# Juridisch kader gegevensverwerking

Horend bij: Werkproces integrale aanpak problematische jeugdgroepen en groepsgedrag

Opgesteld in samenwerking met gemeenten, politie en OM

*Versie 1.0*

| | | |
|---|---|---|
| Titel | : | Juridisch kader gegevensverwerking<br>Horend bij: Werkproces integrale aanpak problematische jeugdgroepen en groepsgedrag |
| Datum | : | 31 maart 2016 |
| Versie | : | 1.0 |
| Status | : | Definitief |
| Opgesteld door | : | Landelijk projectteam proeftuinen in samenwerking met aanvullende (externe juridische) deskundigen |
| Contactpersonen | : | Bernd Wondergem<br>Portefeuille Integrale aanpak kindermishandeling en jeugdgroepen<br>Ministerie van Veiligheid en Justitie |

# Inhoudsopgave

1 INLEIDING 2
1.1 Status en beheer 2
1.2 Logica van de privacywetgeving 2
1.3 Persoonsgegevens 3

2 DE SAMENWERKING: ROLLEN EN VERANTWOORDELIJKHEDEN 5
2.1 Juridische basis voor de samenwerking 5
2.2 Inrichting van de samenwerking 5
2.3 De uitvoeringscoördinator 6
2.4 De rol van de gemeente 7

3 DOEL EN GRONDSLAGEN WBP 9
3.2 Persoonsgegevens delen met partners (stap 2 en verder in het werkproces) 11
3.3 Overige Wbp eisen 12

# 1 Inleiding

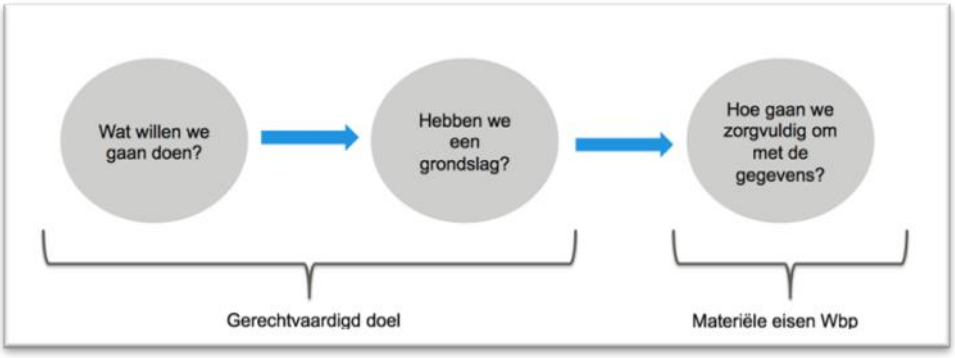
## 1.1 Status en beheer

Binnen het werkproces Integrale Aanpak Problematische Jeugdgroepen en Groepsgedrag (hierna: het werkproces) worden persoonsgegevens verzameld, gedeeld en gebruikt door samenwerkende partners (de partners). Dit document bevat een kader met achtergrondinformatie over de privacywetgeving die relevant is voor de beoordeling van privacyvraagstukken die zich voor kunnen doen in de context van gegevensverwerking in dat werkproces.

## 1.2 Logica van de privacywetgeving

De Wet bescherming persoonsgegevens (Wbp) bepaalt dat persoonsgegevens alleen mogen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.[1] Een doel is pas gerechtvaardigd als er een grondslag in artikel 8 van de Wbp is waarop de verwerking kan worden gebaseerd (zie verder paragraaf 1.5).

Als er eenmaal een gerechtvaardigd doel is dan moeten de gegevens voor dit doel zorgvuldig worden verwerkt, hiertoe stelt de privacywetgeving allerlei materiële eisen zoals beveiliging, informatieplichten, invulling geven aan de rechten van de betrokkenen enzovoorts. Schematisch kan de Wbp dan als volgt worden weergegeven:




In veruit de meeste gevallen wordt het gerechtvaardigd doel bedacht door de partij die de gegevens wil gaan verwerken voor dat doel (de verantwoordelijke). Echter, partijen kunnen ook samenwerken aan één gemeenschappelijk doel er is dan sprake van een samenwerkingsverband waarbinnen de verantwoordelijkheid specifiek moet worden belegd (zie paragraaf 1.4).

[1] Voor de politie geldt de Wet politiegegevens, voor partijen binnen de strafrechtspleging geldt de Wet Justitiële en Strafvorderlijke gegevens.

## 1.3 Persoonsgegevens

De Wbp is alleen van toepassing wanneer sprake is van verwerking van persoonsgegevens. Persoonsgegevens zijn gegevens die "een natuurlijk persoon identificeren of aan de hand waarvan een natuurlijke persoon geïdentificeerd kan worden"[2].

Gegevens die géén betrekking hebben op een geïdentificeerd of identificeerbaar persoon vallen buiten het bereik van de privacywetgeving. Wanneer gegevens over de (jeugd)groep als geheel worden verwerkt, dan zijn de regels van de Wbp en aanverwante wetgeving dus niet van toepassing. Deze gegevens mogen vrij worden gedeeld. Wanneer het echter gaat over individuele leden van de groep, dan zijn alle privacyregels van toepassing. Bijvoorbeeld:

*"In de Merenwijk is een groep van ongeveer 12 jongens en 4 meisjes actief. De groep hangt rond, kent één leider en maakt zich schuldig aan kleine criminaliteit"*

→ géén verwerking persoonsgegevens.

*"Jan Willemsen is de leider van de Merenwijk groep, hij heeft een strafblad en vertoont agressief gedrag"*

→ verwerking persoonsgegevens

Met name in stap 1 van het werkproces worden nog geen persoonsgegevens verwerkt; is dit toch het geval, dan moet dit binnen de regels van de privacywetgeving passen.

Onder het verwerken van persoonsgegevens vallen alle handelingen die een partner kan uitvoeren met zulke gegevens. Handelingen die er volgens de Wet bescherming persoonsgegevens (Wbp) in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens. Deze opsomming is niet limitatief.

### 1.3.1 Bijzondere persoonsgegevens

Er zal gedurende het werkproces integrale aanpak problematische jeugdgroepen in bepaalde gevallen ook sprake zijn van verwerking van bijzondere persoonsgegevens. Onder bijzondere persoonsgegevens vallen gegevens die iets zeggen over iemands ras, godsdienst, gezondheid, politieke gezindheid, lidmaatschap van een vakvereniging, strafrechtelijk verleden of seksuele leven.

In het kader van het werkproces zal het primair gaan om strafrechtelijke en gezondheidsgegevens. Strafrechtelijke gegevens betreffen informatie over misdrijven, overtredingen en veroordelingen van een persoon. Gegevens over de gezondheid omvatten alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen.

[2] Artikel 1 onder a Wbp.

De verwerking van bijzondere persoonsgegevens zorgt voor een grote inbreuk op de privacy van de betrokken personen. Om die reden geldt er een verbod op het verwerken van bijzondere persoonsgegevens (artikel 16 Wbp). In de artikelen 17 – 23 Wbp zijn de uitzonderingen op dit verwerkingsverbod geformuleerd. Het is hulpverleners bijvoorbeeld toegestaan om gezondheidsgegevens te verwerken. Strafrechtelijke gegevens mogen worden verwerkt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht.

De samenwerkende partijen moet zelf bepalen in welke gevallen bijzondere persoonsgegevens mogen worden gebruikt voor het bereiken van de doelen van de samenwerking en welke partijen binnen de samenwerking dan kennis mogen nemen van deze gegevens.

# 2 De samenwerking: rollen en verantwoordelijkheden

## 2.1 Juridische basis voor de samenwerking

Over het algemeen wordt het doel voor een verwerking door één partij vastgesteld (de 'verantwoordelijke'). De verantwoordelijke baseert de rechtvaardiging van zijn doel op een grondslag in de Wbp. Het kan echter ook zijn dat meerdere partijen samenwerken om een gemeenschappelijk doel te bereiken en hiertoe gegevens moeten delen en verder verwerken. Partijen die samenwerken aan dit gemeenschappelijke doel, moeten hun deelname aan de samenwerking kunnen baseren op hun eigen juridische grondslag (bijvoorbeeld omdat zij een publiekrechtelijke taak hebben die alleen goed uitgevoerd kan worden door samen te werken).

Met andere woorden: partijen mogen alleen gegevens ontvangen in het kader van een samenwerking als dit 'gedekt' wordt door hun eigen juridische grondslag om deze gegevens te verwerken. Ook mogen de partijen in het kader van de samenwerking alleen gegevens sturen naar de partijen die deze ook daadwerkelijk mogen ontvangen en verder verwerken op basis van hun juridische grondslag.

Dit luistert extra nauw voor de bijzondere persoonsgegevens, omdat in de meeste gevallen deze gegevens alleen door partijen mogen worden verwerkt als ze daartoe een expliciete basis in de wet hebben.

Nota bene: het opstellen van een convenant kan nooit een juridische grondslag bieden voor partijen om gegevens te verwerken als deze grondslag er niet reeds was op basis van hun eigen grondslagen. Je kan je dus via een convenant jezelf geen nieuwe juridische grondslagen of wettelijke taken geven. Ook is het niet mogelijk om een partij gegevens te laten ontvangen die zij normaliter niet zouden mogen hebben: Bijvoorbeeld als partij X geen strafrechtelijke gegevens zou mogen ontvangen op basis van haar eigen juridisch kader, dan kan dit niet alsnog bij convenant worden geregeld.

## 2.2 Inrichting van de samenwerking

Binnen een samenwerkingsverband kunnen verschillende verwerkingen van persoonsgegevens plaatsvinden. Zo kunnen partijen 1-op-1 gegevens uitwisselen, maar ook gegevens met alle partijen delen. Voor alle verwerkingen (delen van gegevens en vervolgens voor verschillende doelen gebruiken) moet bepaald worden welke partij, of partijen verantwoordelijk zijn.

De samenwerkende partijen moeten voor zichzelf bepalen hoe de verantwoordelijkheid wordt verdeeld. Dit is mede afhankelijk van de concrete inrichting van de samenwerking (welke partijen nemen deel) en de manier waarop het integraal beeld wordt opgesteld (worden

gegevens bijvoorbeeld alleen binnen het eigen domein gedeeld, of krijgen alle partijen inzicht in de gegevens).

Er zijn hierbij grofweg drie scenario's:

1. Partijen delen gegevens, maar er is één **gemeenschappelijke** verantwoordelijke. Deze is aansprakelijk voor het geheel. In een samenwerkingsverband is de meest gerede partner vaak de verantwoordelijke. Dat is degene met de meeste bevoegdheden en de meeste betrokkenheid in het overleg (bijvoorbeeld de burgemeester, of het College van burgemeesters en wethouders).[3]

2. Verschillende verwerkingen zijn min of meer geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van **afzonderlijke** verantwoordelijkheid per (deel-)verwerking.

3. Verschillende verwerkingen zijn geïntegreerd zonder dat een gemeenschappelijke verantwoordelijke aanwezig is. Er is sprake van **gezamenlijke** verantwoordelijkheid. Elk van de verantwoordelijken is aansprakelijk voor het geheel van de gegevensverwerkingen.

Op voorhand is niet te zeggen tot welke verantwoordelijkheidsverdeling de samenwerkingen op basis van het werkproces leiden. Om die reden is in het modelconvenant bij het werkproces de mogelijkheid opengelaten om een gemeenschappelijke verantwoordelijke aan te wijzen, of een situatie van gezamenlijke verantwoordelijkheid te creëren.

Nota Bene: (gezamenlijke) verantwoordelijkheid in de zin van de Wbp betekent dat een partner alle verplichtingen uit de Wbp moet naleven en aansprakelijk is als hierin fouten worden gemaakt (onrechtmatige of onzorgvuldige verwerking). Bij een gezamenlijke verantwoordelijkheid zijn alle partners hoofdelijk aansprakelijk. Het is daarom van belang dat heldere afspraken worden gemaakt tussen partijen over de verantwoordelijkheden (via het convenant) en de onderlinge rechten en plichten.

## 2.3 De uitvoeringscoördinator

Om de samenwerking inhoudelijk goed vorm te geven kan het nodig zijn dat één persoon of organisatie de samenwerking inhoudelijk faciliteert.

De samenwerking van de partners wijst een uitvoeringscoördinator aan die de verantwoordelijkheid draagt het proces in goede banen te leiden. De taak van de uitvoeringscoördinator is specifiek gericht op het coördineren en uitvoeren van de integrale aanpak van een specifieke jeugdgroep en problematisch groepsgedrag en is inhoudelijk van aard. Deze taak betekent niet per se dat de uitvoeringscoördinator inhoudelijk verantwoordelijk is en zonder meer bevoegd is alle informatie te ontvangen en door te geven

[3] Autoriteit Persoonsgegevens (2005), Informatieblad Informatie delen in samenwerkingsverbanden.

aan andere partners. De uitvoeringscoördinator organiseert het overleg van de partners in het kader van het werkproces.

De uitvoeringscoördinator heeft mogelijk verschillende rollen. Binnen het overleg van de driehoekspartners mag hij gegevens delen (mits hij zelf ook vanuit de driehoekspartners komt), nu hiervoor een grondslag is voor gemeente (burgemeester), politie en OM. Bij het benaderen van andere partners en het verzamelen van gegevens aldaar, kan het zo zijn dat hij niet direct alle gegevens met alle partijen mag delen. In deze context moet hij dus afwegen waar uitwisseling van informatie (op persoonsniveau in elk geval) geoorloofd is.

## 2.4 De rol van de gemeente

***Wat is de gemeente?***
In de aanloop naar de stelselherziening van 1 januari 2015 werd in veel parlementaire stukken, media en andere documentatie gesproken over 'de gemeente' die nieuwe verantwoordelijkheden krijgt. Het begrip 'gemeente' wordt beschouwd als koepelbegrip voor de onderdelen waar de gemeente uit bestaat. De gemeente valt uiteen in drie onderdelen:

- Burgemeester
- College van burgemeesters en wethouders
- De gemeenteraad

Daarnaast onderscheiden wij vanuit Wbp perspectief nog een vierde onderdeel:

- Publieke lichamen die gemeentelijke taken uitvoeren (zoals bijvoorbeeld de GGD)

De gemeente zelf wordt niet beschouwd als een bestuursorgaan en kan in privacyrechtelijke zin geen persoonsgegevens verwerken noch als verantwoordelijke voor een verwerking van persoonsgegevens worden aangemerkt. De burgemeester, het college van B&W en de gemeenteraad kunnen wel een verantwoordelijke zijn in de zin van de Wbp.[4] In het licht van de uitvoering van de publiekrechtelijke taak is het daarom belangrijk om in het achterhoofd te houden dat 'de gemeente' zelf niets kan uitvoeren, maar dat deze taken steeds worden uitgevoerd door één van de drie onderdelen binnen de gemeente, of de specifiek bij wet aangestelde publieke lichamen (zoals bijvoorbeeld de GGD op basis van de Wet Publieke Gezondheid). Ieder van deze onderdelen heeft eigen bevoegdheden en taken. Deze taken zijn toebedeeld aan de verschillende onderdelen van de gemeente in onder meer de Gemeentewet, de Wmo en de Jeugdwet. In deze wetten staat ook wat deze publiekrechtelijke taak inhoudt.

***Een regierol voor de gemeente?***
Het beeld leeft bij velen dat door de decentralisaties de gemeente een centrale taak heeft in de coördinatie en uitvoering van alle materiewetten in het sociale domein (de 'regierol'). In zoverre deze regierol er is, betekent dit niet dat voor domeinoverstijgende samenwerkingen, de gemeente de taak heeft om deze inhoudelijk vorm te geven en hiertoe persoonsgegevens te verwerken.

De Autoriteit Persoonsgegevens heeft in haar advies over het jeugddomein hierover het volgende geschreven: "*…in de materiewetten [op het sociaal domein, red.] geen wettelijke taak [is] vastgelegd voor gemeenten om de taken op het gebied van jeugdzorg, maatschappelijke ondersteuning, werk en inkomen en gemeentelijke schuldhulpverlening in onderlinge samenhang uit te voeren. De afzonderlijke wetten voorzien dus niet in een wettelijke basis voor een domeinbrede taakuitoefening in het gedecentraliseerde sociale domein*." [5]

Conclusie is dat gemeenten géén publiekrechtelijke taak hebben om domeinbreed inhoudelijk gegevens te verwerken in het sociaal domein.

Aldus kan de gemeente ook niet vanuit een 'regierol' besluiten nemen over de samenwerking binnen het werkproces en de daarbinnen te verwerken gegevens. Deze verantwoordelijkheid ligt bij de samenwerking zelf (waaruit verschillende onderdelen van een gemeente, ieder vanuit hun eigen publiekrechtelijke taak en verantwoordelijkheid, deel uitmaken). De samenwerking stelt hiertoe een uitvoeringscoördinator aan om te zorgen dat de benodigde regie in de praktijk wel gepakt wordt.

---

[4] Artikel 1 sub d Wbp.

[5] Autoriteit Persoonsgegevens (2014), Advies Privacytoets Jeugddomein, via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies-privacytoets-jeugdhulpdomein.pdf, p. 5.

# 3 Doel en grondslagen Wbp

Persoonsgegevens mogen slechts worden verkregen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden[6].

De vraag in hoeverre de partners persoonsgegevens mogen uitwisselen moet worden beoordeeld aan de hand van de relevante bepalingen uit de Wet bescherming persoonsgegevens (verder: Wbp) en voor sommige partners aan de hand van specifieke wetgeving (bijvoorbeeld OM en politie; zij moeten voldoen aan specifieke eisen voor het delen van gegevens op grond van de Wet justitiële en strafvorderlijke gegevens respectievelijk de Wet politiegegevens). Om te toetsen of het uitwisselen van gegevens tussen de partners legitiem is, moet primair worden gekeken naar het doel en de verwerkingsgrondslag (artikel 7 respectievelijk artikel 8 Wbp) die aan de verwerking van persoonsgegevens ten grondslag liggen.

Een doel is gerechtvaardigd als dit doel gebaseerd kan worden op één van de grondslagen uit artikel 8 Wbp. Kan de verwerking niet gerechtvaardigd worden op basis van één van deze grondslagen, dan is zij niet toegestaan. De grondslagen zijn niet cumulatief: het hebben van één grondslag is voldoende. De zes mogelijke grondslagen zijn:

1. De betrokkene heeft zijn/haar ondubbelzinnige toestemming gegeven[7].
2. De verwerking is noodzakelijk om de overeenkomst met de betrokkene uit te voeren.
3. De verwerking is noodzakelijk om te voldoen aan een wettelijke plicht die op de verantwoordelijke rust.
4. De verwerking is noodzakelijk om de vitale belangen van de betrokkene te waarborgen.
5. De verwerking is noodzakelijk voor de verantwoordelijke om diens publiekrechtelijke taak uit te voeren danwel voor het bestuursorgaan waaraan deze gegevens worden verstrekt.
6. De verwerking is noodzakelijk om een gerechtvaardigd belang van de betrokkene te waarborgen dat zwaarder weegt dan de privacyinbreuk bij de betrokkene.

Hieronder worden de meest relevante verwerkingsgrondslagen kort toegelicht.

***Artikel 8a Wbp: ondubbelzinnige toestemming van de betrokkene***
Wanneer toestemming de grondslag vormt voor gegevensdeling, moet die toestemming voldoen aan de eisen die de Wbp daaraan stelt. De toestemming dient een vrije, specifieke en op informatie berustende wilsuiting te zijn, waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

[6] Artikel 7 Wbp.

[7] Toestemming moet uit vrije wil worden gegeven. Het is in lastig toestemming te verkrijgen in situaties die bedoeld worden in het werkproces.

*Vrij*
Het is van belang dat de betrokkene daadwerkelijk een vrije keuze heeft. Met andere woorden, aan weigering mogen geen negatieve gevolgen kleven voor de betrokkene. Immers, deze kunnen ertoe leiden dat de betrokkene toestemt enkel om deze gevolgen te vermijden.

*Specifiek*
De toestemming moet betrekking hebben op duidelijke en afgebakende doelen. "Wij verwerken uw gegevens in het belang van uw gezondheid en veiligheid" is onvoldoende specifiek.

*Op informatie berustend*
In het verlengde van het voorgaande ligt de eis dat de toestemming op informatie moet berusten. Als het voor de betrokkene volstrekt onduidelijk is wat er met zijn gegevens gebeurt, dan kan de betrokkene geen rechtsgeldige toestemming geven.

De grondslag toestemming kan in het kader van de aanpak van problematisch (jeugd) groepen en individuen alleen gebruikt worden voor vrijwillige trajecten. Van de trajecten waarbij drang of dwang aan de orde is kunnen de bijbehorende verwerkingen niet op toestemming worden gebaseerd.

***Artikel 8e Wbp: de gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt***
Deze grondslag kan gebruikt worden door publiekrechtelijke organen (ministeries, uitvoeringsinstanties, OM, gemeenten) als voor de uitoefening van een aan hen opgedragen publiekrechtelijke taak de verwerking van persoonsgegevens noodzakelijk is.

Een taak is publiekrechtelijk als deze is gebaseerd op een speciaal voor het openbaar bestuur of bij of krachtens wet geschapen grondslag. Dit houdt dus in dat als de gemeente een beroep doet op de Wbp grondslag "noodzakelijk voor de uitvoering van een publiekrechtelijke taak" deze taak in een wet dient te zijn vastgelegd en de gemeente is aangewezen in die wet om deze taak uit te voeren.

Deze grondslag zal voor de meeste partijen in het werkproces de meest geëigende zijn.

***Artikel 8f Wbp: de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert***
Om een beroep op deze grondslag te kunnen doen is het cruciaal dat de verwerking noodzakelijk is met het oog op het belang van de verantwoordelijke of een derde én het belang van degene van wie de gegevens worden verwerkt niet prevaleert. De verantwoordelijke dient voor zichzelf verschillende vragen te beantwoorden:

- Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg (zonder verwerking) worden bereikt?

- Worden alleen gegevens gebruikt die noodzakelijk zijn om het doel te bereiken?
- Wat is het belang dat de verwerking van persoonsgegeven rechtvaardigt?
- Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan afhankelijk van de ernst van de inbreuk gegevensverwerking niet achterwege te blijven?
- Is de verwerking evenredig aan het nagestreefde doel?

Voor het verwerken van persoonsgegevens door de gemeente[8] en eventuele andere partners kan in de meeste gevallen het beste een beroep worden gedaan op de uitvoering van diens publiekrechtelijke taak als grondslag.

### 3.1.1 Noodzakelijkheidsvereiste

Om een succesvol beroep te doen op een grondslag gebaseerd op de artikel 8b tot en met 8f Wbp Wbp, dient het verwerken van persoonsgegevens *noodzakelijk* te zijn. De verwerking moet de proportionaliteits- en subsidiariteitstoets doorstaan. Dit houdt in dat de inbreuk op de belangen van betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel, en dat dit doel in redelijkheid niet op een andere, voor de betrokkene minder nadelige, wijze kan worden verwerkelijkt.[9]

Kort gezegd is het dus van belang dat bij elke stap in het proces en bij elke gewenste gegevensuitwisseling getoetst wordt of:

- Er een concreet doel is om gegevens uit te wisselen met de betreffende partner;
- Er een noodzaak is om de gegevens voor dit doel uit te wisselen met een betreffende partner;
- De uitwisseling proportioneel en subsidiair is.

Nadat de legitimiteit van de verwerking is vastgesteld, moet de partner er ook voor zorgen dat hij aan alle materiële eisen uit de Wbp, zoals informatiebeveiliging en het borgen van rechten van betrokkene, voldoet.

## 3.2 Persoonsgegevens delen met partners (stap 2 en verder in het werkproces)

In principe kunnen persoonsgegevens die noodzakelijk zijn met het oog op het handhaven van de openbare orde en veiligheid en de opsporing van strafbare feiten gedeeld worden, tussen politie, OM en de burgemeester, uiteraard zolang dit noodzakelijk is met het oog op het handhaven van de openbare orde door het aanpakken van problematische jeugdgroepen.

Bij partners buiten deze drie driehoekspartners om, moet gedurende alle stappen in het werkproces per partner een afweging gemaakt worden of er een wettelijke grondslag is voor zowel gegevens verstrekken als ontvangen. De verantwoordelijkheid voor het maken van deze afweging ligt bij de individuele partners zelf: zij beslissen om al dan niet gegevens te

[8] Hier moet wel onderscheid worden gemaakt tussen de verschillende rollen binnen de gemeente. De gemeente is geen op zichzelf staand orgaan, maar wordt onderverdeeld in burgemeester, het college van B&W en de gemeenteraad.
[9] HR NJB 2011/1665 9 september 2011 (Santander/X) Zie ook artikel 11 Wbp.

verstrekken en/of te ontvangen. Wanneer een partij niet wil of mag verstrekken, toont zij aan waarom niet (denk bijvoorbeeld ook aan geheimhoudingsplichten).

Een ander punt van aandacht bij gegevensuitwisseling tussen partners is het delen van bijzondere persoonsgegevens. Hier gelden zoals eerder gesteld strengere regimes.[10]

Telkens wanneer een partner of uitvoeringscoördinator vraagt om informatie te verstrekken aan (partijen) binnen de samenwerking, moet de vraag beantwoord worden of het betrekken van die partner (en dus het delen van gegevens met die partner) noodzakelijk is om tot een integraal beeld te komen.

### 3.2.1 Ontvangen van persoonsgegevens door partners

Een partner kan altijd vragen aan andere partners om informatie te verstrekken. Het is de verantwoordelijkheid van elke partner afzonderlijk om te beoordelen of gegevensverstrekking in een dergelijke situatie gerechtvaardigd is of niet. De partners moeten bij elke gegevensverwerking (zowel verstrekken als ontvangen) een afweging maken of er een noodzaak en geen grondslag voor de verstrekking cq. ontvangst is.

## 3.3 Overige Wbp eisen

Wanneer er een juridische grondslag bestaat voor de verwerking mogen de gegevens verwerkt worden. Hierbij is het wel van belang dat deze gegevens zorgvuldig worden behandeld. Om die reden kent de Wbp diverse materiële eisen. Hieronder zijn de belangrijkste eisen weergegeven.

### 3.3.1 Informatieplicht

Eén van de belangrijkste voorwaarden voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens is het informeren van de betrokkene.[11] Het verwerken van persoonsgegevens van de betrokkene mag niet geschieden zonder dat de betrokkene hierover is geïnformeerd. Eén van de basisbeginselen van de Wbp is namelijk het transparantiebeginsel. Artikel 33 en 34 Wbp vormen een uitwerking van dit transparantie-beginsel. De Wbp verlangt dat een betrokkene wordt voorzien van informatie die van belang is om een beoordeling te maken van de rechtmatigheid van de verwerking van zijn persoonsgegevens. Op het moment dat de gegevens worden verzameld bij de betrokkene, moet alle benodigde informatie worden verschaft aan de betrokkene zodat een behoorlijke en zorgvuldige verwerking wordt gewaarborgd.

Er kunnen uitzonderingen gelden waardoor voldoen aan de informatieplicht niet hoeft. Deze staan in artikel 43 Wbp. De partner hoeft niet te voldoen aan de informatieplicht als dit noodzakelijk is in het belang van:

- De veiligheid van de staat;

[10] Dit wordt nader uitgelegd in 4.5.2.

[11] Artikel 6 Wbp; zie ook: De Vries, in: T&C Telecommunicatierecht 2009, art. 33 Wbp, aant. 1.

- De voorkoming, opsporing en vervolging van strafbare feiten;
- Gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- Het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of
- De bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Indien er sprake is van één of meer van bovenstaande gevallen, mag ook voorbij worden gegaan aan de plichten om persoonsgegevens niet verder te verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn gekregen (artikel 9); op verzoek gegevens te verstrekken ten aanzien van vrijgestelde gegevensverwerkingen (artikel 30 lid 3 jo artikel 28 lid 1 a t/m e); een datalek te melden (artikel 34a) en de rechten van betrokkenen te honoreren (onder andere inzage, artikel 35).

### 3.3.2 Melding

Gegevensverwerkingen moet gemeld worden bij de Autoriteit Persoonsgegevens.

### 3.3.3 Beveiliging

De gegevens moeten goed worden beveiligd. Dit betekent dat er passende organisatorische en technische maatregelen moeten worden genomen door het samenwerkingsverband om te zorgen dat onbevoegden geen kennis van de gegevens kunnen nemen.

### 3.3.4 Rechten van de betrokkenen

Er moet invulling worden gegeven aan de rechten van de betrokkenen zoals inzage, wijziging of verwijdering tenzij er zwaarwegende gronden zijn om dit niet te doen.

### 3.3.5 Bewaartermijnen

Er is op grond van de Wet bescherming persoonsgegevens (Wbp) geen concrete bewaartermijn voor persoonsgegevens. Gegevens mogen niet langer bewaard worden dan noodzakelijk voor de doeleinden van de verwerking. Het uitgangspunt moet zijn: 'need to have', niet 'nice to have'. Wel zijn er concrete bewaartermijnen in andere wetten waar sommige partners zich wellicht aan moeten houden. Bijvoorbeeld op grond van belastingwetgeving. Indien de noodzaak (of de wettelijke plicht) er niet langer is, moeten de persoonsgegevens worden vernietigd.

Ook voor het monitoren van jongeren geldt dat het bewaren van gegevens is toegestaan zo lang het noodzakelijk is. In het algemeen geldt: hoe korter, hoe beter.