk blijft wat hier precies mee bedoeld wordt. Vooral nog interpreteert het CPB het als 'het gericht verzamelen van informatie door middel van eigen observatie'. Dit betekent dat de informatie niet verkregen wordt bij een andere verantwoordelijke. Observeren, posten, gericht burenonderzoek (informatie bij burens vragen en rapport opstellen) enz. vallen hiermee naar het oordeel van het CPB onder deze definitie.

## 6 Tot slot

Over het VO valt veel te zeggen. Veel meer dan op deze plaats ruimte voor is. In het voorgaande heb ik een beeld geschetst van het VO zelf en enige daarmee samenhangende voorbeelden en onderwerpen. Hieruit blijkt duidelijk dat het VO nog lang niet volgroeid is. Zowel wettechnisch als beleidsmatig is er behoorlijke ruimte voor verbetering. In de huidige situatie vormt de route van het VO voor veel verantwoordelijken een langdurige en moeilijk begaanbare weg waarbij het ook nog onzeker is wat zij aan het einde ervan zullen aantreffen.