

# **BESTUURLIJK AKKOORD**

## **Geïntegreerde Decentrale Aanpak**

### **Georganiseerde Misdaad**

#### **September 2008**

#### **Inleiding**

Georganiseerde misdaad moet bij de wortel worden aangepakt, in het bijzonder daar waar sprake is van verwevenheid tussen de onderwereld en de bovenwereld. De schade die georganiseerde misdaad aan de Nederlandse samenleving toebrengt is onverminderd groot. Niet voor niets heeft dit kabinet de aanpak van georganiseerde misdaad hoog op de agenda staan, zoals blijkt uit het eind 2007 opgestelde Programma Versterking Aanpak Georganiseerde Misdaad (PVAGM)<sup>1</sup>. Dit Bestuurlijk Akkoord is één van de beoogde resultaten genoemd in pijler twee van het programma Bestuurlijke Aanpak Georganiseerde Misdaad<sup>2</sup> dat onder regie van de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) tot stand is gekomen.

Prioriteiten bij de bestrijding van de georganiseerde misdaad worden elke vier jaar vastgesteld op basis van het Nationaal Dreigingsbeeld. Zoals beschreven in het PVAGM krijgen binnen die prioriteiten thans de volgende thema's bijzondere aandacht:

- mensenhandel;
- georganiseerde hennepteelt;
- misbruik van vastgoed voor criminele doeleinden;
- witwassen/onverklaarbaar vermogen.

Voor een effectieve bestrijding van georganiseerde misdaad is het nodig dat de aanpak zich zowel richt op individuele daders en criminele samenwerkingsverbanden als op de achterliggende gelegenheidsstructuren of factoren die de misdaad (kunnen) faciliteren.

Zoals gesteld in het programma Bestuurlijke Aanpak Georganiseerde Misdaad vraagt dit om een brede, geïntegreerde aanpak door verschillende partijen op decentraal niveau met de hun ter beschikking staande middelen. Een geïntegreerde aanpak veronderstelt dat de betrokken partijen met elkaar samenwerken om met elkaar te bepalen wat de meest effectieve handelswijze c.q. interventie is van een partij, voor zover dit noodzakelijk is in het belang van en ten behoeve van de opgedragen wettelijke taak van die partij. De interventiemogelijkheden bestaan uit bestuurlijk, preventief optreden en strafrechtelijk, repressief optreden. De bestuurlijke aanpak zal worden ingezet om preventief ingrijpen mogelijk te maken, dan wel om gesignaleerde knelpunten weg te nemen of maatregelen te treffen om drempels op te werpen tegen specifieke vormen van criminaliteit.

De geïntegreerde aanpak staat of valt met doelmatige en doeltreffende samenwerking tussen de partijen, onder andere door het op een rechtmatige wijze delen van informatie. Dit Bestuurlijk Akkoord en het hieraan gehechte Regionaal Convenant Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad (hierna: Regionaal convenant) is het uitgangspunt hiervoor. Volledigheidshalve zij hierbij opgemerkt dat het Bestuurlijk Akkoord niet tornt aan de bestaande wettelijke kaders, bevoegdheden en overlegstructuren van en tussen de betrokken partijen, noch treedt het in de plaats van andere initiatieven op het gebied van de geïntegreerde aanpak c.q. de bestrijding van georganiseerde misdaad.

---

<sup>1</sup> Brief aan Tweede Kamer d.d. 13 december 2007, TK 29 911, nr. 10. Het PVAGM moet worden gezien in samenhang met de versterkingsprogramma's aanpak financieel - economische criminaliteit en aanpak cybercrime. Alle drie de versterkingsprogramma's vormen een nadere uitwerking van het project Veiligheid begint bij Voorkomen (Brief aan Tweede Kamer d.d. 6 november 2007, TK 28 864, nr. 119) dat het huidige kabinet onder pijler vijf van het Beleidsprogramma heeft benoemd.

<sup>2</sup> Brief aan Tweede kamer, d.d. 15 februari 2008, TK 29911, nr. 11

Het doel van dit Bestuurlijk Akkoord is drieledig:

1. Met dit Bestuurlijk Akkoord verklaren de minister van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Justitie, de staatssecretaris van Financiën, de minister van Defensie, de staatssecretaris van Sociale Zaken en Werkgelegenheid, de voorzitter van het College van procureurs-generaal en de voorzitter van de Vereniging van Nederlandse Gemeenten een geïntegreerde aanpak van georganiseerde misdaad op lokaal danwel regionaal niveau actief te ondersteunen, ter realisatie van de doelstelling in het Regionaal convenant. Een geïntegreerde aanpak staat of valt met de wil tot samenwerken. Het gaat dan om samenwerking tussen gelijkwaardige partners waarin de verantwoordelijkheid van iedere individuele partner om per concreet geval (of het nu gaat om gegevensuitwisseling of om een interventie) een eigen afweging te maken, door de andere partners wordt gerespecteerd. Dit laat onverlet dat partijen elkaar aanspreken om ieders bijdrage in de interventiemogelijkheden ten volle te benutten.
2. Het Bestuurlijk Akkoord expliciteert voorts de set spelregels waarbinnen de informatie-uitwisseling in regionale samenwerkingsverbanden ten behoeve van de geïntegreerde aanpak op decentraal niveau vorm kan krijgen. Het maakt de minimum randvoorwaarden van deze werkwijze transparant, in een juridisch kader. Het juridisch kader geeft inzicht in de wettelijke mogelijkheden van de betrokken partijen om informatie, waaronder persoonsgegevens, uit te wisselen, onder andere op basis van de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens, de Algemene Wet inzake Rijksbelastingen en de Wet bescherming persoonsgegevens. Met het Bestuurlijk Akkoord en het Regionaal convenant worden ook handvatten gegeven om op decentraal niveau concreet invulling te geven aan de waarborgen, noodzakelijk voor de rechtsbescherming van de burgers die het betreft. Het College Bescherming Persoonsgegevens heeft kennis genomen van dit juridisch kader. De minister van BZK, in overleg met andere partijen, bewaakt dit juridisch kader opdat de actualiteit gegarandeerd is.
3. Het Bestuurlijk Akkoord is direct toepasbaar voor implementatie op decentraal niveau. Hiertoe is in de bijlage van het Bestuurlijk Akkoord een modelconvenant "*Regionaal Convenant Geïntegreerde Decentrale Aanpak Georganiseerde Misdad Regio....*" (hierna: Regionaal convenant) opgenomen. Met de ondertekening van het Regionaal convenant ontstaat een regionaal samenwerkingsverband ten behoeve van de geïntegreerde aanpak van georganiseerde misdaad. De doelstelling en werkwijze zijn, binnen de kaders van het Bestuurlijk Akkoord, op decentraal niveau nader te specificeren. Het samenwerkingsverband werkt op basis van tijdelijke coalities; op decentraal niveau wordt in overleg per concreet geval gezien op welke wijze - bestuursrechtelijk en/of strafrechtelijk - en door welke partner interventie plaatsvindt. Voorafgaand aan de uitwisseling van persoonsgegevens binnen dit samenwerkingsverband is het noodzakelijk dat een melding aan het College Bescherming Persoonsgegevens plaatsvindt. Bij het Regionaal convenant is als bijlage een '*Checklist Waarborging naleving Wet bescherming persoonsgegevens Regionaal Samenwerkingsverband*' (hierna: Checklist Wbp) opgenomen die handvatten biedt voor deze melding. De Regionale Informatie en Expertise Centra (RIEC's), zoals door de minister van BZK aangekondigd in het programma Bestuurlijke Aanpak Georganiseerde Misdad<sup>3</sup>, kunnen het samenwerkingsverband indien gewenst ondersteuning bieden.

---

<sup>3</sup> zie voetnoot 2

## **1. Juridisch kader informatie-uitwisseling**

Decentrale convenantpartners in het regionale samenwerkingsverband verplichten zich over en weer met inachtneming van de wettelijke bepalingen die informatie te verstrekken die nodig is om de samenwerking effectief en efficiënt te laten verlopen. De bevoegdheid van informatieverstrekking aan een convenantpartner binnen het regionale samenwerkingsverband ten behoeve van de aanpak en bestrijding van de georganiseerde misdaad wordt bepaald door de wettelijke taken, verantwoordelijkheden en bevoegdheden van de afzonderlijke convenantpartners in het regionale samenwerkingsverband en door het wettelijke kader voor de verwerking van persoonsgegevens. Hieronder is het juridisch kader van de decentrale convenantpartners opgenomen op basis waarvan zij binnen het regionale samenwerkingsverband bevoegd zijn persoonsgegevens te verwerken ten behoeve van de aanpak van de georganiseerde misdaad.

### Bevoegdheid gemeenten

Op grond van artikel 172 Gemeentewet is de burgemeester verantwoordelijk voor de handhaving van de openbare orde. De rechtmatigheidsgrondslag om op grond van de Wet bescherming persoonsgegevens (Wbp) in onderhavig samenwerkingsverband persoonsgegevens te verstrekken is artikel 8 sub e van deze wet. Deze rechtmatigheidsgrondslag houdt in dat de verwerking van persoonsgegevens noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van het bestuursorgaan; in casu de gemeente.

In het geval gemeenten persoonsgegevens uit de gemeentelijke basisadministratie verstrekken, zal de gemeente ervoor moeten zorg dragen dat deze verstrekking overeenkomstig het derdenverstrekkingregime (zie de artikel 96, 98 en 100 van de Wet gemeentelijke basisadministratie) is ingericht.

### Bevoegdheid politie

Op grond van artikel 2 van de Politiewet 1993 is de politie bevoegd gegevens te verwerken voor de uitoefening van haar politietaak zoals de handhaving van de rechtsorde.

De verwerking van politiegegevens valt onder het regime van de Wet politiegegevens (hierna: Wpg). Artikel 20 Wpg jo artikel 4.5 Besluit politiegegevens geeft de verantwoordelijke de mogelijkheid om onder bepaalde voorwaarden structureel politiegegevens te verstrekken aan een samenwerkingsverband. Deze voorwaarden voor gegevensverstrekking op grond van artikel 20 Wpg zijn opgenomen in artikel 3.1 van het Regionale convenant. In artikel 3.1 van het Regionale convenant is tevens opgenomen dat met ondertekening van dat convenant aan deze voorwaarden wordt voldaan, ervan uitgaande dat de verantwoordelijke voor de gegevensverstrekking deze beslissing in overeenstemming met het bevoegd gezag heeft genomen. Ten aanzien van het type politiegegevens dat wordt verstrekt is het uitgangspunt dat in principe geen politiegegevens worden verstrekt die worden verwerkt in het kader van een onderzoek in verband met de handhaving van de rechtsorde en in een bepaald geval of in het kader van een onderzoek naar de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (politiegegevens in de zin van artikel 9 en 10 Wpg). Slechts in bepaalde gevallen kan hierop op grond van het bepaalde in artikel 4.5 van het Besluit politiegegevens een uitzondering worden gemaakt.

### Bevoegdheid Openbaar Ministerie (OM)

Het OM is belast met de strafrechtelijke handhaving van de rechtsorde. Het OM heeft het gezag over de opsporing van strafbare feiten en is verantwoordelijk voor het vervolgen daarvan, alsmede voor de tenuitvoerlegging van opgelegde straffen. De verstrekking van gegevens van het OM aan de afzonderlijke deelnemers binnen het regionale samenwerkingsverband is mogelijk op grond van artikel 8a en artikel 39f van de Wet justitiële en strafvorderlijke gegevens (Wjsg). In de Aanwijzing wet justitiële en strafvorderlijke gegevens is onder meer opgenomen onder welke voorwaarden verstrekking van strafvorderlijke gegevens mogelijk is.

### Bevoegdheid Belastingdienst

De Belastingdienst is onder meer belast met de goede uitvoering van de Algemene Wet inzake Rijksbelastingen (Awr). Op grond van artikel 67 lid 2 Awr jo art 43c lid 1 sub I van de Uitvoeringsregeling Algemene Wet inzake Rijksbelastingen (hierna: Uitvoeringsregeling) is de Belastingdienst bevoegd gegevens te verstrekken aan onder meer: gemeenten, politie, en de officier van justitie. De hieraan verbonden voorwaarden zijn dat er sprake moet zijn van een integrale toepassing en handhaving van overheidsregelingen en dat er een convenant aan de samenwerking ten grondslag ligt dat betrekking heeft op een concreet omschreven gemeenschappelijk handhavingstekort. Met de ondertekening van het Bestuurlijk Akkoord en het Regionale convenant wordt aan deze voorwaarden van de Uitvoeringsregeling voldaan.

Wellicht ten overvloede wordt opgemerkt dat de Kmar, SIOD /FIOD niet als zodanig staan benoemd in artikel 43c lid 1 sub I van de Uitvoeringsregeling. De SIOD wordt weliswaar impliciet genoemd in artikel 43c lid 1 sub x van de Uitvoeringsregeling, dit artikel is echter gericht op samenwerking met interventie teams. Gelet op het feit dat:

- de gegevens in het Regionale samenwerkingsverband worden uitgewisseld met het oog op de integrale aanpak van georganiseerde misdaad, en
- de strekking van art 43c lid 1 sub I Uitvoeringsregeling is dat de Belastingdienst gegevens kan uitwisselen met overheidsinstanties ten behoeve van een effectieve en efficiënte handhaving van overheidsregelingen, en
- de Kmar, SIOD /FIOD beschikken over opsporingsbevoegdheden,

wordt het feit dat art. 43c lid 1 sub I Uitvoeringsregeling de Kmar, SIOD /FIOD niet expliciet benoemt niet als een belemmering gezien om - zonder dat deze partijen als zodanig staan benoemd in artikel 43c lid 1 sub I van de Uitvoeringsregeling - aan hen informatie in het kader van dit convenant te verstrekken.

### Bevoegdheid FIOD-ECD

De FIOD- ECD heeft tot taak het opsporen van feiten die strafbaar zijn gesteld in de belastingwetgeving en de Wet economische delicten. Op grond van artikel 46 Wpg vallen de gegevens die overeenkomstig artikel 10, eerste lid onder a van de Wpg door de FIOD- ECD worden verwerkt, oftewel de zogenaamde CIE- gegevens uit de opsporingsonderzoeken van de FIOD-ECD onder het verstrekkingregime van de Wpg. Dit betekent dat verstrekking van CIE-gegevens van de FIOD - ECD aan het regionale samenwerkingsverband moet voldoen aan de voorwaarden van artikel 20 Wpg. Gegevens die niet als CIE-gegevens kunnen worden gekwalificeerd, vallen onder het regime van de Wbp.

### Bevoegdheid SIOD

De SIOD heeft tot taak het opsporen van feiten die strafbaar zijn gesteld in de wet- en regelgeving op het terrein van werk en inkomen. Op grond van artikel 46 Wpg vallen de gegevens die overeenkomstig artikel 10, eerste lid onder a van de Wpg door de SIOD worden verwerkt, oftewel de zogenaamde CIE- gegevens uit de opsporingsonderzoeken van de SIOD onder het verstrekkingregime van de Wpg. Dit betekent dat verstrekking van CIE-gegevens van de SIOD aan het regionale samenwerkingsverband moet voldoen aan de voorwaarden van artikel 20 Wpg. Gegevens die niet als CIE-gegevens kunnen worden gekwalificeerd, vallen onder het regime van de Wbp.

### Bevoegdheid Koninklijke Marechaussee

De KMar heeft tot taak de opsporing van strafbare feiten, alsmede de handhaving van de openbare orde indien het gaat om de uitvoering van de politietaak overeenkomstig het bepaalde in artikel 6 van de Politiewet 1993. Wat betreft de bevoegdheid van de Kmar om politiegegevens te verstrekken, zie hetgeen hierover is gezegd onder het kopje 'Bevoegdheid politie'.

### Bevoegdheid regionaal samenwerkingsverband

Op grond van artikel 8 sub e Wbp zijn bovengenoemde partijen bevoegd om persoonsgegevens in het regionale samenwerkingsverband te ontvangen. Politie, OM en Belastingdienst zijn eveneens op grond van artikel 22 lid 1 Wbp gerechtigd de gegevens te ontvangen.

De gegevensverwerking binnen het regionale samenwerkingsverband is een verwerking van persoonsgegevens die door de decentrale convenantpartners aan elkaar worden verstrekt. De verwerking van de persoonsgegevens van de decentrale convenantpartners binnen het regionale samenwerkingsverband moet worden beschouwd als een aparte verwerking in de zin van de Wbp. De rechtmatigheidsgrondslag van de verwerking van persoonsgegevens binnen het regionale samenwerkingsverband is artikel 8 sub f Wbp: de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de decentrale convenantpartners die deel uitmaken van het regionale samenwerkingsverband. De verwerking van de persoonsgegevens geschiedt immers ter ondersteuning van hun reguliere werkzaamheden en/of de uitoefening van hun taak. Zonder de gegevensuitwisseling binnen het regionale samenwerkingsverband is een geïntegreerde, effectieve en efficiënte aanpak van de georganiseerde misdaad niet mogelijk.

Het in artikel 8 sub f Wbp vastgelegde noodzakelijkheids criterium dient aldus te worden uitgelegd dat de verwerking van persoonsgegevens dient te worden getoetst aan het beginsel van proportionaliteit en subsidiariteit. Voor de volledigheid is deze toets hieronder opgenomen.

Met de persoonsgegevens die worden verwerkt (zie vraag 5 van de Checklist Wbp, pag. 16) in combinatie met het doel van de verwerking van de persoonsgegevens (zie paragraaf 2 van het Bestuurlijk Akkoord) worden geen onevenredige inbreuken gemaakt op de persoonlijke levenssfeer van de betrokkene (proportionaliteitseis). Het doel van de gegevensverwerking wordt nagestreefd met de minst bezwarende maatregelen voor degenen op wie de persoonsgegevens betrekking hebben (subsidiariteitseis). De persoonsgegevens die voor de aanpak van de georganiseerde misdaad worden verwerkt zijn noodzakelijk, gelet op het doel van de gegevensverwerking.

### Derdeverstrekking

De verstrekking van persoonsgegevens van de decentrale convenantpartners aan derden - zijnde niet- decentrale convenantpartners - is de verantwoordelijkheid van de desbetreffende decentrale convenantpartner zelf. Dit houdt in dat iedere decentrale convenantpartner de verstrekking van de persoonsgegevens zelf dient te toetsen aan de voor hem geldende (specifieke) privacy wet- en regelgeving. Indien deze derdeverstrekking onder het algemene regime van de Wbp valt, zal de decentrale convenantpartner zelf moeten toetsen of deze derdeverstrekking op grond van artikel 9 Wbp verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk worden verwerkt, dan wel of in dit verband een beroep kan worden gedaan op de uitzondering van artikel 43 sub b Wbp. Tevens zal de decentrale convenantpartner op grond van artikel 4 van het Regionale convenant de uitdrukkelijke voorafgaande toestemming van de verstreckende decentrale convenantpartner voor deze derdeverstrekking moeten hebben.

## **2. Doel en doelbinding**

2.1 Het Bestuurlijk Akkoord heeft tot doel de samenwerking tussen decentrale convenantpartners in een regionaal samenwerkingsverband ten behoeve van een geïntegreerde aanpak van georganiseerde misdaad te faciliteren, zowel ten behoeve van de bestuursrechtelijke, strafrechtelijke als fiscale handhaving als om te bevorderen dat factoren of gelegenheidsstructuren die een voedingsbodem (kunnen) creëren van de volgende verschijningsvormen van georganiseerde misdaad worden weggenomen, te weten:

1. mensenhandel;
2. georganiseerde hennepcultuur;
- 3a fraude in de vastgoedsector;

- 3b misbruik binnen de vastgoedsector;
- 4. witwassen en daaraan gerelateerde vormen van financieel-economische criminaliteit;
- 5. een nader te specificeren verschijningsvorm van georganiseerde misdaad die blijkt uit het periodiek opgestelde landelijke nationaal dreigingsbeeld dan wel lokale criminaliteitskaarten of regionale criminaliteitsbeeldanalyses.

Het doel van de geïntegreerde aanpak van georganiseerde misdaad is, naast het strafrechtelijk vervolgen van individuele daders en het ontmantelen van criminele samenwerkingsverbanden, om factoren of gelegenheidsstructuren te identificeren en aan te pakken die voornoemde vormen van criminaliteit faciliteren. Verweving van onder- en bovenwereld moet met kracht worden bestreden door te voorkomen dat criminelen en/of criminele organisaties bewust of onbewust worden gefaciliteerd door de overheid en criminelen en/of criminele organisaties kunnen investeren in de reguliere economie.

Meer specifiek zullen decentrale convenantpartners in dit kader bezien of, en zo ja, op welke wijze, zij, al dan niet in onderlinge samenwerking, binnen de bestaande kaders van de voor hen toepasselijke wet- en regelgeving en opgedragen taak met het oog op de aanpak van de georganiseerde misdaad interventies kunnen plegen gericht op:

- a. het voorkomen, opsporen en vervolgen van strafbare feiten;
- b. het handhaven van de openbare orde en nationale veiligheid;
- c. het uitoefenen van toezicht op de naleving van de regelgeving;
- d. het nemen van een bestuursrechtelijke en/of strafvorderlijke beslissing;
- e. het beëindigen van gevaarlijke situaties;
- f. de bescherming van de goede zeden of de gezondheid;
- g. het voorkomen van wanordelijkheden,

in het geval dat één of meer personen of organisaties vermoedelijk hebben gehandeld of handelen in strijd met de wet- en regelgeving in relatie tot de in dit artikel genoemde vormen van georganiseerde misdaad en waarvan de handhaving is opgedragen aan één of meer van de decentrale convenantpartners in het regionale samenwerkingsverband.

2.2 De decentrale convenantpartners in het regionale samenwerkingsverband beogen de hierboven benoemde doelen op de volgende wijze te bereiken:

- a. Het binnen de kaders van wet- en regelgeving uitwisselen van gegevens en/of informatie die met het oog op de uitoefening van ieders wettelijke taken en het realiseren van ieders wettelijke doelstelling van belang zijn.
- b. Het periodiek adviseren van de decentrale convenantpartners (o.a via de beheersdriehoek) en/of de stuurgroep van het regionale samenwerkingsverband over ontwikkelingen binnen de in het Bestuurlijk akkoord genoemde verschijningsvormen van georganiseerde misdaad.
- c. Het aan de hand van concrete gevallen periodiek adviseren van de decentrale convenantpartners (o.a via de beheersdriehoek) en/of de stuurgroep van het regionale samenwerkingsverband over mogelijke interventiestrategieën.
- d. Het afstemmen en coördineren van mogelijke interventies van decentrale convenantpartners waarbij de bestuurlijke interventiemogelijkheden ten volle worden benut.
- e. Het, waar mogelijk en opportuun, gezamenlijk interveniëren van decentrale convenantpartners.

2.3 Elk van de decentrale convenantpartners geeft in het regionale samenwerkingsverband binnen de kaders van de eigen bevoegdheden en verantwoordelijkheden invulling aan zijn eigen taak, zijnde:

- a. voor de gemeente: het handhaven van de openbare orde, de uitoefening van toezicht op en handhaving van wet- en regelgeving en het uitvoeren van de bestuurlijke aanpak van georganiseerde misdaad;

- b. voor de politie: de handhaving van de openbare orde, opsporing van strafbare feiten en het uitoefenen van toezicht op en handhaving van het naleven van de wet- en regelgeving;
- c. voor het Openbaar Ministerie: de strafrechtelijke handhaving van de rechtsorde, het uitoefenen van het gezag over de opsporing van strafbare feiten, het vervolgen daarvan en het tenuitvoerleggen van opgelegde straffen.
- d. voor de Belastingdienst: het uitvoeren van de Algemene Wet inzake Rijksbelastingen alsmede andere fiscale wet- en regelgeving;
- e. voor de FIOD-ECD: de opsporing van strafbare feiten op grond van de Algemene Wet inzake Rijksbelastingen en de Wet Economische Delicten;
- f. voor de SIOD: het opsporen van feiten die strafbaar zijn gesteld in de wet- en regelgeving op het terrein van werk en inkomen.
- g. voor de KMar: de opsporing van strafbare feiten en de handhaving van de openbare orde indien het gaat om de uitvoering van de politietaak overeenkomstig het bepaalde in artikel 6 van de Politiewet 1993.

2.4 Voor de uitvoering van het Bestuurlijk Akkoord op decentraal niveau wordt voor de formele vastlegging van de afspraken in het regionale samenwerkingsverband gebruik gemaakt van het modelconvenant "*Regionaal Convenant Geïntegreerde Decentrale aanpak Georganiseerde Misdaad*" dat als bijlage aan dit Bestuurlijk Akkoord is gehecht.

2.5 Op decentraal niveau wordt de doelstelling van het regionale samenwerkingsverband gespecificeerd naar de in het Bestuurlijk Akkoord benoemde verschijningsvorm van georganiseerde misdaad.

### **3. Waarborgen**

3.1 Decentrale convenantpartners zullen zowel persoonsgegevens als bijzondere persoonsgegevens zoals strafrechtelijke persoonsgegevens binnen het regionale samenwerkingsverband verwerken. Decentrale convenantpartners kunnen deze persoonsgegevens alleen verwerken indien en zolang dit noodzakelijk is voor het realiseren van de in het Bestuurlijk Akkoord genoemde doelstellingen en voor zover dit nodig is voor de goede vervulling van de aan hen opgedragen taak. Hierbij zullen niet meer gegevens worden verwerkt dan noodzakelijk. De persoonsgegevens zijn gelet op de doeleinden waarvoor ze worden verwerkt toereikend, ter zake dienend en niet bovenmatig.

In de Checklist Wbp, zoals opgenomen in de bijlage van het Regionaal convenant, wordt voor de op decentraal gekozen te bestrijden verschijningsvorm van georganiseerde misdaad de bijbehorende gegevensset vastgelegd. Zie in de Checklist Wbp een voorbeeld van een gegevensset.

3.2 De gegevens worden tevens niet langer bewaard dan noodzakelijk is voor het doel waarvoor ze worden verwerkt. Vernietiging van persoonsgegevens vindt in ieder geval plaats in het geval één of meerdere decentrale convenantpartners besluit(en) dat in het concrete geval niet tot interventie wordt overgegaan.

### **4. Regionale samenwerking**

4.1 Op het moment dat één of meer verschijningsvormen van georganiseerde misdaad op decentraal niveau wordt aangepakt overeenkomstig het bepaalde in het Bestuurlijk Akkoord, ontstaat met ondertekening van het Regionaal convenant een regionaal samenwerkingsverband.

4.2 Het regionale samenwerkingsverband bestaat tenminste uit een stuurgroep.

4.3 Ieder lid van de stuurgroep werkt te allen tijde onder de verantwoordelijkheid van de decentrale convenantpartner die zij in de stuurgroep vertegenwoordigt.

4.4 Iedere decentrale convenantpartner kan worden vertegenwoordigd in de stuurgroep. Deze vertegenwoordiging beschikt over het benodigde mandaat en is bevoegd zijn taak en/of werkzaamheden uit te voeren. De korpsbeheerder is te allen tijde lid van de stuurgroep.

4.5 De burgemeester in de hoedanigheid van regionale korpsbeheerder draagt als decentraal convenantpartner zorg voor de melding van de verwerking van Persoonsgegevens van het regionale samenwerkingsverband bij het College bescherming persoonsgegevens.

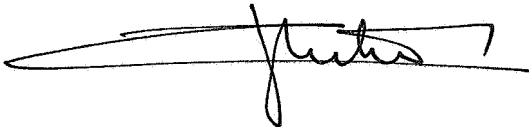
4.6 De stuurgroep geeft richting aan de samenwerking binnen de kaders van het Regionaal convenant. Afbakening kán, bijvoorbeeld door aanwijzing van bepaalde straten/gebieden of van bepaalde branches.

4.7 De taken van de stuurgroep bestaan in ieder geval uit:

- de beleidsmatige sturing gericht op het behalen van de doelstelling van het Bestuurlijk Akkoord;
- het houden van toezicht op het waarborgen van naleving van de in het Bestuurlijk Akkoord en Regionaal convenant opgenomen randvoorwaarden;
- het ontwikkelen van richtlijnen ten aanzien van de besluitvorming over de strafrechtelijke en/of bestuursrechtelijke interventie;
- het toezien op een geregelde evaluatie van de resultaten van het regionale samenwerkingsverband.

4.8 De stuurgroep kan zelf in onderling overleg nadere afspraken maken over de regeling van zijn werkzaamheden en de werkwijze binnen het regionale samenwerkingsverband.

De minister van Binnenlandse Zaken en  
Koninkrijksrelaties,



Mevrouw dr. G. ter Horst

De minister van Justitie,



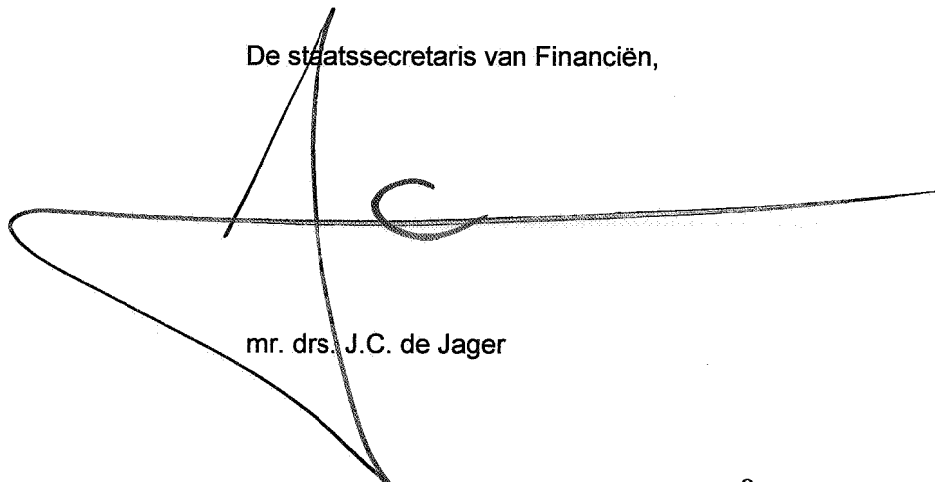
Dr. E.M.H. Hirsch Ballin

De minister van Defensie,



E. van Middelkoop

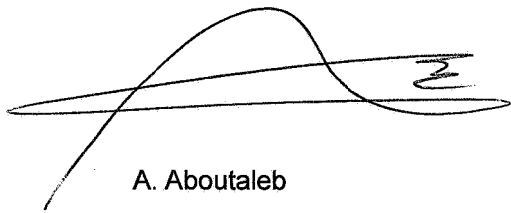
De staatssecretaris van Financiën,



mr. drs. J.C. de Jager

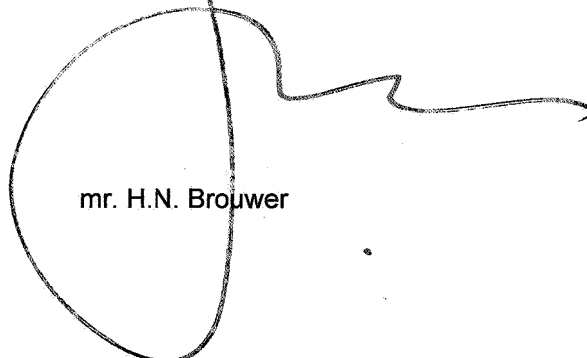


De staatssecretaris van Sociale Zaken en  
Werkgelegenheid,



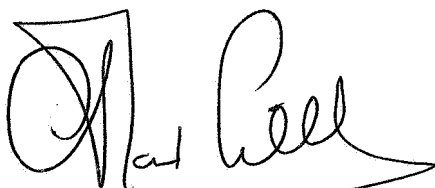
A. Aboutaleb

De voorzitter van het College van procureurs-  
generaal,



mr. H.N. Brouwer

De voorzitter van de Vereniging van Nederlandse  
Gemeenten,



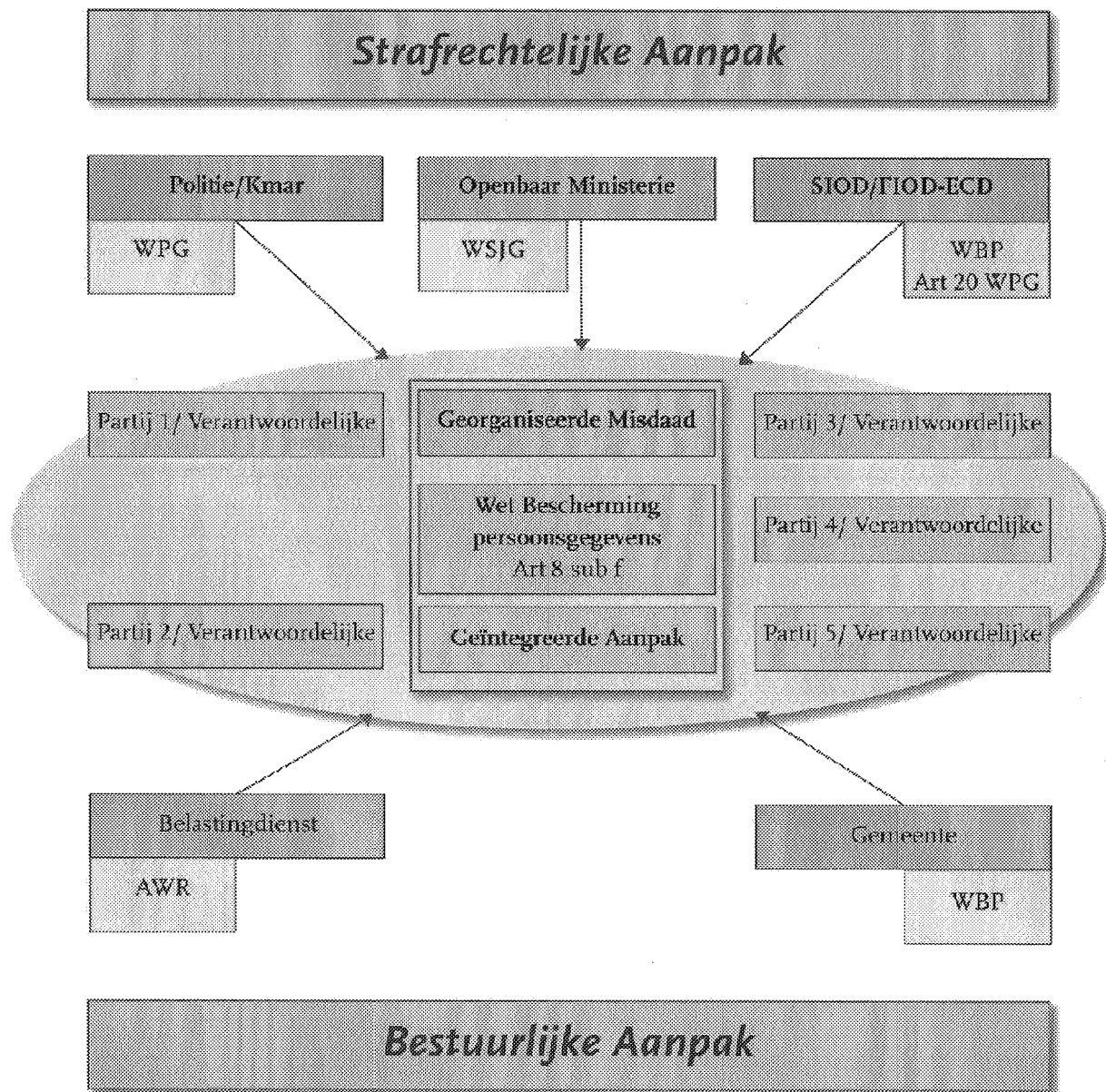
Mevrouw Jorritsma-Lebbink

**Algemene toelichting**  
**op de systematiek van uitwisseling van persoonsgegevens op grond van het Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad (Bestuurlijk Akkoord), inclusief de bijlage zijnde het Regionale Convenant Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad (Regionaal Convenant)**

1. De verstrekking van persoonsgegevens aan een decentrale convenantpartner en/of decentrale convenantpartners in een concreet geval is een verstrekking van persoonsgegevens die moet voldoen aan de voor de verstrekkinge convenantpartijen geldende (specifieke) privacy wet- en regelgeving. Dit houdt in dat alleen de bij het concrete geval betrokken partijen binnen het samenwerkingsverband de persoonsgegevens ontvangen. Voor deze verstrekking is de verstrekkinge convenantpartij zelf verantwoordelijk. Er blijft dan ook altijd een eigen verantwoordelijkheid om in het concrete geval belangen af te wegen en de noodzaak voor de verstrekking te bepalen.
2. De verwerking van de persoonsgegevens van de decentrale convenantpartners binnen het regionale samenwerkingsverband is een aparte verwerking van persoonsgegevens in de zin van de *algemene* privacy wet- en regelgeving: de Wet bescherming persoonsgegevens (Wbp). Binnen het regionale samenwerkingsverband is sprake van een zogenaamde gezamenlijke verantwoordelijkheid voor de verwerking van persoonsgegevens in de zin van de Wbp. Dit betekent dat iedere partij volledig verantwoordelijk is voor diens handelen binnen het samenwerkingsverband. Er worden geen verantwoordelijkheden van een andere decentrale convenantpartner overgenomen. Er is sprake van volledige gelijkwaardigheid van partijen.

*Zie ook het plaatje op volgende pagina*

3. In het Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad (hierna: Bestuurlijk Akkoord) is zowel het juridische kader van de decentrale convenantpartners opgenomen om persoonsgegevens rechtmatig aan een decentrale convenantpartner en/of decentrale convenantpartners te mogen verstrekken, als de juridisch randvoorwaarden die op grond van de Wbp gelden voor een rechtmatige verwerking van deze persoonsgegevens binnen het samenwerkingsverband. Hiermee wordt op een generiek niveau zoveel mogelijk duidelijkheid verschaft met welk doel decentrale convenantpartijen op grond van welke wet- en regelgeving persoonsgegevens kunnen verwerken voor de geïntegreerde aanpak van de in het Bestuurlijk Akkoord opgenomen verschijningsvormen van georganiseerde misdaad.
4. Om ervoor te zorgen dat convenantpartners binnen het regionale samenwerkingsverband overeenkomstig de juridische kaders van de Wbp handelen, is voor deze regionale samenwerkingsverbanden in de bijlage van het Bestuurlijk Akkoord een modelconvenant "*Regionaal convenant Geïntegreerde Decentrale aanpak Georganiseerde Misdaad, Regio....*" (hierna: Regionaal convenant) opgenomen. Door ondertekening van het Regionaal convenant ontstaat een samenwerkingsverband. Dit is van groot belang voor een rechtmatige gegevensuitwisseling. Door het samenwerkingsverband is het mogelijk om op basis van artikel 20 Wet Politiegegevens informatie uit te wisselen. Op het moment dat er op basis van artikel 20 Wet Politiegegevens informatie wordt uitgewisseld, is er géén sprake van "verstrekking ten behoeve van derden" en zal het College Bescherming Persoonsgegevens géén voorafgaand onderzoek instellen.
5. Ter vastlegging en de waarborging van de naleving en de implementatie van de randvoorwaarden van de Wbp is in de bijlage van het Regionale convenant een Checklist Wbp opgenomen. Deze Checklist Wbp biedt tevens handvatten voor de melding van de verwerking van persoonsgegevens binnen het regionale samenwerkingsverband bij het College Bescherming Persoonsgegevens.



## BIJLAGE

### REGIONAAL CONVENANT Geïntegreerde Decentrale Aanpak Georganiseerde Misdad [ REGIO..... ]

- Burgemeester namens het college van B&W, van iedere deelnemende gemeente
- De korpsbeheerder van deelnemende korpsen
- De gedeputeerde, namens GS, van iedere deelnemende provincie
  
- Korpschef regiopolitie van deelnemende korpsen
  
- Hoofd OvJ Arrondissementsparket en/of hoofd OvJ Landelijk Parket en /of hoofd OvJ Functioneel Parket
  
- Belastingdienst regio
  
- FIOD-ECD regio
- SIOD regio
  
- KMar

**hierna afzonderlijk te noemen Decentrale convenantpartner en gezamenlijk te noemen Decentrale convenantpartners**

In beginsel kunnen private organisaties (met een publieke taak) niet deelnemen aan het Regionale samenwerkingsverband. Het driehoeksoverleg vormt de basiscoalitie van het Regionale samenwerkingsverband.

#### ***overwegende dat:***

- I. er signalen zijn dat één of meer vormen van georganiseerde misdaad zoals benoemd in het Bestuurlijk Akkoord Geïntegreerde Decentrale Georganiseerde Misdad (hierna: Bestuurlijk Akkoord) zich op decentraal niveau manifesteren.
- II. Decentrale convenantpartners uitvoering wensen te geven aan het tot stand brengen van een geïntegreerde aanpak van georganiseerde misdaad overeenkomstig en met inachtneming van het bepaalde in het Bestuurlijk Akkoord.
- III. dit Regionale Convenant Geïntegreerde Decentrale Aanpak Georganiseerde Misdad (hierna Regionaal convenant) de formele vastlegging behelst van de afspraken over de coördinatie, samenwerking en informatie-uitwisseling tussen de Decentrale convenantpartners ten behoeve van de geïntegreerde aanpak van de georganiseerde misdaad op decentraal niveau.
- IV. de geïntegreerde aanpak van de georganiseerde misdaad op decentraal niveau niet slechts hoeft plaats te vinden in een bestaande, afgebakende regio zoals 'de politieregio' of 'de veiligheidsregio'.

#### ***komen het volgende overeen:***

## **Artikel 1 Definities en afkortingen**

- 1.1 Betrokkene: degene op wie een persoonsgegeven betrekking heeft.
- 1.2 Bestuurlijk Akkoord: het Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad inclusief bijlage.
- 1.3 Regionaal convenant: het model convenant "*Regionaal Convenant Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad Regio ....*" inclusief bijlage.
- 1.4 Checklist Wbp: "*Checklist Waarborging naleving Wet bescherming persoonsgegevens Regionaal Samenwerkingsverband*" zoals opgenomen in de bijlage van het Regionaal convenant
- 1.5 Decentrale convenantpartners: één of meer betrokken convenantpartners bij het Regionaal convenant.
- 1.6 Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
- 1.7 Bijzondere persoonsgegevens: strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, alsmede een persoonsgegeven betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en het lidmaatschap van een vakvereniging.
- 1.8 Strafrechtelijke persoonsgegevens: strafrechtelijke persoonsgegevens zoals bedoeld in de Wbp en omschreven in de Memorie van Toelichting van de Wbp. Hieruit volgt dat het gaat om 'gegevens in verband met strafbaar gedrag of verwijtbaar gedrag'.
- 1.9 Regionaal samenwerkingsverband: het samenwerkingsverband op decentraal niveau waarvan de formele afspraken met betrekking tot de coördinatie, samenwerking en informatie-uitwisseling in het Regionaal convenant zijn vastgelegd.
- 1.10 Stuurgroep: De verantwoordelijken van het Regionaal samenwerkingsverband, zijnde de ondertekenaars van het Regionaal convenant.
- 1.11 Wbp: Wet bescherming persoonsgegevens
- 1.12 Wpg: Wet politiegegevens.

## **Artikel 2 Doelstelling**

2.1 Decentrale convenantpartners gaan een Regionaal samenwerkingsverband aan met als doel op decentraal niveau invulling te geven aan de volgende in het Bestuurlijk Akkoord geformuleerde doelstellingen: ....**{INVULLEN}**

-  
-

2.2 De Stuurgroep van het Regionale samenwerkingsverband stelt de benodigde set van Persoonsgegevens vast voor de in artikel 2.1 benoemde verschijningsvorm van georganiseerde misdaad en ziet er op toe dat deze gegevensset wordt vastgelegd in de Checklist Wbp.

## **Artikel 3 Randvoorwaarden**

3.1 De uitwisseling van Persoonsgegevens beperkt zich tot die Persoonsgegevens zoals vastgesteld overeenkomstig artikel 2.2 van dit Regionaal convenant.

3.2 Binnen het Regionaal samenwerkingsverband worden nadere afspraken gemaakt ter uitwerking van de wettelijke bepalingen van de Wbp, om een juiste naleving van de Wbp te borgen. Hierbij wordt gebruik gemaakt van de Checklist Wbp.

3.3 Verwerking van de persoonsgegevens binnen het Regionale samenwerkingsverband vindt niet eerder plaats dan na melding hiervan bij het College bescherming persoonsgegevens.

3.4 Met de ondertekening van dit Regionaal convenant neemt de verantwoordelijke in de zin van de Wpg, in overeenstemming met het bevoegde gezag, het besluit overeenkomstig het bepaalde in artikel 20 lid 1 en 2 Wpg en 4.5 van het Besluit politiegegevens, gelet op het feit dat met dit Regionale convenant op de volgende wijze aan de in artikel 20 Wpg gestelde voorwaarden wordt voldaan:

- a. De gegevensverstrekking vindt plaats met het oog op het voorkomen en opsporen van strafbare feiten en/of het handhaven van de openbare orde gelet op voor het (een) doel(einde) zoals opgenomen in het Bestuurlijk Akkoord.
- b. De gegevensverstrekking aan het Regionale samenwerkingsverband is noodzakelijk vanwege een benoemd zwaarwegend algemeen belang zoals opgenomen in het Bestuurlijk Akkoord.
- c. De gegevens die worden verstrekt zijn benoemd en vastgelegd in de Checklist Wbp met inachtneming van de voorwaarden zoals opgenomen van het Bestuurlijk Akkoord .
- d. De gegevens worden in principe alleen aan de bij het concrete geval betrokken Decentrale convenantpartner verstrekt. Verstrekking aan een niet bij het concrete geval betrokken Decentrale convenantpartner of aan een niet- convenantpartner (derden) vindt plaats overeenkomstig het bepaalde in artikel 4.2.

In dit artikel wordt expliciet gesproken over de verantwoordelijke in de zin van de Wpg, aangezien in het geval het om gegevens van de politie gaat, de korpsbeheerder verantwoordelijke is in de zin van de Wpg. In het geval het om gegevens van de Kmar gaat is de Minister van Defensie verantwoordelijk in de zin van de Wpg en zal derhalve het besluit overeenkomstig art. 20 lid 1 en 2 Wpg moeten nemen. Zie voor de invulling van het begrip 'verantwoordelijke' artikel 1 sub f Wpg.

*Let op!* De verantwoordelijke in de zin van de Wpg zal - in overeenstemming met het bevoegde gezag - te allen tijde voor zichzelf moeten onderbouwen dat inderdaad een zwaarwegend algemeen belang wordt gediend met het oog waarop de verstrekking van politiegegevens in dit verband noodzakelijk is.

Wellicht ten overvloede wordt opgemerkt dat het de verantwoordelijkheid van de partij die onder het regime van de Wpg valt, ervoor waakt dat politiegegevens overeenkomstig het bepaalde in art 20 Wpg jo art. 4.5 Besluit politiegegevens aan het Regionale samenwerkingsverband worden verstrekt. De beslissing van het bevoegd gezag voor gegevensverstrekking op grond van artikel 20 Wpg dient ook inzicht te bieden om welke gegevens het gaat. Het uitgangspunt van de in de Checklist Wbp op te nemen gegevensset is dat het hier geen politiegegevens betreft in de zin van de in artikel 4.5 Besluit politiegegevens benoemde gegevens: de politiegegevens in de zin van artikel 9 en 10 Wpg.

3.5 Met de ondertekening van dit Regionale convenant zeggen de Decentrale conventpartners toe ervoor te waken dat de verwerking van Persoonsgegevens door de Decentrale convenantpartners plaatsvindt in overeenstemming met de wettelijke kaders.

Per regio kunnen zowel de Decentrale convenantpartners als de doelstelling bij het Regionaal convenant verschillen. Ieder Regionaal samenwerkingsverband is zelf verantwoordelijk voor de naleving van de privacy wet- en regelgeving en zal hiervan ook zelf bij het Cbp melding moeten doen. Om de Regionale samenwerkingsverbanden zoveel mogelijk tegemoet te komen is in de bijlage een Checklist Wbp opgenomen die handvatten biedt om per regio vast te leggen op welke wijze de naleving van de Wbp wordt gewaarborgd. Deze checklist Wbp kan ook worden gebruikt voor de melding van de verwerking van de persoonsgegevens bij het Cbp. Indien gewenst kan het RIEC het Regionaal samenwerkingsverband ondersteunen en/of adviseren bij het zorg dragen van de naleving van de Wbp.

#### **Artikel 4           Geheimhouding en beveiliging**

4.1 Decentrale convenantpartners zijn verplicht tot geheimhouding van de in het kader van dit Regionaal convenant ontvangen gegevens, over elkaars organisatie en over al hetgeen waarvan

redelijkerwijs is aan te nemen dat bekendmaking daarvan de belangen van de andere Decentrale convenantpartner zou schaden, behoudens voor zover de uitvoering van de taak met het oog waarop de gegevens zijn verkregen tot het ter kennis brengen daarvan noodzaakt.

4.2 Decentrale convenantpartners verbinden zich jegens elkaar om informatie die zij hebben ontvangen niet zonder uitdrukkelijke voorafgaande toestemming van de verstreckende Decentrale convenantpartner en met inachtneming van het in het Bestuurlijk akkoord opgenomen juridische kader door te verstrekken aan een andere Decentrale convenantpartner en/of niet- convenantpartner (derden).

4.3 Decentrale convenantpartners verplichten zich jegens elkaar om passende technische en organisatorische maatregelen te treffen ter beveiliging van de gegevens tegen verlies of tegen enige vorm van onrechtmatige verwerking, alsmede om de informatie strikt vertrouwelijk en met gepaste geheimhouding te behandelen.

## **Artikel 5 Veiligheidsaspecten**

5.1 Indien één of meer Decentrale convenantpartners op grond van het Regionale convenant handhavingsactiviteiten ondernemen, draagt de regiopolitie die deelneemt aan het Regionale samenwerkingsverband er waar nodig zorg voor dat voldoende capaciteit beschikbaar is voor de sterke-armfunctie, zodat de Decentrale convenantpartners hun werkzaamheden veilig en ongestoord kunnen verrichten. Decentrale convenantpartners stemmen hun activiteiten waar zij verwachten de sterke-arm functie nodig te hebben ruim van te voren af en geven de regiopolitie die deelneemt aan het Regionale samenwerkingsverband voldoende gelegenheid om voor verantwoorde planning van de te verrichten werkzaamheden zorg te dragen.

5.2 Bij het beletten en/of belemmeren van ambtshandelingen, het plegen van wederspanning en bij strafbare feiten (o.a. mishandeling, bedreiging en vernieling) tegen de persoonlijke integriteit van één of meer medewerkers van een Decentrale convenantpartner die werkzaamheden verricht op grond van het Regionaal convenant, voert de regiopolitie die deelneemt aan het Regionale samenwerkingsverband een opsporingsonderzoek uit en wordt zo mogelijk proces-verbaal opmaken tegen de daders. Het Openbaar Ministerie van het Arrondissement dat deelneemt aan het Regionale samenwerkingsverband gaat afhankelijk van de resultaten van het opsporingsonderzoek in beginsel over tot vervolging van de strafbare feiten.

5.3 Decentrale convenantpartners bevorderen dat hun medewerkers die met één van de in het voorgaande lid genoemde strafbare feiten worden geconfronteerd worden geacht daarvan aangifte doen bij de politie. Daarbij kiest een medewerker domicilie van de Decentrale convenantpartner.

## **Artikel 6 Inwerkingtreding, opzegging en beëindiging**

6.1 Het Regionaal convenant treedt in werking op dag dat de laatste Decentrale convenantpartner het heeft ondertekend en eindigt per 1 januari 2012. Het staat de Decentrale convenantpartners vrij in gezamenlijkheid de looptijd van het Regionaal convenant te verlengen.

6.2 Elk van de Decentrale convenantpartners kan het Regionaal convenant met inachtneming van een opzegtermijn van 6 maanden opzeggen, tenzij alle Decentrale convenantpartners instemmen met directe opzegging.

6.3 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindigingen van het Regionaal convenant voort te duren, blijven na beëindiging van het Regionaal convenant bestaan. Tot deze verplichting behoort in ieder geval het bepaalde omtrent geheimhouding in artikel 4 van het Regionaal convenant.

## **Artikel 7 Toetreding**

7.1 Het Regionaal convenant staat open voor toetreding door elke overheidsinstelling die de in het Bestuurlijk Akkoord en Regionaal convenant geformuleerde doelstellingen nastreeft en gerechtigd is tot informatie-uitwisseling binnen de gestelde wettelijke kaders.

7.2 Een organisatie die tot het Regionaal convenant wil toetreden, kan daartoe een aanvraag indienen bij de voorzitter van de Stuurgroep van het Regionale samenwerkingsverband.

7.3 De voorzitter van de Stuurgroep voor het Regionale samenwerkingsverband legt een verzoek tot toetreding van een andere overheidsinstelling voor aan de Decentrale convenantpartners. Een verzoek tot toetreding wordt alleen gehonoreerd na instemming van alle Decentrale convenantpartners. Indien de Decentrale convenantpartners toetreding door een andere overheidsinstelling goedkeuren, vindt toetreding tot het Regionaal convenant plaats door middel van ondertekening van een bijlage bij dit Regionaal convenant door die andere overheidsinstelling.

#### **Artikel 8 Kosten**

8.1 De kosten en benodigde inzet van middelen ter uitvoering van het Regionaal convenant wordt door iedere Decentrale convenantpartner zelf gedragen.

#### **Artikel 9 Aanpassingen en wijzigingen**

9.1 Waar nodig maken Decentrale convenantpartners nadere afspraken om een goede uitvoering van het Regionaal convenant te verzekeren.

9.2 Het Regionaal convenant kan slechts worden gewijzigd indien alle Decentrale convenantpartners hiermee schriftelijk instemmen.

#### **Artikel 10 Geschillen**

10.1 Het Regionaal convenant is niet in rechte afdwingbaar met uitzondering van de in artikel 4 opgenomen geheimhoudingsbepaling voor de Decentrale convenantpartners.

#### **Artikel 11 Evaluatie**

11.1 Het Regionaal convenant zal uiterlijk in 2011 ten behoeve van de geïntegreerde decentrale aanpak van georganiseerde misdaad worden geëvalueerd en worden herzien indien de evaluatie uitwijst dat het aanpassing behoeft. Deze evaluatie dient tevens als input voor een evaluatie op landelijk niveau van de decentrale geïntegreerde aanpak van georganiseerde misdaad.

*Aldus overeengekomen te ..... op .....,*

**Organisatie**

**Bevoegde functionaris**

**Ondertekening**

---



## BIJLAGE

### **Checklist Waarborging naleving Wet bescherming persoonsgegevens Regionaal samenwerkingsverband**

Personen en organisaties die persoonsgegevens verwerken dienen zich te houden aan de normen die de Wet bescherming persoonsgegevens daaraan stelt. Deze checklist heeft tot doel vast te leggen op welke wijze het Regionale samenwerkingsverband de waarborgen van de Wbp naleeft. Voor zover mogelijk is deze checklist al ingevuld. Binnen het Regionale samenwerkingsverband zal deze checklist aan de regionale situatie moeten worden aangevuld en/of aangepast.

Onderhavige checklist kan tevens worden gebruikt voor de melding van de gegevensverwerking binnen het Regionale samenwerkingsverband aan het Cbp. De antwoorden op de vragen uit de checklist die zijn gemarkeerd met (\*M) kunnen worden gebruikt voor deze melding.

#### **Vraag 1      Verantwoordelijke (\*M)**

Wie stelt het doel en de middelen vast van de gegevensverwerking en is derhalve verantwoordelijk voor de verwerking van persoonsgegevens?

#### **Antwoord**

Ten aanzien van de verwerking van persoonsgegevens binnen het Regionale samenwerkingsverband is sprake van een zogenaamde gezamenlijke verantwoordelijkheid in de zin van de Wbp. Alle Decentrale convenantpartners zijn er zelf voor verantwoordelijk dat de gegevensuitwisseling binnen het Regionale samenwerkingsverband noodzakelijk is ten behoeve van de uitoefening van hun taak. Ten behoeve van deze samenwerking draagt iedere Decentrale convenantpartner zelf de hiervoor benodigde kosten.

Voor de melding van de verwerking van persoonsgegevens bij het Cbp betekent deze gezamenlijke verantwoordelijkheid dat *alle* Decentrale convenantpartners in de melding moeten worden opgenomen. Aangezien de regionale samenwerkingsverbanden veelal op initiatief van de burgemeester/ korpsbeheerder van de grond komen, is in artikel 4 van het Bestuurlijk Akkoord opgenomen dat hij de meest aangewezen persoon is om er op toe te zien dat de gegevensverwerking van het regionale samenwerkingsverband wordt gemeld bij het Cbp. Iemand moet deze melding immers verzorgen.

De verantwoordelijke in de zin van de Wbp is "de natuurlijke persoon, rechtspersonen of ieder ander die of het bestuursorgaan dat, allen of tezamen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt". Zie artikel 1 sub d Wbp.

De gezamenlijke verantwoordelijkheid van de Decentrale convenantpartners ten behoeve van de verwerking van persoonsgegevens binnen het Regionale samenwerkingsverband kan als volgt worden omschreven. De verwerkingen van persoonsgegevens van de Decentrale convenantpartners worden binnen het Regionale samenwerkingsverband verwerkt zonder dat er hiervoor een gemeenschappelijke verantwoordelijke is. Iedere Decentrale convenantpartner blijft immers verantwoordelijk voor het inbrengen van de persoonsgegevens - die binnen zijn organisatie worden verwerkt - in het Regionale samenwerkingsverband. Er is hiermee sprake van een afzonderlijke verantwoordelijke per deelverwerking. De betrokkene kan slechts één van de afzonderlijke verantwoordelijken aanspreken.

#### **Vraag 2      Doel van de verwerking (\*M)**

Wat is het doel of zijn de doeleinden voor de verwerking?

#### **Antwoord**

<< Invullen >>

Het Regionale samenwerkingsverband maakt hier een keuze voor de decentrale situatie binnen de doelomschrijving en kaders van artikel 2 van het Bestuurlijk Akkoord en zoals gespecificeerd in artikel 2.1 van het Regionaal convenant.

**Vraag 3      Rechtmatigheidsgrondslag**

Wat is de rechtmatigheidsgrondslag voor de verwerking van persoonsgegevens?

**Antwoord**

De rechtmatigheidsgrondslag voor de verwerking van de gegevens binnen het Regionale samenwerkingsverband is artikel 8 sub f Wbp. Zie ook het juridisch kader in het Bestuurlijk Akkoord onder het kopje "Bevoegdheid Regionaal samenwerkingsverband".

**Vraag 4      Betrokkene(n) (\*M)**

Van welke personen of categorieën van personen worden er gegevens verwerkt?

**Antwoord**

Personen die in een concreet geval onderwerp van onderzoek zijn van het Regionale samenwerkingsverband.

Let op. Zowel het Bestuurlijk Akkoord als het Regionaal convenant hebben betrekking op het naleven van de privacy wet- en regelgeving voor de verwerking van Persoonsgegevens in het kader van de aanpak van de georganiseerde misdaad op decentraal niveau. Dit is een verwerking van persoonsgegevens van het zogenaamde primaire bedrijfsproces van het Regionale samenwerkingsverband. Voor de zogenaamde secundaire bedrijfsprocessen van dit Regionale samenwerkingsverband, zoals het autorisatiebestand van medewerkers, zullen waarschijnlijk ook Persoonsgegevens worden verwerkt. Ook voor deze secundaire verwerkingen zullen de waarborgen van de Wbp moeten worden nageleefd. Voor ondersteuning en/ of advies bij de inrichting van de naleving de Wbp voor deze secundaire bedrijfsprocessen kan een beroep worden gedaan op het RIEC.

**Vraag 5      Gegevensset (\*M)**

Welke persoonsgegevens worden verwerkt?

**Antwoord**

--- << Invullen >>

.....

.....

***Een voorbeeld van persoonsgegevens die in Limburg Zuid worden verwerkt voor de aanpak van vastgoedfraude:***

**Algemene persoonsgegevens**

1. naam, adres en woonplaats
2. datum inschrijving GBA
3. geboortegegevens.
4. burgerlijke staat.
5. gegevens omtrent woonsituatie.
  - a. soort perceel (bestemming)
  - b. WOZ-waarde
  - c. aangevraagde vergunningen (milieu, bouw, drank & horeca)
  - d. aanwezigheid eventuele huurders
6. gegevens aangaande aankopen en verkopen van panden over een periode van 3 jaar of langer.
7. ondernomen (bestuurlijke) handhavingsacties
8. hypothecaire gegevens
  - a. inschrijving hypotheek
  - b. hypotheekhouder
9. openbare gegevens kadaster.

- a. Kadasternummer
  - b. kadastrale aanduiding
  - c. betrokken recht:
  - d. toestandsdatum:
  - e. historie
10. gegevens van rechtspersonen waarbij de genoemde personen betrokken zijn en die panden in eigendom kunnen hebben.
11. openbare gegevenshandelsregister
- a. handelsregister
  - b. inschrijvingsnummer
12. fiscale gegevens

**Vraag 6 Gegevensset (\*M)**

Worden er bijzondere persoonsgegevens verwerkt?

Zo ja welke?

**Antwoord**

Ja, Strafrechtelijke persoonsgegevens zoals:

-... << Invullen >>

-.....

-.....

**Een voorbeeld van Bijzondere persoonsgegevens die in Limburg Zuid worden verwerkt voor de aanpak van vastgoedfraude:**

1. gegevens ten aanzien van strafbare feiten de volgende Strafrechtelijke persoonsgegevens:
  - a. lijst van incidenten
  - b. periode incident
  - c. locatie van het incident
2. sofi-nummer voor zover dit onvermijdelijk kan zijn vermeld op documenten die noodzakelijkerwijs ter beschikking zijn gekomen zoals kopieën van identiteitsbewijzen en voor het overige alleen in incidentele en op voorhand onvoorzienbare situaties. In Limburg Zuid wordt het SOFI/Burgerservicenummer verkregen via de GBA en wordt dit bij de informatiebevraging uitgezet naar met name SIOD en de Belastingdienst omdat zijn hun bevraging binnen hun systemen voornamelijk doen aan de hand van deze nummers.
3. Overig:
 

Door de Betrokkene zelf verstrekte gegevens die in relatie tot de doelstellingen van de regionale samenwerking van belang zijn zoals VOG/Verkl. Belastingdienst/Uittreksel Bevolkingsregister/ Geboorteakte/ Huwelijksakte.

**Algemeen.** Gelet op het doel (zie ook vraag 2 van de Checklist Wbp), moet voor de beantwoording van vraag 5 en 6 de bijbehorende gegevensset van persoonsgegevens en bijzondere persoonsgegevens worden opgenomen voor de door het Regionale samenwerkingsverband op te pakken verschijningsvorm van georganiseerde misdaad. De te verwerken persoonsgegevens moeten juist, nauwkeurig, niet bovenmatig en noodzakelijk zijn voor het door Regionale samenwerkingsverband op te pakken verschijningsvorm van georganiseerde misdaad zoals omschreven in vraag 2 van de checklist Wbp. De verwerking van bijzondere persoonsgegevens, zoals de strafrechtelijke persoonsgegevens moet specifiek zijn toegestaan op grond van de Wbp. De verwerking van strafrechtelijke persoonsgegevens binnen het Regionaal samenwerkingsverband is toegestaan op grond van artikel 22 lid 1 Wbp.

**Vraag 7 Ontvangers (\*M)**

Wie zijn de ontvangers van de persoonsgegevens?

**Antwoord**

- de leden van de stuurgroep
- de door hen aangewezen deelnemers aan het samenwerkingsverband

**Vraag 8 Verstrekking buiten EU (\*M)**

Worden gegevens doorgegeven naar landen buiten de Europese Unie of is er een voornemen daartoe?

Zo ja:

- om welke gegevens gaat het?
- om welke landen gaat het?

**Antwoord**

Nee

**Vraag 9 Beveiliging (\*M)**

Op welke wijze zijn de persoonsgegevens beveiligd en waar is dat terug te vinden?

**Antwoord**

<< In te vullen door het Regionale samenwerkingsverband >>

Een security-officer zal een risicoanalyse moeten uitvoeren en op basis hiervan een beveiligingsplan moeten opstellen + zorg dragen voor de implementatie en de naleving van de beveiligingsmaatregelen.

*Persoonsgegevens dienen te worden beveiligd door passende technische en organisatorische maatregelen. Hierbij kan gebruik worden gemaakt van het rapport "Beveiliging van persoonsgegevens, Achtergrondstudies en Verkenningen, nummer 23" van het College Bescherming persoonsgegevens. Dit rapport onderscheidt hiervoor de volgende stappen:*

*I Stel de aard, de omvang en het gebruik van de persoonsgegevens vast.*

*De vaststelling van de aard van de gegevens heeft betrekking op de vraag hoe privacygevoelig de gegevens zijn voor betrokkene. De vaststelling van de omvang en het gebruik van de gegevens wordt bepaald door te kijken naar het doel van de verwerking en de hoeveelheid persoonsgegevens die worden verwerkt.*

*II Inventariseer de mogelijke vormen van onbevoegde en onzorgvuldige verwerking.*

*Deze risicoanalyse heeft tot doel reële vormen van verlies, aantasting en onbevoegde kennisneming, wijziging of verstrekking van de verwerking van de persoonsgegevens te inventariseren.*

*III Bepaal de risicoklasse.*

*Onderstaand schema is een vereenvoudigde weergave van het schema dat het Cbp in haar rapport hanteert om de onderlinge relatie tussen de risicoklassen weer te geven.*

Hoeveelheid persoonsgegevens	Persoonsgegevens	Bijzondere persoonsgegevens	Financiële en/of economische persoonsgegevens
Weinig persoonsgegevens	<b>Risicoklasse 0</b>	<b>Risicoklasse II</b>	<b>Risicoklasse II</b>
Veel persoonsgegevens	<b>Risicoklasse I</b>	<b>Risicoklasse III</b>	

*IV Bepaal de noodzakelijke te nemen beveiligingsmaatregelen*

*Het rapport van het Cbp biedt handvatten voor de per risicoklasse te nemen beveiligingsmaatregelen*

*Wellicht ten overvloede verdient het aanbeveling de risicoanalyse op grond van de Wbp (en de te nemen beveiligingsmaatregelen) onderdeel uit te laten uitmaken van de risicoanalyse en beveiligingsmaatregelen ten behoeve van de naleving van het algemene informatiebeveiligingsbeleid.*

Een voorbeeld van een organisatorische beveiligingsmaatregel is een autorisatiebesluit en/of procedure waarin wordt vastgelegd wie wanneer toegang heeft tot welke gegevens. De toegang zal bijvoorbeeld moeten worden beperkt tot degenen die de gegevens nodig hebben voor de uitoefening van hun taak/werkzaamheden, een ieder die gegevens ontvangt heeft een ambtshalve geheimhoudingsplicht en/of beschikt over een (A) screening + de geheimhoudingsbepaling in het Regionale convenant.

**Vraag 10      Bewerker (\*M)**

Is er een bewerker?

Zo ja, is er met de bewerker een bewerkersovereenkomst afgesloten?

**Antwoord**

Nee.

In art. 1 sub e Wbp wordt onder een bewerker verstaan: *degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen*. Gelet op de privacygevoeligheid van de gegevens die binnen het Regionale samenwerkingsverband worden verwerkt, is het uitgangspunt dat het beheer hiervan intern wordt geregeld.

Indien het wenselijk blijkt dat toch een bewerker wordt ingeschakeld kan hiervoor bijvoorbeeld door het RIEC een modelbewerkersovereenkomst worden opgesteld die de Regionale samenwerkingsverbanden kunnen gebruiken.

**Vraag 11      Herkomst**

Wat is de herkomst van de gegevens?

**Antwoord**

De gegevens zijn afkomstig van de Decentrale convenantpartners.

Het verdient aanbeveling om de herkomst van de persoonsgegevens vast te leggen indien in het concrete geval blijkt dat de Betrokkene niet hoeft te worden geïnformeerd over de verwerking van zijn persoonsgegevens als gevolg van het feit een beroep kan worden gedaan op een uitzondering van de informatieplicht op grond van artikel 43 of 34 lid 4 van de Wbp. In dat geval dient namelijk in ieder geval de herkomst van de gegevens te zijn vastgelegd. Met een grote mate van waarschijnlijkheid zal binnen het Regionale samenwerkingsverband een beroep kunnen worden gedaan op de uitzondering zoals opgenomen in artikel 43 Wbp. De herkomst van de gegevens zal dan ook moeten worden vastgelegd. Zie ook hetgeen hierover wordt opgemerkt bij vraag 13.

**Vraag 12      Bewaartermijn**

Wat is de bewaartermijn voor de verwerking van persoonsgegevens?

**Antwoord**

De persoonsgegevens worden in ieder geval vernietigd als:

1. binnen het Regionale samenwerkingsverband wordt besloten niet tot interventie over te gaan;
2. een verdenking onterecht op een verdachte was gericht;
3. de gedraging in het concrete geval niet is te kwalificeren als een strafbaar feit;
4. ....
5. ....

Het gaat om een valide beargumentering waarom een bepaalde bewaartermijn – gelet op het doel van de verwerking - noodzakelijk is.

### **Vraag 13 Informatieverstrekking**

Worden de betrokkenen geïnformeerd over de verwerking van hun persoonsgegevens?

Zo ja, hoe?

Zo nee, waarom niet?

#### **Antwoord**

Ja, tenzij in het concrete geval een beroep kan worden gedaan op één van de uitzonderingen op de informatieplicht.

De verwerking van persoonsgegevens in het Regionale samenwerkingsverband heeft als doel de aanpak van georganiseerde misdaad zoals verwoord in het Bestuurlijk Akkoord. De gegevens zijn afkomstig van de Decentrale convenantpartners (art. 34 Wbp). Ten aanzien van deze verstrekking is het waarschijnlijk dat in bijna alle gevallen een beroep kan worden gedaan op de uitzondering van de plicht tot informatieverstrekking op grond van artikel 43 sub b of d Wbp (zie kader hieronder). Per concreet geval zal echter moeten worden bekeken of inderdaad een beroep op (één van) deze uitzonderingsgronden kan worden gedaan.

#### **Publicatie Regionaal convenant**

Om ervoor te zorgen dat personen en organisaties binnen de regio in ieder geval weet hebben van de gegevensuitwisseling in het kader van het Regionale samenwerkingsverband kunnen bijvoorbeeld op regionaal niveau tenminste de volgende maatregelen worden genomen:

- informatieverstrekking over de samenwerking in een (aantal) regiona(a)l(e) dagblad(en).
- informatieverstrekking over de samenwerking op de website van de Decentrale convenantpartners

In principe moet een Betrokkene te allen tijde actief worden geïnformeerd over:

- welke persoonsgegevens met welk doel worden verwerkt;
- wie hiervoor verantwoordelijk is;
- of er sprake is van derdeverstrekking;
- de rechten (inzage, correctie en verzet) die hij tegen de verwerking kan uitoefenen, alsmede bij wie hij deze rechten kan uitoefenen.

Slechts in een aantal gevallen kan een uitzondering op deze informatieplicht worden gemaakt. De informatieplicht kan slechts achterwege blijven in de volgende gevallen (art. 34 en 43 Wbp):

1. de betrokkene is al op de hoogte van de verwerking (34 lid 1 Wbp);
2. de informatieverstrekking blijkt onmogelijk of kost een onevenredige inspanning (34 lid 4 Wbp);
3. de verwerking vindt plaats in het kader van de voorkoming, opsporing en vervolging van strafbare feiten (43 sub b Wbp)
4. de verwerking vindt plaats ten behoeve van het toezicht op de naleving van de van de wettelijke voorschriften die zijn gesteld ten behoeve het bepaalde onder 3. (43 sub d Wbp)

#### **Vraag 14 Voorafgaand onderzoek (\*M)**

Is een zogenaamd voorafgaand onderzoek door het Cbp vereist?

##### **Antwoord**

Nee, er is geen voorafgaand onderzoek door het Cbp vereist als het Regionale samenwerkingsverband basis van het Bestuurlijke Akkoord en het Regionaal convenant vorm krijgt want:

1. In het Regionaal samenwerkingsverband worden geen nummers ter identificatie van een persoon verwerkt - met als doel een koppeling met andere bestanden tot stand te brengen - zoals bedoeld in artikel 31 lid 1 sub a Wbp. Het Sofi/BSN nummer worden slechts dan verwerkt indien deze noodzakelijkerwijs ter beschikking zijn gekomen zoals kopieën van identiteitsbewijzen en voor het overige alleen in incidentele en op voorhand onvoorzienbare situaties. (Zie ook vraag 5 van de checklist Wbp ).
2. Binnen het Regionale samenwerkingsverband is geen sprake van zogenaamde heimelijke waarneming zoals opgenomen in artikel 31 lid 1 sub b Wbp.
3. Gelet op het feit dat de verwerking van gegevens binnen het Regionale samenwerkingsverband is gebaseerd op artikel 20 Wpg, is er geen sprake van verwerking van strafrechtelijke persoonsgegevens ten behoeve van derden zoals verwoord in artikel 31 lid 1 sub c Wbp. Derden zijn in dit geval partijen die geen Decentrale convenantpartner zijn.

Over vorenstaande lijn - dat er geen voorafgaand onderzoek door het Cbp hoeft plaats te vinden - heeft informeel afstemming plaats gevonden tussen het ministerie van BZK en het Cbp.

#### **Vraag 15 Melding Cbp**

Is het Vrijstellingsbesluit van toepassing op de verwerking?

Zo ja, op grond van welk artikel is de verwerking vrijgesteld van melding bij het Cbp of de functionaris van gegevensbescherming?

##### **Antwoord**

Nee, de verwerking is niet vrijgesteld van melding. Er is sprake van meerdere verantwoordelijken in de zin van de Wbp. In dat geval moet een verwerking altijd worden gemeld bij het Cbp.

#### **Vraag 16 Contact Cbp (\*M)**

a) Wie is de contactpersoon voor de melding bij het Cbp

b) Wat is het meldingsnummer van het Cbp

##### **Antwoord**

- a) Invullen bij melding
- b) Kan pas worden opgenomen nadat de verwerking is gemeld en een meldingsnummer van het Cbp is ontvangen.