COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

AAN College van Burgemeester & Wethouders
van de gemeente M

DATUM 31 mei 2007
ONS KENMERK z2006-01300
CONTACTPERSOON
070-8888500

UW BRIEF VAN 12 oktober 2006
UW KENMERK bestuurlijke aanpak Provincie

ONDERWERP Voorafgaand Onderzoek; definitief besluit

1. Inleiding

Op 12 oktober 2006 heeft het College bescherming persoonsgegevens (CBP) een melding ontvangen van een geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens (bestuurlijke aanpakProvincie).

De gemelde gegevensverwerking betreft, kort gezegd, de uitwisseling van persoonsgegevens tussen partijen die een bestuurlijke aanpak nastreven van georganiseerde criminaliteit, in het bijzonder op het vlak van het gebruik van niet-vergunningplichtige onroerende zaken voor malafide activiteiten.

Aan het slot van de melding is het CBP om een Voorafgaand Onderzoek (VO) gevraagd omdat er sprake zou zijn van elk van de drie in artikel 31, eerste lid, Wet bescherming persoonsgegevens (Wbp) genoemde risicovolle verwerkingen die een verzoek om een VO rechtvaardigen.

2. Verloop van het onderzoek tot nu toe

Naar aanleiding van de melding 'bestuurlijke aanpak Provincie' heeft het CBP op 7 november 2006 een VO zoals bedoeld in artikel 31 Wbp ingesteld. Het door het CBP ingestelde VO heeft geleid tot het besluit een nader onderzoek, zoals bedoeld in artikel 32, vierde lid, Wbp in te stellen. Het CBP heeft dit bij brief van 21 november 2006 meegedeeld aan de projectleider van het project bestuurlijke aanpak Provincie.

Het doel van het nader onderzoek was allereerst om te bepalen of er sprake is van een VO-waardige verwerking. Anders gezegd: of de verwerking voldoet aan de criteria genoemd in artikel 31, eerste lid, Wbp. Als geconstateerd kan worden dat er terecht een verzoek om een VO gedaan is, dient vervolgens onderzocht te worden of deze extra risicovolle verwerking toelaatbaar is.
In het kader van het nader onderzoek heeft het CBP de projectleider bestuurlijke aanpak georganiseerde criminaliteit Provincie op 11 december 2006 en 9 februari 2007 een aantal vragen voorgelegd. Bij brief van 12 januari en 16 februari 2007 zijn deze vragen beantwoord. Op 23 februari 2007 heeft ten kantore van het CBP een gesprek plaatsgevonden tussen het CBP en namens het project bestuurlijke aanpak georganiseerde criminaliteit Provincie, de projectleider en Adviesbureau. Op 2 maart 2007 zijn per email nog enkele vragen van het CBP beantwoord.
Bij brief van 9 maart 2007 heeft het CBP de voorlopige bevindingen van het onderzoek en zijn voorlopige conclusie aan bestuurlijke aanpak georganiseerde criminaliteit Provincie. Hierop is bij

email van 15 maart 2007 gereageerd. Naar aanleiding van deze reactie heeft het CBP bij email van 15 maart 2007 nog enkele vragen gesteld, welke zijn beantwoord bij email van diezelfde dag en voorts zijn besproken in een gezamenlijk telefonisch overleg tussen de projectleider bestuurlijke aanpak georganiseerde criminaliteit Provincie, Adviesbureau en CBP op 16 maart 2007.
De reacties op de voorlopige bevindingen van het CBP hebben geleid tot een aanpassing van het oordeel van het CBP. Het aangepaste oordeel is aan de projectleider bestuurlijke aanpak georganiseerde criminaliteit Provincie gestuurd. Van dit ontwerpbesluit is mededeling gedaan in de Staatscourant.

Het CBP heeft zijn besluit gebaseerd op de volgende informatie: de melding van de bestuurlijke aanpak Provincie en de informatie die is verstrekt in de schriftelijke, telefonische en mondelinge contacten tussen het CBP en de projectleider van het project bestuurlijke aanpak Provincie, die plaatsvonden op eerdergenoemde data. De 'Privacyregeling convenant ketensamenwerking bestuurlijke aanpak georganiseerde criminaliteit Provincie' (hierna: de privacyregeling) van Adviesbureau van mei 2006 en het 'Convenant ketensamenwerking bestuurlijke aanpak georganiseerde criminaliteit Provincie' (hierna: het convenant) dat is ondertekend op 23 juni 2006 hebben gediend ter illustratie.

Voor de goede orde merkt het CBP hier op dat het geen goedkeuringsverklaring of rechtmatigheidsoordeel afgeeft voor reglementen en convenanten. Deze kunnen naar hun aard geen uitsluitsel geven over daadwerkelijke verwerkingen van persoonsgegevens.

3. Bevindingen en conclusie

Het CBP legt hierbij zijn definitieve besluit in bovenstaand VO voor. Het College van Burgemeester en Wethouders van de gemeente Mt ontvangt dit besluit voordat het gepubliceerd wordt in de Staatscourant.

Op basis van het VO oordeelt het CBP dat de voorgenomen werkwijze van de bestuurlijke aanpak Provincie zal leiden tot een gegevensverwerking die in overeenstemming met de wet en dus rechtmatig is. Hieronder, bij punt 4, licht het CBP dit verder toe.

a. Samenwerking

De beoogde bestuurlijke aanpak is een samenwerkingsverband dat tot doel heeft misstanden in de onroerend goedsector te signaleren en door samenwerking tussen deelnemende partijen bestuursrechtelijk aan te pakken. Het gaat om de integrale aanpak van transacties in onroerende zaken die zijn gefinancierd met vermogen dat met criminele activiteiten is verkregen en de aanpak van het gebruik van onroerende zaken voor witwassen van crimineel vermogen.

Gemeenten en provincies kunnen op grond van de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Wet Bibob) persoonsgegevens verwerken met het oog op het beoordelen van de integriteit van aanvragers van gemeentelijke vergunningen en overheidssubsidies. De gegevensverwerkingen die plaatsvinden in het kader van een procedure op basis van de Wet Bibob staan los van de werkwijze van de beoogde bestuurlijke aanpak. Dergelijke gegevensverwerkingen vallen buiten de reikwijdte van dit VO. Het CBP heeft zijn VO dus gericht op de gegevensverwerkingen door het Regionaal Projectteam (RPT) die betrekking

hebben op niet-vergunningplichtige panden, dat wil zeggen onroerende zaken waarop de Wet Bibob niet van toepassing is.

Aan de beoogde bestuurlijke aanpak nemen de volgende partijen deel: OM, vijf gemeenten (M, S, K, H, V), de provincie L, het regionaal politiekorps , SIOD en FIOD-ECD. Er is ten behoeve van de beoogde bestuurlijke aanpak een RPT opgericht, dat naar aanleiding van een verzoek van een deelnemer bij de andere deelnemers informatie opvraagt over een of meer panden. Die informatie kan ook bestaan uit persoonsgegevens van personen die op enigerlei wijze betrokken zijn bij een pand. Het RPT slaat informatie uit open, halfopen en gesloten bronnen op in respectievelijk checklist 1, 2 en 3. Het RPT anonimiseert deze gegevens ten behoeve van het informatieoverleg.

In het informatieoverleg worden onder leiding van het RPT door daartoe door elke deelnemer aangewezen vertegenwoordigers geanonimiseerde casus besproken en voorstellen gedaan ten aanzien van mogelijke handhavende acties. Partijen die tot (gezamenlijk) handhaven willen overgaan ontvangen van het RPT de bij de betreffende casus behorende persoonsgegevens die het RPT ter voorbereiding en ondersteuning van het informatieoverleg had verzameld opdat zij deze casus in het casusoverleg nader, concreter, kunnen bespreken en afspraken kunnen maken over wie daadwerkelijk tot handhaven zal/zullen overgaan. Het RPT houdt van iedere zaak die wordt opgepakt een dossier bij waarin ondermeer (in checklist 4) de resultaten van de handhavende acties worden vermeld.

Overigens wijst het CBP erop dat er in deze context altijd sprake is van gegevensuitwisselingen tussen verantwoordelijken en niet tussen de individuele werknemers/ambtenaren werkzaam bij die verantwoordelijken.

b. Artikel 31, eerste lid, sub a, b en c, Wbp

Het VO is aangevraagd vanwege drie typen risicovolle verwerkingen.

Op grond van artikel 31, eerste lid, sub a, Wbp is een voorafgaand onderzoek vereist indien de verantwoordelijke voornemens is om een nummer ter identificatie van personen te verwerken voor een ander doeleinde dan waarvoor het nummer specifiek bestemd is teneinde gegevens in verband te kunnen brengen met gegevens die worden verwerkt door een andere verantwoordelijke, tenzij gebruik van het nummer geschiedt voor de gevallen als omschreven in artikel 24 Wbp.

Uit de aan het CBP verstrekte informatie begrijpt het CBP dat de gemelde gegevensverwerking geen verwerking is als bedoeld in artikel 31, eerste lid, sub a, Wbp. Het RPT is immers niet voornemens om het sofinummer te verwerken teneinde een koppeling tot stand te brengen.

Overigens merkt het CBP in dit verband het volgende op. Voor de verwerking van het sofinummer is ingevolge artikel 24 Wbp een wettelijke grondslag vereist. In casu is noch in een wet noch in een AMvB voorzien in enig gebruik van het sofinummer door het RPT. De verwerking van het sofinummer door het RPT zou daarom onrechtmatig zijn.

Op grond van artikel 31, eerste lid, sub b, Wbp stelt het CBP een onderzoek in indien een verantwoordelijke voornemens is gegevens vast te leggen op grond van eigen waarneming zonder de betrokkene daarvan op de hoogte te stellen.

Uit de aan het CBP verstrekte informatie begrijpt het CBP dat er van 'eigen waarneming' in de zin van artikel 31, eerste lid, sub b, Wbp geen sprake is. In het kader van de beoogde bestuurlijke aanpak worden door het RPT voor de deelnemende gemeenten gegevens verzameld en doorverstrekt. Bij deze gegevensverwerking worden echter geen waarnemingen ter plaatse door functionarissen van het RPT verricht.

Wat betreft het (niet) informeren van betrokkenen over de verwerking van hen betreffende persoonsgegevens verwijst het CBP naar het hieronder onder punt 4h gestelde.

Op grond van artikel 31, eerste lid, sub c, Wbp stelt het CBP een onderzoek in indien een verantwoordelijke 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 voor derden.

Op basis van de aan het CBP verstrekte informatie komt het CBP tot de conclusie dat de gemelde gegevensverwerking een verwerking is als bedoeld in artikel 31, eerste lid, sub c, Wbp. Het RPT verzamelt immers persoonsgegevens van ondermeer politie, Openbaar Ministerie (OM) en FIOD-ECD en verstrekt deze aan deelnemers van de bestuurlijke aanpak Provincie (voor zover zij hebben besloten tot actie over te gaan).

Het VO richt zich derhalve op de risicovolle aspecten van de verwerkingen van strafrechtelijke persoonsgegevens die in het kader van de beoogde bestuurlijke aanpak plaatsvinden ten behoeve van derden (zoals bedoeld in artikel 31, eerste lid, sub c, Wbp).

4. Verwerking van strafrechtelijke persoonsgegevens

a. Grondslagen voor gegevensverwerkingen

Artikel 6 Wbp stelt dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Omdat onder verwerken alles verstaan wordt wat je met persoonsgegevens kunt doen (zie artikel 1 Wbp), betekent dat onder meer dat ook de ontvangst van persoonsgegevens in overeenstemming met de wet moet zijn.

Het CBP maakt uit de beschikbare informatie op dat de verwerkingen van strafrechtelijke persoonsgegevens die plaatsvinden in het kader van de beoogde bestuurlijke aanpak op de volgende grondslagen kunnen worden gebaseerd.

Het RPT kan persoonsgegevens ontvangen van politie, gemeente, OM, FIOD-ECD en SIOD op grond van 8, onder e, Wbp. Voor de ontvangst van strafrechtelijke persoonsgegevens biedt artikel 22, lid 1, Wbp een uitzondering op het verbod van artikel 16 Wbp.

De gegevensverstrekking van het RPT aan politie, gemeente(n), OM, FIOD-ECD en SIOD zou verenigbaar zijn (artikel 9, eerste en tweede lid, Wbp) en ingevolge artikel 22, vierde lid, sub c, Wbp niet verboden (zoals bedoeld in artikel 16 Wbp).

Het CBP plaatst bij deze grondslagen de volgende opmerkingen.

Artikel 30 Wpolr

Artikel 30, eerste lid, Wpolr bevat een bepaling die ontvangers van gegevens uit politieregisters in beginsel tot geheimhouding verplicht. Artikel 30 Wpolr blijft van toepassing op gegevens die zijn verstrekt uit een politieregister, ook wanneer deze door de ontvanger worden verwerkt en doorverstrekt onder het regime van de Wbp.

Blijkens de wetsgeschiedenis van de Wpolr is de geheimhouding waartoe artikel 30 verplicht doelgebonden: de gegevens mogen worden gebruikt voor het doel waarvoor zij zijn verstrekt (Memorie van Antwoord II, 19589, nr. 6, p. 26). Artikel 30, eerste lid, Wpolr bevat daarnaast een uitzonderingsgrond. Verstrekking van gegevens die afkomstig zijn uit een politieregister is mogelijk voor zover een op de wet gebaseerd voorschrift mededeling toelaat, dan wel de uitvoering van de betrokken taak tot bekendmaking noodzaakt.

Artikel 18, vijfde lid, Wpolr

De door het Ministerie van Justitie verstrekte machtiging op grond van artikel 18, vijfde lid, Wpolr vormt (tot het moment van inwerkingtreding van de Wet politiegegevens, zie hieronder) een grondslag voor het verstrekken van persoonsgegevens door de politie aan het RPT. De artikelen 15, eerste lid, sub b, Wpolr en artikel 14, eerste lid, sub k, Besluit politieregisters (Bpolr) kunnen daarom buiten beschouwing blijven.

De artikel 18, vijfde lid, Wpolr machtiging stelt overigens wel voorwaarden aan de gegevensverstrekking uit een politieregister.

Concept-artikel 20 Wet politiegegevens

Zoals het zich laat aanzien zal de onderhavige verstrekking gebaseerd kunnen worden op het concept-artikel 20 Wet politiegegevens (Wpolg) zodra de Wpolg in werking is getreden. Politiegegevens kunnen op basis van concept-artikel 20 Wpolg ten behoeve van een samenwerkingsverband alleen worden verstrekt aan personen of instanties voor zover dit met het oog op een zwaarwegend algemeen belang noodzakelijk is. Het doel van de verstrekking uit een politieregister dient daarnaast overeen te stemmen met dan wel verenigbaar te zijn met de uitvoering van de politietaak, zoals bedoeld in artikel 2 Politiewet 1993. Dat wil zeggen dat gegevens uit een politieregister ten behoeve van een samenwerkingsverband alleen kunnen worden verstrekt voor een viertal doeleinden: het voorkomen en opsporen van strafbare feiten; het handhaven van de openbare orde; hulpverlening; het uitoefenen van toezicht op het naleven van regelgeving.

Voorts zal de Wpolg net zoals de Wpolr een geheimhoudingsplicht kennen: de ontvangers van gegevens uit een politieregister zijn in beginsel verplicht tot geheimhouding daarvan (concept-artikel 7 Wpolg).

Paragraaf 3 Wpolr

De gegevens uit voorlopige registers en zwacri-registers van de CIE-SIOD vallen onder het striktere Wpolr regime.

Wjsg

Hoewel in het informatieoverleg geanonimiseerde casus worden besproken, zal niet altijd voorkomen kunnen worden dat ook persoonsgegevens worden verwerkt. Bijvoorbeeld: de aankondiging van het OM dat het OM tot vervolging overgaat en de registratie daarvan door het RPT kunnen reeds een verwerking van strafvorderlijke gegevens vormen.

De verantwoordelijke dan wel het RPT moet in dat geval aantonen dat is voldaan aan de voorwaarden die de Wjsg en de Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (Aanwijzing Wet justitiële en strafvorderlijke gegevens) stellen aan de verstrekking van strafvorderlijke gegevens. Strafvorderlijke gegevens zijn bovendien bijzondere gegevens in de zin van artikel 16 Wbp, hetgeen betekent dat een uitzondering op het verbod op verwerking ervan moet worden gevonden (in artikel 22 of 23 Wbp).

b. Omvang set persoonsgegevens voor het casusoverleg

Naar het CBP begrijpt verstrekt het RPT de persoonsgegevens die het heeft verzameld in een door het RPT voorgezeten casusoverleg aan de (vertegenwoordigers van de) deelnemers van de beoogde bestuurlijke aanpak die hebben besloten een casus te gaan oppakken.
In het overleg met het CBP op 23 februari 2007 heeft de rojectleider bestuurlijke aanpak georganiseerde criminaliteit Provincie aangegeven dat nog niet is besloten of alle persoonsgegevens die het RPT tot zijn beschikking heeft worden verstrekt aan de deelnemers van het casusoverleg, of uitsluitend de persoonsgegevens die afkomstig zijn van deelnemers aan de beoogde bestuurlijke aanpak die daadwerkelijk tot aanpak overgaan.

Artikel 11, eerste lid, Wbp bepaalt dat persoonsgegevens slechts worden verwerkt voor zover zij, gelet op de doeleinden van de verwerking, toereikend, ter zake dienend en niet bovenmatig zijn. Het CBP wijst erop dat bij de beslissing ten aanzien van de verstrekking van persoonsgegevens aan deelnemers van het casusoverleg rekening gehouden moet worden met dit proportionaliteitsvereiste.

c. Toestemming

In het convenant wordt aangegeven dat deelnemers aan het casusoverleg toestemming aan verstrekkende deelnemers aan de beoogde bestuurlijke aanpak dienen te vragen alvorens zij ontvangen informatie doorverstrekken aan andere deelnemers dan wel derden.
Het CBP wijst erop dat het vragen van toestemming aan verstrekkende deelnemers alvorens door te verstrekken in casu geen wettelijke grondslag voor verstrekking vormt. Ook hier geldt dat iedere partij zelf in de Wbp (artikel 8) of een andere wet een grondslag voor gegevensverwerking dient te kunnen aanwijzen.

d. Informatieplicht

Ingevolge artikel 34 Wbp is de verantwoordelijke, dan wel het RPT, in beginsel verplicht op eigen initiatief de betrokkene op de hoogte te stellen van het bestaan van de gegevensverwerking, zodat de betrokkene in staat is de gegevensverwerking over hem of haar te volgen (en zodoende eventueel onrechtmatig gedrag van de verantwoordelijke aan te vechten).
Artikel 34, vierde lid, Wbp biedt een uitzondering op de informatieplicht, maar deze dient restrictief geïnterpreteerd te worden en altijd per geval onderbouwd. Indien informeren onmogelijk blijkt of een onevenredige inspanning kost kan worden volstaan met het vastleggen van de herkomst van persoonsgegevens die door het RPT zijn verzameld.

In casu kan er mogelijk door de verantwoordelijke een beroep gedaan worden op artikel 43 Wbp. Dit artikel stelt dat onder andere artikel 34 Wbp buiten toepassing kan worden gelaten voor zover dit noodzakelijk is in het kader van de in artikel 43 Wbp genoemde belangen, waaronder het belang van de voorkoming, opsporing en vervolging van strafbare feiten. Er kan alleen een beroep gedaan worden op deze uitzondering op het zeer belangrijke principe van transparantie na afweging in concreto. Die belangenafweging kan niet op voorhand door middel van een samenwerkingsovereenkomst gemaakt worden. De woorden 'voor zover' in artikel 43 Wbp wijzen er op dat, zodra dit mogelijk is, de betrokkene geïnformeerd moet worden.

e. Beveiliging

Het CBP leidt uit de beschikbare informatie af dat in het kader van de beoogde bestuurlijke aanpak voorts de volgende waarborgen zijn getroffen voor de bescherming van de persoonlijke levenssfeer van betrokkenen.

1. Er is aangegeven dat gegevensverwerkingen door het RPT plaatsvinden via het Veiligheidsnet bij de politie. Dossiers die het RPT bewaart worden opgeslagen binnen een digitaal afgeschermde werkomgeving op het politienetwerk, dat alleen toegankelijk is voor leden van het RPT. Door deze werkwijze bestaan naar het oordeel van het CBP extra waarborgen bestaan wat betreft informatiebeveiliging.

2. Alleen het RPT heeft toegang tot alle persoonsgegevens die door de deelnemende instanties zijn verstrekt ten behoeve van de beoogde bestuurlijke aanpak. Verder kan iedere deelnemer alleen zijn eigen informatie terugvinden in het dossier bij het RPT. Deze werkwijze draagt naar het oordeel van het CBP bij aan een zorgvuldige omgang met persoonsgegevens.

3. Er wordt functiescheiding toegepast ten aanzien van de toegang tot (bijzondere) persoonsgegevens. Het RPT vraagt informatie op bij de aanspreekpunten van de andere convenantpartners. Aan het informatieoverleg nemen echter niet aanspreekpunten maar de vertegenwoordigers van de convenantpartners deel. Het CBP is van oordeel dat deze werkwijze het waarborgen van anonimiteit van de besproken casus in het informatieoverleg ten goede komt.

f. Vernietigen en bewaren

Het CBP heeft vernomen dat checklist 3 (waarin persoonsgegevens uit gesloten bronnen zijn opgenomen) vernietigd wordt zodra in het informatieoverleg is besloten dat geen handhavende acties zullen worden ondernomen. Het CBP acht dit correct.

Indien een casus op basis van het casusoverleg wordt opgepakt door een of meerdere deelnemers wordt het op die zaak betreffende dossier door het RPT bewaard. In aanvulling op de checklists 1, 2 en 3 (met gegevens uit open, halfopen respectievelijk gesloten bronnen) wordt een vierde checklist opgesteld. Checklist 4 bestaat uit de voorlopige conclusies van checklists 1, 2 en 3; een vermelding van de partij of partijen die handhavend gaat of gaan optreden; en een samenvatting van de resultaten van de handhavende acties. De gegevens worden maximaal drie jaar bewaard, alvorens aan een update te worden onderworpen. Gegevens uit checklist 4 worden niet verstrekt aan deelnemers aan het informatieoverleg. Informatie uit checklist 4 kan, indien relevant, door het RPT worden ingebracht in het casusoverleg.

Het CBP wijst in dit verband op het volgende:

Voor de verstrekking van persoonsgegevens door ieder van de deelnemers van het casusoverleg aan het RPT, ten behoeve van de registratie van resultaten van handhavende partijen in checklist 4, dient een wettelijke grondslag aanwezig te zijn (zie ook hierboven onder punt 4a).

Het verdient aanbeveling om periodiek te evalueren in hoeverre de noodzaak om dossiers met persoonsgegevens te bewaren nog aanwezig is. Voor monitoring en evaluatie van de beoogde bestuurlijke aanpak kan zeer waarschijnlijk worden volstaan met informatie die van identificerende gegevens is ontdaan.

Het CBP adviseert om, als de beoogde bestuurlijke aanpak gedurende enkele jaren is uitgevoerd, te evalueren in hoeverre de bewaartermijn van 3 jaar die thans als uitgangspunt geldt adequaat is met het oog op artikel 11 Wbp.

g. Rechten betrokkenen

Ten aanzien van de mogelijkheden voor betrokkenen om hun rechten (inzage, correctie, verwijdering, verzet) uit te oefenen is het CBP geïnformeerd over de volgende voorzieningen.
- Er is een privacyreglement opgesteld. In artikelen 18 t/m 25 van de privacyregeling worden de rechten van betrokkenen beschreven.
- Daarnaast maakt ieder van de vijf deelnemende gemeenten bij het gemeenteloket en op de website bekend wie het privacyaanspreekpunt bij de desbetreffende gemeente is en op welke wijze de contactpersoon van het RPT kan worden bereikt. De contactpersoon van het RPT zal verzoeken om inzage, correctie en verwijdering behandelen.

Hoewel het CBP geen privacyreglementen toetst, hecht het CBP er aan om op te merken dat de huidige privacyregeling de tekst uit de Wbp bijna woordelijk herhaalt, maar geen vertaling biedt van de Wbp-normen naar praktische voorzieningen of regels. Het verdient aanbeveling om toereikende voorzieningen te treffen die waarborgen dat betrokkenen in staat worden gesteld om hun rechten uit te oefenen.

Bij email van 15 maart 2007 heeft de heer Rovers aangegeven dat deze voorzieningen zullen worden getroffen. Daarnaast kan de Functionaris voor de Gegevensbescherming (FG), die blijkens genoemde waarschijnlijk wordt aangesteld in het kader van het project bestuurlijke aanpak Provincie, mogelijk een rol vervullen bij het treffen van adequate praktische voorzieningen.

h. Toekomstige uitbreiding aantal samenwerkenden

Voorzien wordt dat veertien gemeenten in de regio zich zullen aansluiten bij het project en dat daarnaast samenwerking wordt gezocht met de Nationale Recherche en de Arbeidsinspectie.

Het CBP wijst er op dat er onderscheid is tussen samenwerken en samen persoonsgegevens uitwisselen. Een afspraak om samen te werken legitimeert op zich niet dat persoonsgegevens uitgewisseld worden. Het is heel wel mogelijk dat het aantal deelnemers aan een samenwerkingsverband niet samenvalt met het aantal verantwoordelijken dat persoonsgegevens met elkaar mag delen. Het is zelfs denkbaar dat deelnemers aan een samenwerkingsverband geen enkel persoonsgegeven aan elkaar mogen verstrekken. Een uitbreiding van het aantal samenwerkende partijen betekent ook niet noodzakelijkerwijs een uitbreiding van het aantal rechtmatige ontvangers van persoonsgegevens. Iedere partij dient immers een grondslag voor gegevensverwerking te kunnen aanwijzen.

Een samenwerkingsverband moet niet bij het CBP gemeld worden. Een gegevensverwerking die daaruit voortvloeit wel, voor zover het een meldingsplichtige verwerking is. Een uitbreiding van de deelnemende instanties kan gevolgen hebben voor de rechtmatigheid van de gegevensverwerkingen die in het kader van de beoogde bestuurlijke aanpak plaatsvinden en voor de melding van de gegevensverwerking bij het CBP.

i. Melding bij het CBP

Het CBP verzoekt de verantwoordelijke om de melding via het meldingenprogramma aan te passen in overeenstemming met het bovenstaande.

De melding dient tevens wat betreft de aanvraag van een voorafgaand onderzoek (vanwege artikel 31, eerste lid, sub a en b Wbp) aangepast te worden.
De Provincie Limburg en de Belastingdienst zijn niet direct betrokken bij de gegevensverwerkingen die via het RPT plaatsvinden in het kader van de beoogde bestuurlijke aanpak, aangezien de provincie en Belastingdienst geen gegevens van het RPT ontvangen. De melding dient in lijn hiermee aangepast te worden.

Het CBP geeft de verantwoordelijke in overweging om de naam van de melding aan te passen zodat de werkwijze en doelstelling van de bestuurlijke aanpak beter tot uitdrukking komen.

Thans is het College van Burgemeester & Wethouders van de gemeente Maastricht verantwoordelijke in de zin van artikel 1 Wbp. Voorzien wordt dat het RPT in de nabije toekomst een rechtspersoon zal worden. In dat geval zal de RPT als (gedeeltelijk) verantwoordelijke rechtspersoon in de melding genoemd moeten worden. Indien een FG wordt aangesteld in het kader van de beoogde bestuurlijke aanpak dan zal deze natuurlijke persoon aangesteld worden door en werkzaam zijn voor de rechtspersoon RPT. Een FG dient overigens te worden aangemeld bij het CBP.

5. Besluit

Op basis van al het voorgaande is het CBP van oordeel dat de onderhavige verwerking van strafrechtelijke persoonsgegevens ten behoeve van derden in beginsel in overeenstemming met de wet en daarom rechtmatig is.

Gedurende zes weken na plaatsing van het definitieve besluit in de Staatscourant liggen besluit en onderliggende stukken ter inzage bij het CBP. Tegen het definitieve besluit kan door een belanghebbende beroep worden ingesteld bij de rechtbank. Indien niemand beroep instelt, is het besluit na zes weken onherroepelijk geworden. Het dossier zal dan worden gesloten.

Het College bescherming persoonsgegevens,
Voor het College,

mw. mr. dr. J. Beuving
collegelid