Juridische aspecten bij het inrichten van een meldpunt niet acute zorg / E. Schreuders / januari 2021
Behoort bij de handreiking: "Meldpunten niet-acuut. Handvatten voor Gegevensverwerking" oorspronkelijke datum aug 2020, aangevuld in jan 2021.

1 Inleiding

In dit document gaat het over de juridische aspecten bij het verwerken van persoonsgegevens bij het uitvoeren door meldpunten van hun taken en werkzaamheden. De vijf juridische aspecten die aan de orde komen zijn:

1. de juridische basis om meldpunten niet acute zorg op te richten voor zover deze basis nodig is om persoonsgegevens te kunnen verwerken;
2. de juridische aspecten bij gegevensverwerking door meldpunten niet acute zorg. Hierbij gaat het om:
    - het vastleggen van gegevens. Dit start bij het ontvangen van een melding;
    - het verzamelen van aanvullende informatie (lees: het vragen om informatie) voor het behandelen van een melding ten behoeve van triage en het bepalen van de vervolgactie. Hierbij worden door het meldpunt persoonsgegevens verstrekt in het kader van een vraag om informatie ten behoeve van de werkzaamheden van het meldpunt. Het gaat hierbij bijvoorbeeld om het door het meldpunt bij het stellen van een vraag verstrekken van persoonsgegevens aan:
        - de melder;
        - de persoon over wie de melding gaat;
        - andere meldpunten of loketten (partijen) waar de melding inhoudelijk bezien thuishoort;
        - overleg met andere meldpunten niet acute zorg;
        - diverse partijen, waaronder partijen die bijvoorbeeld al zorg of hulp verlenen of toegekend hebben of partijen die zorg of hulp aan kunnen gaan bieden of toe kunnen gaan kennen;
    - het verstrekken van gegevens door meldpunten aan:
        - partij(en) die de casus verder behandelen en bijvoorbeeld zorg- en hulp gaan toewijzen of verlenen (het verstrekken van gegevens voor de vervolgacties);
        - de melder om deze te informeren over de opvolging van de melding.
3. het verstrekken van persoonsgegevens aan meldpunten bij een melding en als antwoord op een informatievraag van het meldpunt;
4. het vereiste van noodzaak en dat enkel noodzakelijke gegevens verwerkt mogen worden;
5. De informatieplicht van de AVG.

2 De juridische basis om meldpunten op te richten voor zover van belang voor het kunnen verwerken van persoonsgegevens

Het gaat in dit onderdeel om de juridische basis om meldpunten niet acute zorg op te richten voor zover deze basis nodig is om persoonsgegevens te kunnen verwerken. De conclusies van dit onderdeel zijn:

1. Er is geen *specifieke* wettelijke regeling voor het oprichten van meldpunten;
2. De WAMS-regelgeving die thans nog in ontwikkeling is zal naar verwachting een deugdelijke en duidelijke wettelijke basis bieden voor het oprichten van meldpunten en is daarvoor ook nodig.
3. Zolang de nieuwe WAMS-wetgeving er nog niet is, komen de volgende opties in aanmerking:
a) meldpunten met een taak van algemeen belang formeel opgericht c.q. ingesteld door het College van B&W en de burgemeester (van één of meerdere gemeenten) en ondergebracht bij een GGD.
b) meldpunten met een gecombineerde taak van algemeen belang en (medische) zorgverlening gezamenlijk opgericht c.q. ingesteld door het College van B&W (van één of meerdere gemeenten) en de GGZ-instelling waar het meldpunt is ondergebracht.
c) meldpunten met een taak van algemeen belang formeel opgericht c.q. ingesteld door het College van B&W en de burgemeester (van één of meerdere gemeenten) en ondergebracht bij een bij de oprichting aangewezen andere partij dan GGD of GGZ.
4. Het is (en blijft) mogelijk dat, naast het besluit c.q. de beslissing tot oprichting van het meldpunt, meerdere partijen afspraken maken over bijvoorbeeld de bemensing of de werklocatie van het meldpunt.

Deze conclusies zijn gebaseerd op het volgende:

Meldpunten zijn vooral ontstaan door een praktische aanpak en – voorheen – als specifieke in de eerdere Wmo als prestatieveld geregelde OGGZ.

Het gaat bij het oprichten van meldpunten om het in art. 6, lid 3, AVG bedoelde Nederlandse recht als basis om meldpunten aan te wijzen en hen een taak van algemeen belang te geven zodat de gegevensverwerking gebaseerd kan worden op art. 6, lid 1, onder e, AVG.

Bij het op grond van art. 6, lid 3, AVG bedoelde recht om gegevensverwerking met als grondslag art, 6, lid 1, onder e, AVG bij een taak van algemeen belang mogelijk te maken gaat het bij meldpunten om een 'optelsom' van de taken en werkzaamheden van de burgemeester in verband met de openbare orde en de taken en werkzaamheden en verantwoordelijkheden van het College van B&W in het sociaal domein. Een besluit tot oprichten van een meldpunt kan, uitgaande van een 'optelsom' door het College van B&W en door de burgemeester genomen worden op basis van de artikelen 160, lid 1, onder a, en 170, lid 3, van de Gemeentewet. Deze artikelen van de gemeentewet geven het College van B&W de bevoegdheid om het dagelijks bestuur van de gemeente te voeren, voor zover niet bij of krachtens de wet de raad of de burgemeester hiermee is belast en geven de burgemeester de bevoegdheid om een goede behartiging van de gemeentelijke aangelegenheden te bevorderen.
Voor het college spelen daarbij ook de taken uit de materiewetten voor het sociaal domein (Wmo, Jeugdwet, Participatie wet). Voor de burgemeester spelen daarbij diens bevoegdheden ten aanzien van de openbare orde.

Bij het oprichten en onderbrengen van een meldpunt bij een GGZ-instelling gaat het om dezelfde 'optelsom' aangevuld met de GGZ als een instelling voor gezondheidszorg.

In bepaalde situaties wordt het meldpunt bijvoorbeeld bemenst door medewerkers van meerdere organisaties. Het is (en blijft) daarbij mogelijk dat, naast het besluit c.q. de beslissing tot oprichting van het meldpunt, meerdere partijen afspraken maken over bijvoorbeeld de bemensing en/of de werklocatie van het meldpunt en daarbij zo nodig afspraken maken over de verdeling van kosten c.q. de verdeling van een eventuele subsidie voor het meldpunt.

3 De verwerkingsverantwoordelijke(n) en het soort juridische regime voor gegevensverwerking

3.1 De verwerkingsverantwoordelijke(n)

Het gaat in dit onderdeel om de vraag welke organisatie aan te merken is als verwerkingsverantwoordelijke of welke organisatie aangemerkt zouden kunnen worden als gezamenlijk verwerkingsverantwoordelijken en wat voor een soort juridisch regime voor gegevensverwerking aangewezen is. De conclusies van dit onderdeel zijn:

1. Er dient bij een meldpunt niet-acuut een eenduidig regime voor gegevensverwerking door het meldpunt dient te zijn met, bij voorkeur, één verwerkingsverantwoordelijke. Een keuze voor meerdere verantwoordelijken biedt ten aanzien van het (kunnen) verwerken van persoonsgegevens geen enkel voordeel (ook dan dient er een eenduidig regime te zijn) en levert (onnodige) beheersmatige nadelen op.
2. De WAMS-regelgeving die thans nog in ontwikkeling is zal naar verwachting een eenduidige regime voor gegevensverwerking bieden en zal duidelijke basis bieden voor het bepalen van de verwerkingsverantwoordelijke. De WAMS-wetgeving is daarvoor ook nodig.
3. Zolang de nieuwe WAMS-wetgeving er nog niet is, komen de volgende opties in aanmerking:
a) de GGD als verwerkingsverantwoordelijke voor een meldpunt ondergebracht bij de GGD;
b) de GGZ-instelling als verwerkingsverantwoordelijke voor een meldpunt ondergebracht bij de GGZ-instelling
c)) voor een meldpunt ondergebracht bij een andere partij dan de GGD of een GGZ-instelling een bij de oprichting van het meldpunt specifiek aangewezen verwerkingsverantwoordelijke, waarbij het voor de hand ligt om de aangewezen partij of het College van B&W als verwerkingsverantwoordelijke aan te wijzen (bij meerdere gemeenten bijvoorbeeld de centrumgemeente).
4. Het is de verwerkingsverantwoordelijke die bijvoorbeeld een privacyreglement of protocol vaststelt. Als een meldpunt bemenst wordt door medewerkers van verschillende partijen vallen die medewerkers ten aanzien van gegevensverwerking onder het gezag van de verwerkingsverantwoordelijke.

5. Het is mogelijk dat het meldpunt (lees: de verwerkingsverantwoordelijke) voor de gegevensverwerking door het meldpunt gebruik maakt van een ICT-systeem dat de verwerkingsverantwoordelijke al gebruikt bij de eigen al bestaande (primaire) taken en werkzaamheden.
6. Het is ook mogelijk dat door het meldpunt gebruik gemaakt wordt van het ICT-systeem van een gemeente of van een andere partij. Dan geldt de partij die het ICT-systeem ter beschikking stel als verwerker en is een verwerkersovereenkomst nodig tussen de verwerkingsverantwoordelijke en deze partij.

Deze conclusies zijn gebaseerd op het volgende:

Op grond van de AVG dient er bij meldpunten niet-acuut altijd een verwerkingsverantwoordelijke te zijn. Anders gezegd: een meldpunt niet-acuut zonder verwerkingsverantwoordelijke is niet toegestaan.

De AVG gaat er, als uitgangspunt, vanuit dat er één verwerkingsverantwoordelijke is. De AVG maakt ook meerdere verwerkingsverantwoordelijken mogelijk (art. 26 AVG). Door deze mogelijkheid van meerdere verwerkingsverantwoordelijken wordt er in de praktijk nogal eens als een soort van 'automatisme' vanuit gegaan, dat er bij samenwerking van meerdere partijen (bij een samenwerkingsverband) dus ook sprake is of altijd sprake zou dienen te zijn van meerdere verwerkingsverantwoordelijken en dat een vormgeving met meerdere verwerkingsverantwoordelijke 'dus' ook altijd mogelijk is. Dit is een misverstand. Of en in welke mate meerdere verwerkingsverantwoordelijken voor een meldpunt niet-acuut ook daadwerkelijk mogelijk of nodig is hangt niet (zozeer) van de AVG af, maar hangt vooral af van a) de vorm van samenwerking, b) de (primaire) taken en werkzaamheden van samenwerkende partijen en c) de specifieke nationale regels over gegevensverwerking voor die partijen (lees: de verwerkingsverantwoordelijken) in de Uitvoeringswet AVG en in materiewetten voor die partijen. Voor een scenario met meerdere verwerkingsverantwoordelijken dient dan ook bezien te worden welke invloed de kenmerken van de samenwerking hebben op een aantal specifieke aspecten bij het verwerken van persoonsgegevens. Pas als de invloed van de kenmerken van de samenwerking op de gegevensverwerking bij de samenwerking bekend is, kan een oordeel gegeven worden of en in welke mate een vormgeving met meerdere verwerkingsverantwoordelijken mogelijk is. Ook de omschrijving van verwerkingsverantwoordelijke in de AVG (art. 4, onder 7, AVG) dat de partij of partijen die het doel en de middelen voor de gegevensverwerking bepalen de verwerkingsverwerkingsverantwoordelijke is of zijn, leidt er niet toe dat bij een samenwerkingsverband de oprichtende partijen dus allemaal verwerkings-verantwoordelijken zouden *moeten* zijn. De definitie verbiedt immers niet om bij samenwerking één partij als verwerkingsverantwoordelijke aan te wijzen c.q. aan te merken.

Bij meldpunten speelt daarbij ook dat het in de regel het meldpunt zelf zal zijn (zeker bij een meldpunt bij de GGD of een GGZ-instelling) die de ICT-middelen kiest en ook zullen meldpunten in de praktijk bij de uitvoering van werkzaamheden en bij gegevensverwerking zodanig zelfstandig opereren dat het meldpunt gelet op de feitelijke omstandigheden als verwerkingsverantwoordelijke optreedt en aangemerkt kan worden. Ook aan art. 26 AVG waarin geregeld is dat er bij meerdere gezamenlijke verwerkingsverantwoordelijken afspraken dienen te zijn kan het argument ontleend worden dat het daarbij ook mogelijk is om in een besluit van de oprichters van het meldpunt of bij samenwerkingsafspraken (op voorhand) één verwerkingsverantwoordelijke aan te wijzen. Dit omdat het op voorhand aanwijzen van één verwerkingsverantwoordelijke voor de praktijk in feite neerkomt op zowat de eenvoudigste manier om duidelijkheid over de rollen van eventuele meerdere partijen en de rol van verwerkingsverantwoordelijke vast te leggen. En ook als bijvoorbeeld meerdere partijen afspraken maken over bijvoorbeeld de bemensing of de werklocatie van het meldpunt geldt dat het op basis hiervan niet nodig is om al die partijen ten aanzien van de gegevensverwerking door het meldpunt als gezamenlijk verwerkingsverantwoordelijken aan te merken. In de praktijk zal het voor komen dat dat door het meldpunt (lees: de verwerkingsverantwoordelijke) gebruik gemaakt wordt van het ICT-systeem van een gemeente of van een andere partij. Dan geldt de partij die het ICT-systeem ter beschikking stel als verwerker en is op grond van art. 28, lid 3, AVG een verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en deze partij of een andere rechtshandeling verplicht is. Ook dit door een andere partij ter beschikking stellen van ICT-middelen leidt er niet tot dat die ter beschikking stellende partij (altijd) als gezamenlijk verwerkingsverantwoordelijke aangemerkt zou moeten worden.

Een ander misverstand is dat bijvoorbeeld een Convenant of Samenwerkingsovereenkomst met meerdere gezamenlijk verwerkingsverantwoordelijken inhoudelijk bezien gegevensverwerking voor meldpunten mogelijk zou (kunnen) maken die zonder een dergelijk Convenant of Samenwerkingsafspraak niet mogelijk is. Op grond van de UAvg biedt een Convenant of Samenwerkingsovereenkomst alleen een mogelijkheid om daarmee

gebruik van persoonsgegevens van strafrechtelijke aard mogelijk te maken bij zogenaamde 'zwarte lijsten' (art. 33, lid 4, onder c, UAvg met een vergunning van de Autoriteit Persoonsgegevens) of gebruik van persoonsgegevens van strafrechtelijke aard mogelijk te maken ten behoeve van publiekrechtelijke samenwerkingsverbanden (art. 33, lid 1, onder b, UAvg). Bij meldpunten is er geen sprake van een 'zwarte lijst' en in onderdeel 3 wordt aangegeven dat een publiekrechtelijk samenwerkingsverband niet of nauwelijks toepasbaar is voor meldpunten en geen toereikende oplossing kan bieden omdat er bij dergelijk publiekrechtelijk samenwerkingsverband geen mogelijkheid is om een zelfstandige regeling te treffen om persoonsgegevens over de gezondheid van de betrokkene te kunnen verwerken (art. 33, lid 1, onder b, UAvg gaat enkel over het gebruik van persoonsgegevens van strafrechtelijke aard) .

Bij de verwerkingsverantwoordelijke(n) voor de meldpunten niet-acuut zijn er – in beginsel – vier mogelijkheden. Welke van de vier mogelijkheden ten aanzien van een keuze voor één of meerdere verwerkingsverantwoordelijken ook daadwerkelijk bruikbaar zijn hangt, zoals gezegd, af van de concrete situatie en bij samenwerking hangt dit af van de kenmerken van de samenwerking. De vier mogelijkheden bij meldpunten niet-acuut zijn:

1) er is één verwerkingsverantwoordelijke met een eenduidig regime voor gegevensverwerking door het meldpunt;
2) er zijn meerdere verwerkingsverantwoordelijken met per dossier een ander regime voor gegevensverwerking waarbij het toepasselijke regime per dossier iedere keer ontleend wordt aan het regime van de moederorganisatie van de 'toevallige' (hoofd)behandelaar van de melding;
3) er zijn meerdere verwerkingsverantwoordelijken met voor alle dossiers als het ware een 'optelsom' of 'combinatie' van de juridische regimes van de verschillende verwerkingsverantwoordelijken;
4) er zijn meerdere verwerkingsverantwoordelijken met een voor de samenwerking specifiek en eenduidig regime voor gegevensverwerking dat los staat van de (afzonderlijke) regimes voor de (primaire) taken en werkzaamheden van de verschillende samenwerkende partijen. Het specifieke regime voor gegevensverwerking door het meldpunt dient daarbij duidelijk beschreven te worden.

Situatie 1 zal vooral spelen bij het positioneren van een meldpunt bij bijvoorbeeld een GGD of bij een GGZ-instelling.
De situaties 2, 3 en 4 kunnen spelen als een meldpunt gepositioneerd wordt bij een samenwerkingsverband zoals bijvoorbeeld sommige wijkteams of sociale wijkteams die opgericht zijn als samenwerking van meerdere partijen en die bestaan uit medewerkers van verschillende organisaties.

Situatie 2 is voor de praktijk (volstrekt) onwerkbaar. Hierbij speelt ook dat de juridische regimes voor gegevensverwerking van de 'moederorganisaties' gekoppeld zijn aan de (primaire) taken en werkzaamheden van de 'moederorganisaties' en ook daarom al geen juridische basis kunnen bieden voor gegevensverwerking bij de andere taken en werkzaamheden van een meldpunt niet-acute zorg (zie hiervoor ook onderdeel 3). Situatie 2 is bijvoorbeeld wel mogelijk als meerdere partijen voor dezelfde soort werkzaamheden bijvoorbeeld als samenwerkingsverband een dienstenorganisatie oprichten waarbij de gegevens van de samenwerkende partijen afgeschermd van elkaar verwerkt worden en het ook niet nodig is dat de samenwerkende partijen onderling gegevens uitwisselen. Een voorbeeld van een dergelijke samenwerking is het met name om efficiency redenen oprichten van een HRM organisatie als facilitair bedrijf. Het gaat dan om gedeelde verantwoordelijkheid waarbij iedere partij zelf de (enige) verantwoordelijke is voor de gegevensverwerking van de eigen personeelsleden.

Inhoudelijk bezien komen de situaties 1 en 4 op hetzelfde neer: er is één eenduidig regime voor gegevensverwerking nodig. De meerwaarde van meerdere verwerkingsverantwoordelijken bij een dergelijke constructie bij een meldpunt niet-acuut is (wat) onduidelijk omdat men daarbij een regime vast dient te stellen dat los staat van de eigen afzonderlijke regimes. Om complexiteit en discussies bij bijvoorbeeld de op grond van art 26 AVG verplichte afspraken en bij het vaststellen en het naleven van een afzonderlijk vast te stellen regime voor gegevensverwerking zoveel mogelijk te vermijden, kan bij meldpunten inhoudelijk bezien ook (en evengoed) gekozen worden voor het aanwijzen van één partij als de verwerkingsverantwoordelijk. Een keuze voor een constructie met (toch) meerdere verwerkingsverantwoordelijken zou nog wel verband kunnen houden met het feit dat de samenwerkende partijen of de als enige verwerkingsverantwoordelijke aangewezen partij het onwenselijk vinden dat de ICT-kosten en eventuele boeten of schadevergoeding geheel ten laste komen van de ene aangewezen partij. Om dergelijke eenzijdige kosten te vermijden is een keuze voor

meerdere verwerkingsverantwoordelijken echter niet noodzakelijk of nodig. Ook bij de afspraken tot oprichting van de samenwerking zelf (de oprichting van het samenwerkingsverband) kan een verdeelsleutel voor dergelijke kosten afgesproken worden. Anders gezegd: om bij samenwerking een afspraak te maken over dergelijke kosten is het niet nodig om enkel daarvoor de partijen (tevens) als gezamenlijk verwerkingsverantwoordelijken aan te merken.

Situatie 3 is niet of nauwelijks mogelijk bij meldpunten-niet acuut als samenwerkingsverband met meerdere verantwoordelijken en een soort 'optelsom' of 'combinatie' van juridische regimes voor gegevensverwerking. Daarvoor zullen de juridische regimes voor die partijen teveel van elkaar verschillen. Bij situatie 3 speelt ook dat de regimes van de 'moederorganisaties' gekoppeld zijn aan de (primaire) taken en werkzaamheden van de 'moederorganisaties' en ook daarom als 'optelsom' geen of nauwelijks een juridische basis kunnen bieden voor gegevensverwerking bij de andere taken en werkzaamheden van een meldpunt niet-acute zorg (zie hiervoor ook onderdeel 3). Samenwerkingsverbanden bij meldpunten zijn in die zin (geheel) anders dan bijvoorbeeld sommige vormen van sociale wijkteams of casusoverleggen bij Zorg- en Veiligheidshuizen waarbij de verschillende partijen juist wel deelnemen vanuit hun eigen primaire eigen taken en werkzaamheden. Situatie 3 is bijvoorbeeld wel mogelijk als partijen inhoudelijk bezien dezelfde primaire taken en werkzaamheden hebben, samenwerken en gegevens uitwisselen om die inhoudelijk gelijke werkzaamheden gezamenlijk beter uit te kunnen voeren en als de samenwerkende partijen tevens eenzelfde (of zeer vergelijkbaar) regime voor gegevensverwerking hebben. Samenwerking gebeurt dan in de eerste plaats om redenen van effectiviteit omdat samenwerken inhoudelijke voordelen oplevert ten opzichte van de situatie waarbij iedere partij afzonderlijk opereert.

3.2 Mogelijke regimes voor gegevensverwerking door meldpunten

Het gaat in dit onderdeel om de vraag of en in welke mate er sprake is van een eenduidig en toereikend regime voor gegevensverwerking door meldpunten. De conclusies van dit onderdeel zijn:

1. Er is geen *specifieke* wettelijke regeling voor gegevensverwerking door meldpunten in materiewetten. Het juridisch regime zal gebaseerd dienen te worden op (enkel) de AVG en de uitvoeringswet AVG;
2. De WAMS-regelgeving die thans nog in ontwikkeling is zal naar verwachting een specifieke wettelijke regeling bieden voor gegevensverwerking door meldpunten en is daarvoor ook nodig;
3. Zolang de nieuwe WAMS-wetgeving er nog niet is, komen de volgende opties in aanmerking:
a) een regime gebaseerd op enkel de AVG, de UAvg voor meldpunten ondergebracht bij de GGD en voor meldpunten (niet bij een GGZ-instelling) ondergebracht bij een bij de oprichting aangewezen partij;
b) een regime gebaseerd op de AVG, de UAvg met eveneens overeenkomstige toepassing van de regeling over medische dossiers in de WGBO voor meldpunten ondergebracht bij een GGZ-instelling;
4. Bij het verstrekken van persoonsgegevens *door* meldpunten kan het in dit onderdeel beschreven overzicht van belangen en vuistregels gebruikt worden. Dit overzicht kan ook zonder de komende WAMS-wetgeving gebruikt worden en de WAMS-wetgeving is niet nodig voor het *door* meldpunten kunnen verstrekken van gegevens.

Deze conclusies zijn gebaseerd op het volgende:

Er is voor de meldpunten niet-acuut geen specifieke wettelijke regeling voor gegevensverwerking zoals die er bijvoorbeeld in de Wmo is voor de Amhk's.

Er is voor de meldpunten niet-acuut ook geen regime dat eenduidig en direct ontleend kan worden aan het regime voor:
- de taken en werkzaamheden van de GGD zoals geregeld in de Wet publieke gezondheidszorg
- het verlenen van medische zorg zoals bedoeld in de Wgbo omdat er geen sprake is van een daarbij vereiste behandelovereenkomst
- de gemeentelijk toeleiding bij de Wmo of Jeugdwet.

De verschillende materiewetten bieden geen juridisch regime voor gegevensverwerking. Bij meldpunten zal het juridisch regime voor gegevensverwerking gebaseerd dienen te worden op (enkel) de AVG en de UAvg.

Bij een dergelijk juridisch regime zijn voor het verwerken en verstrekken van persoonsgegevens door meldpunten de volgende onderdelen van belang:
- de in art. 6, lid 1, AVG bedoelde grondslag voor het verwerken van gegevens (al behandeld in onderdeel 2);
- de mogelijkheid om bijzondere gegevens (gezondheid) en strafrechtelijke gegevens te kunnen verwerken;
- het doelbindingsbeginsel van art. 5, lid 1, onder b, en art. 6, lid 4, AVG;
- het (eventueel) aanwezig zijn van een geheimhoudingsverplichting;
- de AVG-grondslag voor het door het meldpunt verstrekken van gegevens;
- de AVG-informatieplicht voor het informeren van betrokkenen dat persoonsgegevens verwerkt worden.

3.3 Het gebruik van bijzondere en/of strafrechtelijke gegevens

Bijzondere gegevens (art. 9 AVG) zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Strafrechtelijke gegevens (art. 10 AVG en vooral art. 1 Uavg) zijn persoonsgegevens van strafrechtelijke aard en dit zijn zijn persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.

Als uitgangspunt kan genomen worden dat er bij de gegevens over meldingen altijd of nagenoeg altijd ook sprake zal zijn van gegevens over de gezondheid. Ook bij de informatie dat iemand psychische klachten of een aandoening heeft of zeer waarschijnlijk zal hebben, dat iemand bij een bepaalde medische beroepsbeoefenaar of instelling in behandeling is of dat er sprake is van een persoon met verward gedrag is er (al) sprake van gegevens over de gezondheid.
Daarnaast zal er in een groot aantal gevallen ook sprake zijn van gegevens van strafrechtelijke aard. Hierbij gaat het bijvoorbeeld om gegevens over strafbare feiten c.q. informatie over handelingen waarvoor een strafrechtelijke aanpak (bijvoorbeeld aangifte) op zich mogelijk zou zijn.
Als derde zou er in bepaalde gevallen (uitzonderingen) ook sprake kunnen zijn van andere bijzondere gegevens met gegevens over ras of etnische afkomst, over religieuze of levensbeschouwelijke overtuigingen of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid als deze noodzakelijk zijn in aanvulling op gegevens over gezondheid voor het bepalen van de juiste zorg- of hulp of als deze gegevens noodzakelijk zijn in aanvulling op strafrechtelijke gegevens als deze direct te maken hebben met het gepleegde strafbare feit.

<u>Alle bijzondere gegevens, waaronder gegevens over gezondheid</u>

Een mogelijkheid om bijzondere gegevens te gebruiken is in bepaalde gevallen artikel 23, onder c, UAvg. Dit artikel maakt het gebruik van bijzondere gegevens mogelijk in aanvulling op strafrechtelijke gegevens.

<u>Gegevens over gezondheid</u>

Mogelijkheden om gegevens betreffende de gezondheid te gebruiken zijn eventueel:
Art. 30, lid 1, onder a, UAvg: bestuursorgaan voor de goede uitvoering van wettelijke voorschriften die voorzien in aanspraken die afhankelijk zijn van de gezondheid (meldpunt als onderdeel van een bestuursorgaan)
Art. 30, lid 3, onder a, UAvg: hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging en er een geheimhoudingsverplichting is.

<u>Andere bijzondere gegevens in aanvulling op gegevens over gezondheid</u>
Het gebruik va andere bijzondere gegevens dan die over gezondheid is mogelijk op grond van art. 30, lid 5, UAvg als deze gegevens nodig zijn in aanvulling op gegevens betreffende de gezondheid.

Strafrechtelijke gegevens

De mogelijkheid om strafrechtelijke gegevens te gebruiken kan liggen in:
- Art. 33, lid 1, onder a, UAvg: indien verkregen van de politie
- art. 33, lid 1, onder c, UAvg in aanvulling op gezondheid bij 30, lid 3, onder a, UAvg

Daadwerkelijke mogelijkheden voor meldpunten om bijzondere en strafrechtelijke gegevens te gebruiken

Bij het door meldpunten verwerken van gegevens over de gezondheid en/of strafrechtelijke gegevens kan er bij het gebruik van gegevens over gezondheid en bij strafrechtelijke gegevens sprake zijn van de volgende (theoretische) situaties:

1 - gegevens over de gezondheid is mogelijk
2 - strafrechtelijke gegevens is mogelijk
3 - gegevens over de gezondheid is mogelijk en in aanvulling daarop zijn strafrechtelijke gegevens mogelijk
4 - strafrechtelijke gegevens is mogelijk en in aanvulling daarop zijn gegevens over gezondheid mogelijk

Voor meldpunten zal in de praktijk optie 3 toereikend zijn c.q. de optie zijn.

4 Het verstrekken van gegevens

4.1 Verstrekken van gegevens *door* meldpunten

Bij het verstrekken van persoonsgegevens zijn de volgende elementen van belang:
- de doelbinding van de AVG van art. 5, lid 1, onder b, en art. 6, lid 4, AVG;
- Een eventuele strikte doelbinding die er op neerkomt dat gegevens enkel verder gebruikt mogen worden voor dezelfde doelen als waarvoor deze eerder verzameld zijn;
- Geheimhoudingsverplichtingen waarbij er voor gegevens over gezondheid op basis van art. 30, lid 4, UAvg en voor strafrechtelijk verkregen van de politie op basis van art. 7, lid 2, Wet politiegegevens altijd een geheimhoudingsverplichting geldt.

In de praktijk staan medewerkers vaak voor de lastige vraag of gegevens nu wel of niet verstrekt mogen worden. Het overzicht van belangen en vuistregels dat in dit onderdeel aan de orde komt is een hulpmiddel voor de praktijk bij het verstrekken van gegevens aan derden en bij eigen hergebruik voor andere doelen de algemene en abstracte privacybeginselen toe te passen. Het gaat bij deze beginselen om het grondrecht op privacy, de toegestane inbreuken op het grondrecht, de taken en doelen waarvoor gegevens verwerkt worden, doelbinding en verenigbaarheid bij het verstrekken van gegevens en de algemene vereisten van zorgvuldigheid, proportionaliteit en subsidiariteit.
De belangen en de daarbij behorende vuistregels zijn als het ware een ‘vertaling’ van deze abstracte privacybeginselen voor medewerkers om het verstrekken van gegevens in een bepaald geval of een concrete situatie te kunnen beoordelen. Daarnaast is het overzicht van belangen en vuistregels een hulpmiddel om het verstrekken te kunnen beoordelen bij het aanwezig zijn van een (wettelijke) geheimhoudingsverplichting of een (wettelijke) strikte doelbinding.

A-Belangen: het verstrekken geschiedt voor de uitvoering van de eigen taken en werkzaamheden van de verstrekker

Bij A-Belangen worden gegevens verstrekt voor de uitvoering van de eigen taken en werkzaamheden van de verstrekker. A-belangen spelen als een de partij gegevens vraagt aan een andere partij en spelen voor de partij die een overleg organiseert of voor wiens taak een overleg plaatsvindt.

Bezien vanuit het beginsel van doelbinding van de AVG valt het verstrekken bij A-Belangen binnen het algemene doelbindingsbeginsel van art. 5, lid 1, onder b, AVG. Het gaat bij A-Belangen niet om een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld zoals bedoeld in art. 6, lid 4, AVG.
De AVG grondslag is hetzelfde als de AVG-grondslag voor de verstrekker voor verwerken van gegevens voor de eigen taken.

Bij de A-belangen kunnen twee (deel)belangen onderscheiden worden.

A1) De eigen taken en werkzaamheden uit kunnen voeren op basis van informatie, advies of expertise van anderen.
A2) Zicht krijgen op de betrokkenheid van anderen zodat duidelijk wordt of verbinding met de eigen taken en werkzaamheden noodzakelijk is en mogelijk wordt. Bij verbinding met de taken en werkzaamheden van andere partijen kan het gaan om afstemming, om het bevorderen van effectiviteit of om het bewerkstellingen van voortgang en routering.

Vuistregels bij A-Belangen
Vuistregel 1 Bij een A-belang is verstrekken toegestaan. Als er bij de te verstekken gegevens bijzondere gegevens of strafrechtelijke gegevens zijn, dan is verstrekken van die gegevens toegestaan ten behoeve van enkel het geven van een reactie of als ook de ontvanger gerechtigd is om dergelijke gegevens te verwerken.
Vuistregel 2 Uitzondering bij wettelijk beroepsgeheim: medici, jeugdhulpverleners en medewerkers van een Gecertificeerde instelling hebben een zeer specifiek wettelijk beroepsgeheim en daardoor geldt dat verstrekken bij A-belangen altijd specifiek gericht moet zijn op de uitvoering van de medische behandelovereenkomst met de patiënt of specifieke gericht moeten zijn op de uitvoering van jeugdhulp (jeugdhulpverleningsplan) of de uitvoering van een kinderbeschermingsmaatregel of jeugdreclassering (plan van aanpak) . Als dit niet zo is, dan zal een specifieke wettelijke bepaling voor de verstrekking of toestemming nodig zijn of dient het te gaan om een uitzonderingssituatie die doorbreken van de geheimhouding mogelijk maakt (een vitaal belang c.q. een conflict van plichten in verband met een noodtoestand of in verband met goed hulpverlenerschap).
Specifiek voor meldpunten: als de WGBO niet rechtstreeks van toepassing is, maar wel een rol speelt via de schakelbepaling, dan geldt voor medici c.q. BIG-geregistreerden ook vuistregel 1.

B-Belangen: het verstrekken geschiedt ter uitvoering van de taken en werkzaamheden van zowel de verstrekker als de ontvanger waarbij dit (direct) van invloed is op de acties of interventies van beide partijen

Bij B-Belangen worden gegevens verstrekt ter uitvoering van de taken en werkzaamheden van zowel de verstrekker als de ontvanger. Het gaat bij B-belangen om gegevensverstrekking die direct samenhangt en direct van invloed is op de werkzaamheden (acties of interventies) van beide partijen in een bepaald geval. B-belangen kunnen spelen bij het antwoord op een vraag van een andere partij en bij overleg tussen partijen. B-belangen spelen bij overleg vooral als het voor de partij die het overleg organiseert om het A2-belang gaat. B-belangen (met name de B3 en B4-belangen) spelen ook bij ketensamenwerking waarbij de werkzaamheden van de ene partij (verstrekker) overgenomen of voortgezet worden door de volgende partij (ontvanger).

Bezien vanuit het beginsel van doelbinding van de AVG valt het verstrekken bij B-Belangen binnen het algemene doelbindingsbeginsel van art. 5, lid 1, onder b, AVG. Ook bij B-Belangen gaat het niet om een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld zoals bedoeld in art. 6, lid 4, AVG.
De AVG grondslag is hetzelfde als de AVG-grondslagen (combinatie) voor de verstrekker en de ontvanger voor verwerken van gegevens voor de eigen taken.

Bij de B-belangen kunnen vier (deel)belangen onderscheiden worden.

B1) De eigen taken en werkzaamheden afstemmen met andere partijen. Dit om elkaar bijvoorbeeld niet in de weg te lopen en om geen afbreuk te doen aan elkaars acties of interventies.
B2) De eigen taken en werkzaamheden gezamenlijk uitvoeren met die van andere partijen die vanuit hun taken en werkzaamheden ook betrokken zijn. Dit om grotere effectiviteit te bereiken in verband met de onderlinge afhankelijkheid van acties of interventies.
B3) Acties of interventies door andere partijen in gang zetten en mogelijk maken in aanvulling op de eigen taken en werkzaamheden. Dit om grotere effectiviteit te bereiken.
B4) Acties of interventies door andere partijen in gang zetten en mogelijk maken als vervolg op de eigen taken en werkzaamheden die afgerond worden/zijn. Dit om voortgang te bewerkstelligen.

Vuistregels bij B-Belangen

Vuistregel 3 Bij een B-belang is verstrekken toegestaan. Als er bij de te verstekken gegevens bijzondere gegevens of strafrechtelijke gegevens zijn, dan is verstrekken van die gegevens toegestaan als ook de ontvanger gerechtigd is deze gegevens te verwerken.

Vuistregel 4 Uitzondering bij wettelijk beroepsgeheim: Medici, jeugdhulpverleners en medewerkers van een GI hebben een zeer specifiek wettelijk beroepsgeheim en voor hen geldt dat verstrekken zonder toestemming zou kunnen bij een B2, een B3 of een B4-belang. De werkzaamheden van de ontvangende partij dienen dan wel direct verbonden te zijn met de uitvoering van de medische behandelovereenkomst van de medicus met de patiënt of de uitvoering van jeugdhulp, of de uitvoering van een kinderbeschermingsmaatregel of jeugdreclassering (plan van aanpak). Bij een B1-belang is een specifieke wettelijke bepaling voor de verstrekking of toestemming nodig of dient het te gaan om een uitzonderingssituatie die doorbreken van de geheimhouding mogelijk maakt (een vitaal belang c.q. een conflict van plichten in verband met een noodtoestand of in verband met goed hulpverlenerschap).

Specifiek voor meldpunten: als de WGBO niet rechtstreeks van toepassing is, maar wel een rol speelt via de schakelbepaling, dan geldt voor medici c.q. BIG-geregistreerden ook vuistregel 3.

C-Belangen: Het verstrekken geschiedt ter uitvoering van de taken en werkzaamheden van de ontvanger

Bij C-belangen worden gegevens verstrekt ter uitvoering van de taken en werkzaamheden van de ontvanger. De gegevens zijn daarbij (direct) van invloed op de werkzaamheden (acties of interventies) van de ontvanger. Vanuit de verstrekker bezien is de verstrekking van gegevens echter niet (direct) van invloed op de werkzaamheden (acties of interventies) van de verstrekker. C-Belangen spelen vaak een rol als het voor de partij die gegevens vraagt om een A1-belang gaat. De grondslag voor de verstrekking van gegevens is hetzelfde als de AVG-grondslag voor de ontvanger voor het verwerken van gegevens voor de eigen taken.

Bij de C-belangen kunnen twee (deel)belangen onderscheiden worden:

C1) Het verschaffen van informatie voor de uitvoering van de taken en werkzaamheden van de ontvanger in aansluiting op of in verband met de eigen taken en werkzaamheden, waarbij dit niet direct van invloed is op de eigen acties of interventies van de verstrekker.

Bij een C1 belang worden de gegevens voor een (wat) ander doel dan dat waarvoor ze eerder verzameld zijn verstrekt en voldoet (past binnen) het verstrekken voor het andere doel aan het algemene doelbindingsbeginsel van art. 5, lid 1, onder b, AVG én aan de vijf criteria van art. 6, lid 4, AVG over:

- het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de verstrekking;
- het kader waarin de persoonsgegevens zijn verzameld en met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
- de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard worden verwerkt;
- de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
- het bestaan van passende waarborgen.

Bezien vanuit het beginsel van doelbinding van de AVG valt het verstrekken bij C1-Belangen binnen het algemene doelbindingsbeginsel van art. 5, lid 1, onder b, AVG en binnen art. 6, lid 4, AVG.

C2) Het verschaffen van informatie voor de uitvoering van de taken en werkzaamheden van de ontvanger zonder (enig) verband met de uitvoering van de taken en werkzaamheden van de verstrekker.

Bij een C2 belang worden de gegevens voor een (geheel) ander doel dan dat waarvoor ze eerder verzameld zijn verstrekt en voldoet (past binnen) het verstrekken voor het andere doel niet aan de vijf criteria van art. 6, lid 4, AVG. Bezien vanuit het beginsel van doelbinding van de AVG valt het verstrekken bij C2-Belangen buiten het algemene doelbindingsbeginsel van art. 5, lid 1, onder b, AVG en moet het verstrekken binnen de mogelijkheden van art. 6, lid 4, AVG vallen.

Vuistregels bij C-Belangen

Vuistregel 5 Als er een specifieke (wettelijke) geheimhouding of een specifieke (wettelijke) strikte doelbinding is, is verstrekken bij C-belangen niet toegestaan. Verstrekken kan bij C-belangen wel als:

- er een specifieke wettelijke bepaling voor de verstrekking is die doorbreken van de geheimhouding of de strikte doelbinding mogelijk maakt;
- er toestemming voor verstrekken is (de toestemming om de geheimhouding/doelbinding te doorbreken en bij een C2-belang tevens de toestemming van art. 6, lid 4, AVG);
- er een uitzonderingssituatie is die doorbreken van de geheimhouding of strikte doelbinding mogelijk maakt: (een vitaal belang / een conflict van plichten in verband met een noodtoestand of een conflict van plichten in verband met goed hulpverlenerschap)

Als er bij de te verstekken gegevens ook bijzondere gegevens of strafrechtelijke gegevens zijn, dan is verstrekken van die gegevens toegestaan als:

- er uitdrukkelijke toestemming is om die gegevens te verstrekken (de uitdrukkelijke toestemming van art. * UAvg en art. * UAvg);
- de gegevens door de persoon duidelijk openbaar gemaakt zijn;
- er sprake is van een volkenrechtelijke verplichting;
- er een uitzonderingssituatie is in verband met vitaal belang / een conflict van plichten in verband met een noodtoestand of een conflict van plichten in verband met goed hulpverlenerschap;
- het gaat om de instelling, uitoefening of onderbouwing van een rechtsvordering;
- er een specifieke wettelijke bepaling is die aangeeft dat ook bijzondere of strafrechtelijke gegevens verstrekt kunnen worden.

Vanuit een meer juridisch oogpunt kan het bij geheimhoudingen en strikte doelbindingen gaan om:

5a Specifieke wettelijke geheimhouding voor alle gegevens

5b Specifieke wettelijke geheimhouding voor bepaalde gegevens (als er geen wettelijke geheimhouding voor alle gegevens is):

- gegevens verkregen van de politie (art. 7, lid 2, Wpg)
- gegevens verkregen van het OM (art. 52, lid 1, Wjsg)
- gegevens over gezondheid (art. 30, lid 4, AVG).

5c Specifieke wettelijke strikte doelbinding voor alle gegevens

5d Specifieke wettelijke strikte doelbinding voor bepaalde gegevens (als er geen wettelijke strikte doelbinding voor alle gegevens is)*:*

- de bijzondere gegevens anders dan de gegevens over gezondheid
- strafrechtelijke gegevens anders dan verkregen van politie of OM

5e Keuze van de organisatie voor het hanteren van een eigen 'bovenwettelijke' geheimhouding of eigen 'bovenwettelijke' strikte doelbinding voor alle gegevens (als er geen wettelijke geheimhouding of wettelijke strikte doelbinding is).

Vuistregel 6 Als er geen specifieke (wettelijke) geheimhouding of (wettelijke) strikte doelbinding is, is verstrekken bij een C1-belang mogelijk.

Verstrekken bij een C2-belang kan als:

- er een specifieke wettelijke bepaling voor de verstrekking is;
- er toestemming voor verstrekken is (de toestemming van art. 6, lid 4, AVG);
- er een uitzonderingssituatie is in verband met vitaal belang / een conflict van plichten in verband met een noodtoestand;
- er sprake is van een situatie die vermeld is in een algemene wettelijke bepaling zoals bedoeld in art. 6, lid 4, AVG waarin doelen vermeld zijn zoals bedoeld in art. 23, lid AVG.

Als er bij de te verstekken gegevens ook bijzondere categorieën van persoonsgegevens of gegevens van strafrechtelijke aard zijn, dan is verstrekken van die gegevens toegestaan als:

- er uitdrukkelijke toestemming is om ook die gegevens te verstrekken (de uitdrukkelijke toestemming van art. * UAvg);
- de gegevens door de persoon duidelijk openbaar gemaakt zijn;

- er sprake is van een volkenrechtelijke verplichting;
- er een uitzonderingssituatie is in verband met vitaal belang / een conflict van plichten in verband met een noodtoestand;
- het gaat om de instelling, uitoefening of onderbouwing van een rechtsvordering;
- er een specifieke wettelijke bepaling is die aangeeft dat ook bijzondere of strafrechtelijke gegevens verstrekt kunnen worden.

Vuistregel als er een specifieke wettelijke bepaling over verstrekken is

Vuistregel 7 ziet op de situatie dat er een specifieke wettelijke bepaling over verstrekken bestaat. Dan spelen de belangen een minder grote rol bij de vraag óf verstrekt mag worden (want dat staat nu juist in de wettelijke bepaling).

Bij specifieke wettelijke bepalingen over verstrekken kan het gaan om:
7a) bepalingen met een verplichting om te verstrekken;
7b) bepalingen met een bevoegdheid om te verstrekken. Hierbij zijn er:

7b1) bepalingen die in de tekst van de bepaling of gelet op de context aangeven dat ook zonder toestemming en met het doorbreken van een geheimhouding of doorbreken van een strikte doelbinding verstrekt kan worden;

7b2) bepalingen die in de tekst van de bepaling of gelet op de context niet aangeven of waarbij onduidelijk is dat ook zonder toestemming en met doorbreken van een geheimhouding of doorbreken van een strikte doelbinding verstrekt kan worden. Voor deze bepalingen kan het volgende uitgangspunt gehanteerd worden:

7b2.1) als de bepaling opgenomen is in de materiewetgeving van de verstrekker zelf, dan is verstrekken ook bij een geheimhouding of strikte doelbinding toegestaan zonder toestemming;

7b.2.2) als de bepaling opgenomen is in de materiewetgeving van de ontvanger, dan is verstrekken bij een geheimhouding of strikte doelbinding niet toegestaan zonder toestemming.

Of ook bijzondere of strafrechtelijke gegevens verstrekt kunnen worden hangt daarbij af van de tekst of de context van de wettelijke bepaling.

4.2 Verstrekken van gegevens *aan* meldpunten

Het gaat in dit onderdeel om de vraag of en in welke mate burgers en organisaties gegevens kunnen verstrekken *aan* meldpunten. De conclusies van dit onderdeel zijn:

1. Er is geen *specifieke* wettelijke regeling voor het verstrekken van persoonsgegevens *aan* meldpunten;
2. Burgers kunnen ‘als burger’ persoonsgegevens verstrekken aan meldpunten;
3. Organisaties kunnen bij het verstrekken van persoonsgegevens aan meldpunten eveneens het in onderdeel drie beschreven overzicht van belangen en vuistregels gebruiken;
4. De komende WAMS-wetgeving is nodig voor het in een aantal situaties door organisaties kunnen verstrekken van gegevens aan meldpunten. De WAMS-wetgeving is (enkel) nodig om gegevens aan meldpunten te kunnen verstrekken in situaties waarbij de gegevens voor een geheel ander doel aan het meldpunt verstrekt worden dan het doel waarvoor de gegevens eerder verzameld zijn of in bepaalde situaties waarbij toestemming voor het verstrekken nodig is omdat er een geheimhoudingsverplichting of strikte doelbinding voor die gegevens geldt.

Deze conclusies zijn gebaseerd op het volgende:

Burgers vallen als melder en bij het verstrekken van gegevens aan meldpunten niet onder de AVG. Voor wat burgers betreft gaat het als eerste om de vraag of en in hoeverre de AVG wel van toepassing is als zij een melding doen of als burgers antwoord geven op een vraag van een meldpunt. Als eerste zal er, ook bij een melding door burgers, sprake zijn van persoonsgegevens. Het zal bij een melding gaan om al geïdentificeerde personen. Dit valt onder de definitie van persoonsgegevens (art. 4, onder 1, AVG). En ook bij een vraag van een meldpunt om informatie zal er, in ieder geval aan de kant van het meldpunt, sprake zijn van persoonsgegevens.

Als tweede zal er, zelfs bij bijvoorbeeld enkel een mondelinge melding, als zeer snel sprake zijn van het verwerken van persoonsgegevens. Het meldpunt zal de mondeling medegedeelde gegevens immers geheel of gedeeltelijk geautomatiseerd gaan verwerken en/of opslaan in een bestand (art. 2, lid 1, AVG en de definities van verwerking in art. 4, onder 2, AVG en bestand in art. 4, onder 6, AVG).

Voor het doen van een melding is voor burgers ten aanzien van de vraag of de AVG van toepassing is ook art. 2, lid 2, onder c, AVG van belang. Daarin staat dat de AVG niet van toepassing is op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit. Van een zuiver persoonlijke of huishoudelijke activiteit is geen sprake als een burger bijvoorbeeld informatie openbaar op internet publiceert of deze informatie ook werkmatig gebruikt. Bij het doen van een melding zal het voor een burger veelal gaan om een handeling die de burger als diens 'burgerplicht' beschouwd en zich daarbij dus persoonlijk geroepen voelt om de melding te doen. Vanuit dat oogpunt kan het doen van meldingen gerekend worden tot 'zuiver persoonlijke of huishoudelijke activiteiten' van de burger waarop de AVG niet van toepassing is. In overweging 18 bij de AVG wordt bijvoorbeeld gesproken over het voeren van correspondentie. Daarbij dient het uiteraard wel te gaan om kennis en informatie die de burger persoonlijk (en niet beroeps- of arbeidsmatig) heeft. Het op het werk uitprinten van informatie en die vervolgens als burger toevoegen aan een melding valt uiteraard niet meer onder 'zuiver persoonlijke of huishoudelijke activiteiten'. In overweging 18 bij de AVG wordt bijvoorbeeld opgemerkt dat er bij louter persoonlijke of huishoudelijke activiteit geen enkel verband mag zijn met een beroeps of handelsactiviteit. Hetzelfde geldt als burgers antwoord geven op een vraag van een meldpunt.

Organisaties en beroepsbeoefenaren kunnen bij het verstrekken van persoonsgegevens aan meldpunten eveneens het in onderdeel 3 beschreven overzicht van belangen en vuistregels gebruiken. Dit overzicht kan ook voor hen zonder de komende WAMS-wetgeving gebruikt worden. Op basis van het overzicht van belangen en vuistregels gaat het bij het verstrekken van persoonsgegevens aan meldpunt om het volgende:
- Verstrekken bij A2- en B- belangen aan de kant van de verstrekker kan, ook als het om bijzondere of strafrechtelijke gegevens gaat;
- Verstrekken bij C-belangen kan niet bij een strikte doelbinding of een geheimhoudingsverplichting voor de verstrekker. Een strikte doelbinding of geheimhoudingsverplichting geldt in de praktijk voor de meeste partijen en geldt altijd als het om het verstrekken van gegevens over de gezondheid gaat;
- Verstrekken bij een C1 belang kan wel als er geen strikte doelbinding of geheimhoudingsverplichting voor de verstrekker is en als er geen bijzondere of strafrechtelijke gegevens verstrekt worden;
- Verstrekken bij C2 belangen kan niet, ook niet als er geen strikte doelbinding of geheimhoudingsverplichting voor de verstrekker is en als er geen bijzondere of strafrechtelijke gegevens verstrekt worden.

De komende WAMS-wetgeving zal verstrekken bij alle belangen mogelijk maken omdat daarin naar verwachting een specifieke bepaling over het aan meldpunten kunnen verstrekken opgenomen zal worden zoals beschreven bij vuistregel 7 van het overzicht van belangen en vuistregels: organisaties zullen in de WAMS-wetgeving naar verwachting de bevoegdheid krijgen om ook zonder toestemming en met doorbreking van een geheimhoudingsplicht gegevens te verstrekken aan meldpunten.

5 Noodzaak en noodzakelijke gegevens

5.1 Achtergrond over noodzaak en noodzakelijke gegevens

Een belangrijke voorwaarde bij het gebruik van persoonsgegevens is het vereiste van noodzakelijkheid. Deze noodzakelijkheid heeft twee kanten of, zo men wil, stappen. Als eerste moet het noodzakelijk zijn om überhaupt gegevens te gebruiken. Het is duidelijk dat het bij de aanpak van mensenhandel noodzakelijk is om persoonsgegevens te gebruiken. Als tweede gaat het er vervolgens om dat dan enkel de noodzakelijke gegevens gebruikt worden. Er is in die zin sprake van een dubbele noodzakelijkheid (óf gegevens gebruikt worden, en zo ja, welke gegevens dan).

Proportionaliteit, subsidiariteit en dataminimalisatie

Vanuit een juridisch oogpunt gaat het bij de noodzakelijkheid over welke gegevens gebruikt kunnen worden om de eisen van proportionaliteit en subsidiariteit. Bij proportionaliteit gaat het om de afweging tussen middel (de te gebruiken gegevens) en doel (de werkzaamheden c.q. concrete activiteiten waarvoor de gegevens

gebruikt worden). Bij subsidiariteit gaat het er enerzijds om dat zo min mogelijk gegevens gebruikt worden (dataminimalisatie) en anderzijds dat als er een alternatief is, dat alternatief gevolgd wordt. Bij alternatieven kan bijvoorbeeld gedacht worden aan de betrokkene zelf als bron van gegevens of aan een andere partij als bron (verstrekker) van de gegevens.

Opsommen van gegevens en soorten van gegevens

Soms wordt de invulling van het vereiste van noodzakelijkheid getracht te bereiken door de te gebruiken gegevens of soorten van gegevens op te sommen. Het geven van een opsomming van de gegevens of de soorten van gegevens kan inderdaad (enige) richting geven.
Echter, als het daarbij om een opsomming gaat welke gegevens 'maximaal' verwerkt kunnen worden, wordt nog niet aangegeven welke gegevens dan in een bepaald geval inderdaad noodzakelijk zijn. Daarnaast bestaat bij het opsommen van de 'maximale' gegevens ook het risico dat geen of onvoldoende rekening gehouden wordt met de vele verschillende situaties die kunnen spelen waardoor de opsomming te beperkt is.
Als aangegeven zou worden welke gegevens in ieder geval ('minimaal') noodzakelijk zijn, wordt daarmee nog niet aangegeven welke gegevens dan in een bepaald geval in aanvulling op de 'minimale' gegevens ook noodzakelijk (kunnen) zijn.
Een opsomming van 'maximale' of 'minimale' gegevens om daarmee het vereiste van noodzakelijkheid in te vullen, is mogelijk als het om standaard-werkzaamheden, om een gestandaardiseerd werkproces of om gestandaardiseerde en gestructureerde gegevensuitwisseling gaat waarbij alle gevallen in grote mate gelijk zijn en waarbij de gegevens ook precies aangegeven kunnen worden.

Uitgangspunten bij noodzakelijkheid

Een mogelijkheid om handvatten voor het bepalen van de noodzakelijkheid van gegevens te bieden is om uitgangspunten te formuleren. De uitgangspunten zijn een toepassing van de algemene en abstracte privacybeginselen van noodzakelijkheid, proportionaliteit en subsidiariteit en 'need to know' versus 'nice to know'.

'Dat-informatie' en 'uitwendige- of buitenkant-informatie'

Bij vooral het verstrekken en delen van gegevens worden vaak de begrippen 'dat-informatie' en 'uitwendige- of buitenkant-informatie' gebruikt. Bij de vraag welke gegevens in een bepaalde situatie wel of niet noodzakelijk zijn, worden dan als algemene uitgangspunten gehanteerd:

- als met 'dat informatie' volstaan kan worden, gebruik dan enkel 'dat-informatie';
- als met 'uitwendige- of buitenkant-informatie' volstaan kan worden, gebruik dan enkel 'uitwendige- of buitenkant-informatie'.

Alhoewel deze uitgangspunten zeker hun waarde hebben om toe te passen, zijn er een aantal zaken die nadere aandacht verdienen. Zo is er soms het misverstand dat het gebruik van 'dat-informatie' altijd wel toegestaan zou zijn. Daarnaast is het onderscheid tussen 'dat-informatie', 'uitwendige- of buitenkant informatie' en inhoudelijk informatie niet altijd scherp te maken. Factoren die tevens een rol spelen zijn het eventueel aanwezig zijn van een specifieke wettelijke bepaling over het verstrekken van gegevens, of er een specifiek beroepsgeheim voor de verstrekker van gegevens is en de belangen die voor de verstrekkende partij spelen.

'Dat-informatie'

Met 'dat'-informatie' wordt het gegeven bedoeld dát een organisatie bij een persoon of een casus is betrokken is, dan wel dát een persoon bekend is bij een bepaalde organisatie of bekend is in een bepaald gegevensbestand of register. Dit dan zonder vermelding van andere gegevens over die persoon en zonder gegevens over de inhoud van bijvoorbeeld de hulpverlening, de begeleiding of de ondersteuning. Bij 'dat-informatie' kan ook wel gesproken worden over "ja/nee-informatie": op de vraag of iemand bekend is, volgt dan de reactie 'ja of nee'. Bij het bevragen van registers wordt ook wel gesproken over 'hit/no-hit informatie'.

Het is, zoals al is aangegeven, een misverstand om 'dat-informatie' als privacy-neutraal aan te merken of om te veronderstellen dat het gebruik van 'dat-informatie' (altijd) toegestaan is omdat het enkel maar om 'dat-

informatie' gaat. Ook het enkele feit dát iemand bekend is, is een persoonsgegeven en kan tevens al (veel) context-informatie opleveren. Of en in welke mate het enkele feit dát iemand bekend is tevens extra context-informatie oplevert, hangt in overgrote mate af van de persoon of instantie die het antwoord geeft. Zo zal bijvoorbeeld een bevestigend antwoord van een gespecialiseerd medicus ook informatie opleveren over het soort aandoening van de persoon. En een 'ja-antwoord' van een specifieke politieafdeling of een specifiek politieteam zal ook informatie over het soort strafbare feiten opleveren.

Als vuistregel kan voor eventuele (extra) context-informatie gehanteerd worden: hoe specifieker de doelgroep is waar de persoon of instantie die antwoord geeft zich op richt, hoe meer context-informatie dit antwoord op zal leveren. Hetzelfde geldt als een gegevensverzameling of een register zoals bijvoorbeeld een verwijsindex geraadpleegd wordt: hoe specifieker de groep van personen is waarover gegevens in die verzameling of dat register zijn opgenomen, hoe meer context-informatie een antwoord (een 'hit') op zal leveren.

In de praktijk zal er bij 'dat-informatie' dan ook al snel en tegelijkertijd sprake zijn van tenminste 'uitwendige- of buitenkant-informatie'. En soms zal er ook bij enkel 'dat-informatie' tegelijkertijd sprake kunnen zijn van inhoudelijke informatie. Zo zal bijvoorbeeld het feit dat iemand opgenomen is in een kliniek voor epilepsie of als leerling ingeschreven is op een blindenschool, al meteen de aard van de aandoening aangeven. En het feit dat iemand op de kieslijst van een bepaalde politieke partij of vakbond staat, zal al direct zicht geven op de politieke overtuiging of op het lid zijn van een vakbond. Deze twee voorbeelden geven aan dat er zelfs bij enkel 'dat-informatie' al sprake kan zijn van bijzondere categorieën van persoonsgegevens.

'Uitwendige- of buitenkant-informatie'

Bij 'uitwendige- of buitenkant-informatie' gaat het om meer informatie dan enkel 'dat-informatie' of 'ja/nee', maar gaat het nog niet om (specifieke) inhoudelijke informatie. Alhoewel een onderscheid tussen enerzijds 'uitwendige- of buitenkant-informatie' en anderzijds inhoudelijke informatie niet altijd even scherp te maken is, kunnen wel wat voorbeelden gegeven worden.

'Uitwendige- of buitenkant-informatie':

- is niet de medisch inhoudelijke informatie zoals bijvoorbeeld de aard en oorzaak (diagnose) en de behandeling van een ziekte of de voorgeschreven medicatie. 'Buitenkant' is dus niet de diagnose dat er sprake is van schizofrenie, maar eventueel wel de mededeling door de behandelend medicus dat er sprake kan zijn van 'onvoorspelbaar impulsief agressief gedrag' . En 'buitenkant' is niet welke medicijnen voorgeschreven zijn, maar eventueel wel dat het noodzakelijk is dat medicatie ook regelmatig ingenomen wordt;
- is bij informatie van de politie niet welke strafbare feiten gepleegd zijn en de omstandigheden die daarbij aanwezig waren, maar eventueel wel dat er meerdere relevante strafbare feiten zijn voor de situatie of casus waarbij de gegevens verstrekt worden.

Specifieke uitgangspunten voor inhoudelijke gegevens

Naast de meer algemene uitgangspunten over 'dat- en uitwendige- of buitenkant-informatie' kunnen een aantal specifieke uitgangspunten gebruikt worden over noodzakelijkheid van verschillende categorieën van inhoudelijke gegevens. Daarbij kan dan per fase of situatie binnen een bepaald werkproces aangegeven worden of deze gegevens wel of niet noodzakelijk (kunnen) zijn. De categorieën van inhoudelijke gegevens die bij het bepalen van de noodzaak gebruikt zouden kunnen worden zijn:

- er is een wettelijke verplichting voor gebruik van de (specifiek benoemde) gegevens (denk aan gegevens die bij een aanvraag of vergunning verplicht zijn of verplichte identiteitsvaststelling);
- zonder de gegevens kunnen de werkzaamheden of interventie niet uitgevoerd worden (denk aan personalia of (formele) voorwaarden);
- zonder de gegevens loopt het fout (denk aan veiligheid en bescherming);
- de gegevens zijn nodig om de werkzaamheden op inhoudelijk goede / verantwoorde / te verantwoorden wijze uit te voeren (denk aan professionele standaarden). Anders gezegd: zonder de gegevens is het nog maar de vraag of de werkzaamheden op inhoudelijk juiste wijze uitgevoerd worden;
- de gegevens geven een beeld van de situatie;

- de gegevens zorgen voor een efficiënte uitvoering (lees: het zou zonder de gegevens kunnen, maar of de werkzaamheden dan efficiënt uitgevoerd worden is nog maar de vraag);
- de gegevens vergemakkelijken de werkzaamheden of interventie: het is handig om de gegevens te hebben;
- mogelijk zijn de gegevens op een later tijdstip nodig.

Op welke wijze de uitgangspunten om te kunnen bepalen welke gegevens noodzakelijk zijn in de praktijk wordt hieronder nader uitgewerkt in een aantal tabellen en uitgangspunten.

5.2 Uitwerking uitgangspunten noodzaak meldpunten en verstrekken door meldpunten

5.2.1 Vastleggen gegevens in dossiers meldpunt

	Vastleggen gegevens in dossiers meldpunt Uitgangspunten bij verschillende soorten gegevens	Gegevens (met uitzondering van bijzondere en strafrechtelijke gegevens)	Bijzondere gegevens	Strafrechtelijke gegevens
1	Wettelijke verplichting voor gebruik van de (specifiek benoemde) gegevens (denk aan gegevens die bij een aanvraag of vergunning verplicht zijn of aan verplichte identiteitsvaststelling)	OK, maar niet aanwezig	OK, maar niet aanwezig	OK, maar niet aanwezig
2	Zonder de gegevens kunnen de werkzaamheden of interventie niet uitgevoerd worden (denk aan personalia of (formele) voorwaarden, zoals leeftijd of inwoner van de gemeente)	OK	OK, maar uitzondering	OK, maar uitzondering
3	Zonder de gegevens loopt het fout (denk aan veiligheid voor en de bescherming van personen)	OK	OK	OK
4	De gegevens zijn nodig om de werkzaamheden op inhoudelijk goede / verantwoorde / te verantwoorden wijze uit te voeren (professionele standaarden) Anders gezegd: zonder de gegevens is het nog maar de vraag of de werkzaamheden op inhoudelijk juiste wijze uitgevoerd worden	OK	OK	OK
5	De gegevens geven een beeld van de situatie *	Kan	Kan	Kan
6	De gegevens zorgen voor een efficiënte uitvoering door meldpunt (het zou zonder de gegevens kunnen, maar of de werkzaamheden dan efficiënt uitgevoerd worden is nog maar de vraag)	Kan	Neen	Kan bij melding door politie, maar beperk tot 'dat- of 'buitenkant-informatie'
7	De gegevens vergemakkelijken de werkzaamheden of interventie: het is handig om de gegevens te hebben	Neen	Neen	Neen
8	Mogelijk zijn de gegevens op een later tijdstip nodig	Neen	Neen	Neen

* Voor een meldpunt behoort het verkrijgen van een beeld van de situatie tot de (kern)werkzaamheden en voor hen valt dit ook onder 4)

5.2.2 Informatievragen door meldpunt

Algemeen: beperk de te verstrekken informatie in **alle** gevallen (gegevens, bijzondere en strafrechtelijke gegevens) zoveel mogelijk tot 'dat- of 'buitenkant-informatie', vooral bij bijzondere en strafrechtelijke gegevens

	Informatievragen door meldpunt Uitgangspunten bij verschillende soorten gegevens	Gegevens (met uitzondering van bijzondere en strafrechtelijke gegevens)	Bijzondere gegevens	Strafrechtelijke gegevens
1	Wettelijke verplichting voor gebruik van de (specifiek benoemde) gegevens (denk aan gegevens die bij een aanvraag of vergunning verplicht zijn of aan verplichte identiteitsvaststelling)	OK, maar niet aanwezig	OK, maar niet aanwezig	OK, maar niet aanwezig
2	Zonder de gegevens kunnen de werkzaamheden of interventie niet uitgevoerd worden (denk aan personalia of (formele) voorwaarden, zoals leeftijd of inwoner van de gemeente)	OK	OK, maar uitzondering	OK, maar uitzondering
3	Zonder de gegevens loopt het fout (denk aan veiligheid voor en de bescherming van personen)	OK	OK	OK
4	De gegevens zijn nodig om de werkzaamheden op inhoudelijk goede / verantwoorde / te verantwoorden wijze uit te voeren (professionele standaarden) Anders gezegd: zonder de gegevens is het nog maar de vraag of de werkzaamheden op inhoudelijk juiste wijze uitgevoerd worden	OK	OK	OK
5	De gegevens geven een beeld van de situatie	Neen	Neen	Neen
6	De gegevens zorgen voor een efficiënte uitvoering door meldpunt (het zou zonder de gegevens kunnen, maar of de werkzaamheden dan efficiënt uitgevoerd worden is nog maar de vraag)	Neen	Neen	Neen
7	De gegevens vergemakkelijken de werkzaamheden of interventie: het is handig om de gegevens te hebben	Neen	Neen	Neen
8	Mogelijk zijn de gegevens op een later tijdstip nodig	Neen	Neen	Neen

5.2.3 Overdracht aan ander meldpunt

Algemeen: gehele dossiers melding

5.2.4 Uitzetten vervolgacties

Algemeen: gegevens op maat per partij en niet alles (dezelfde set van gegevens)aan alle partijen
Indien met uitwendig volstaan kan worden (bijzondere en strafrechtelijke gegevens)

	Uitzetten vervolgacties Uitgangspunten bij verschillende soorten gegevens	Gegevens (met uitzondering van bijzondere en strafrechtelijke gegevens)	Bijzondere gegevens	Strafrechtelijke gegevens
1	Wettelijke verplichting voor gebruik van de (specifiek benoemde) gegevens (denk aan gegevens die bij een aanvraag of vergunning verplicht zijn of aan verplichte identiteitsvaststelling)	OK, maar niet aanwezig	OK, maar niet aanwezig	OK, maar niet aanwezig
2	Zonder de gegevens kunnen de werkzaamheden of interventie niet uitgevoerd worden (denk aan personalia of (formele) voorwaarden, zoals leeftijd of inwoner van de gemeente)	OK	OK, maar uitzondering	OK, maar uitzondering
3	Zonder de gegevens loopt het fout (denk aan veiligheid voor en de bescherming van personen)	OK	OK	OK
4	De gegevens zijn nodig om de werkzaamheden op inhoudelijk goede / verantwoorde / te verantwoorden wijze uit te voeren (professionele standaarden) Anders gezegd: zonder de gegevens is het nog maar de vraag of de werkzaamheden op inhoudelijk juiste wijze uitgevoerd worden	OK	OK, maar beperk zo mogelijk tot dat- of 'buitenkant-informatie'	OK, maar beperk zo mogelijk tot dat- of 'buitenkant-informatie'
5	De gegevens geven een beeld van de situatie	Neen	Neen	Neen
6	De gegevens zorgen voor een efficiënte uitvoering door meldpunt (het zou zonder de gegevens kunnen, maar of de werkzaamheden dan efficiënt uitgevoerd worden is nog maar de vraag)	Neen	Neen	Neen
7	De gegevens vergemakkelijken de werkzaamheden of interventie: het is handig om de gegevens te hebben	Neen	Neen	Neen
8	Mogelijk zijn de gegevens op een later tijdstip nodig	Neen	Neen	Neen

5.2.5 informeren melder

Algemeen: Beperk tot 'dat- of 'buitenkant-informatie' en geen bijzondere of strafrechtelijke gegevens (niet inhoud en ook niet welke GGZ-behandelaar bijvoorbeeld)

5.2.6 Verstrekken door partijen aan meldpunten

	Verstrekken aan meldpunt Uitgangspunten bij verschillende soorten gegevens	Gegevens (met uitzondering van bijzondere en strafrechtelijke gegevens)	Bijzondere gegevens	Strafrechtelijke gegevens
1	Wettelijke verplichting voor gebruik van de (specifiek benoemde) gegevens (denk aan gegevens die bij een aanvraag of vergunning verplicht zijn of aan verplichte identiteitsvaststelling)	OK, maar niet aanwezig	OK, maar niet aanwezig	OK, maar niet aanwezig
2	Zonder de gegevens kunnen de werkzaamheden of interventie niet uitgevoerd worden (denk aan personalia of (formele) voorwaarden, zoals leeftijd of inwoner van de gemeente)	OK	OK, maar uitzondering	OK, maar uitzondering
3	Zonder de gegevens loopt het fout (denk aan veiligheid voor en de bescherming van personen)	OK	OK	OK
4	De gegevens zijn nodig om de werkzaamheden op inhoudelijk goede / verantwoorde / te verantwoorden wijze uit te voeren (professionele standaarden) Anders gezegd: zonder de gegevens is het nog maar de vraag of de werkzaamheden op inhoudelijk juiste wijze uitgevoerd worden	OK	OK, maar beperk zo mogelijk tot dat- of 'buitenkant-informatie'	OK, maar beperk zo mogelijk tot dat- of 'buitenkant-informatie'
5	De gegevens geven een beeld van de situatie *	Kan	Kan, maar beperk zo mogelijk tot dat- of 'buitenkant-informatie'	Kan, maar beperk zo mogelijk tot dat- of 'buitenkant-informatie'
6	De gegevens zorgen voor een efficiënte uitvoering door meldpunt (het zou zonder de gegevens kunnen, maar of de werkzaamheden dan efficiënt uitgevoerd worden is nog maar de vraag)	Kan, maar beperk tot dat- of 'buitenkant-informatie'	Neen	Neen
7	De gegevens vergemakkelijken de werkzaamheden of interventie: het is handig om de gegevens te hebben	Neen	Neen	Neen
8	Mogelijk zijn de gegevens op een later tijdstip nodig	Neen	Neen	Neen

* Voor een meldpunt behoort het verkrijgen van een beeld van de situatie tot de (kern)werkzaamheden en voor hen valt dit ook onder 4)

6 Het informeren van betrokkenen op grond van de AVG

Dit onderdeel gaat over het op grond van de AVG verplicht informeren van betrokkenen over het feit dat persoonsgegevens verwerkt worden. De conclusies van dit onderdeel zijn:

1. De informatieplicht van de AVG is voor meldpunten (goed) uitvoerbaar in de praktijk en deze levert geen belemmeringen op voor meldpunten bij het uitvoeren van hun werkzaamheden;

2. De informatieplicht van de AVG is uitvoerbaar in de praktijk voor partijen die gegevens aan meldpunten verstrekken. Deze partijen kunnen bijvoorbeeld op eenzelfde wijze als de meldpunten gebruik maken van de uitzonderingen op de informatieplicht van art. 41, lid 1, AVG;
3. Bij de komende WAMS-wetgeving zal de informatieplicht van de AVG voor zowel meldpunten als voor partijen die persoonsgegevens *aan* meldpunten verstrekken naar verwachting vervallen voor gegevens die niet van de betrokkene zelf verkregen worden of eerder verkregen zijn (art. 14 AVG);
4. De informatieplicht voor gegevens die bij de betrokkene zelf verzameld zijn of worden (van de betrokkene verkregen zijn of worden) zal bij de komende WAMS-wetgeving blijven bestaan (art. 13 AVG).

Deze conclusies zijn gebaseerd op het volgende:

De AVG bevat in de artikelen 12, 13 en 14 een uitgebreide informatieplicht. In de praktijk gaat het bij meldingen om de informatieplicht van art. 14 AVG over situaties wanneer de persoonsgegevens niet van de betrokkene zelf verkregen worden. Bij een melding is dit het geval. Daarnaast geldt voor meldpunten de informatieplicht van art. 13 AVG wanneer de persoonsgegevens bij de betrokkene zelf worden verzameld. Voor meldpunten speelt art. 13 AVG als het meldpunt contact opneemt met de betrokkene.
Op grond van art. 14 , lid 3, AVG is het informeren vereist:
a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.
Op grond van art. 13, lid 1, AVG is het informeren vereist op het moment dat de gegevens bij de betrokkene verkregen worden.

De informatieplicht van de AVG kan op twee manieren uitgevoerd worden.
1. Het afzonderlijk AVG-informeren (los van inhoudelijk contact met de betrokkene bij de uitvoering van de werkzaamheden). Hierbij ontvangt de betrokkene veelal een afzonderlijke AVG-informatiebrief c.q. mededeling.
2. Het AVG-informeren 'meenemen' tijdens de uitvoering van de werkzaamheden. Hierbij is er voor de uitvoering van de inhoudelijke werkzaamheden contact met de betrokkene en die wordt daarbij dan tevens over de gegevensverwerking geïnformeerd.

Het afzonderlijk AVG-informeren door het meldpunt met bijvoorbeeld een afzonderlijke AVG-informatiebrief c.q. mededeling is (los van het moment van inhoudelijk contact met de betrokkene) niet noodzakelijk (mag wel) in de volgende gevallen. Een essentiële voorwaarde bij deze gevallen is wel dat er dan op een website van het meldpunt eenvoudig vindbare en duidelijk informatie is over het door het meldpunt verwerken van persoonsgegevens (zie ook art. 12, lid 1, AVG).

De gevallen waarin een afzonderlijke AVG-informatiebrief brief of -mededeling niet noodzakelijk is zijn:

- de melder heeft al medegedeeld dat een melding gedaan zal worden of gedaan is;
- de melding wordt (direct) en zonder verdere informatieverzameling overgedragen aan een ander meldpunt of andere partij die de betrokkene zal informeren en daarbij tevens aan zal geven dat het meldpunt eerder gegevens over de melding verwerkt heeft;
- bij c.q. tijdens het onderzoek door het meldpunt wordt contact opgenomen met de betrokkene waar de melding betrekking op heeft en daarbij wordt deze geïnformeerd over de gegevensverwerking;
- het meldpunt wil voor de inhoudelijke uitvoering van de werkzaamheden contact opnemen met de betrokkene waar de melding betrekking op heeft en kan deze, ondanks enkele pogingen, niet bereiken en de partij die de vervolgactie uit zal voeren zal de betrokkene informeren en zal daarbij aangeven dat het meldpunt eerder gegevens over de melding verwerkt heeft;
- er is bij het behandelen van de melding sprake van een situatie zoals bedoeld in art. 41, lid 1, UAvg (zie hieronder) en de partij die de vervolgactie uit zal voeren zal de betrokkene informeren en zal daarbij tevens aangeven dat het meldpunt eerder gegevens over de melding verwerkt heeft. In situaties waarbij de melder betrokkene niet geïnformeerd heeft en waarbij het meldpunt geen contact kan krijgen met de betrokkene waar de melding over gaat, kan in veel gevallen (tijdelijk) een beroep

gedaan worden door het meldpunt op de uitzondering van art. 41, lid 1, onder i, AVG (zie hieronder met toelichting).

Art. 14, lid 3, onder a, AVG gaat er vanuit, dat de betrokkene uiterlijk één maand na het ontvangen van de melding geïnformeerd wordt. Als er geen contact met de betrokkene is en als de vervolgactie binnen één maand start en de partij die de vervolgactie uitvoert de betrokkene informeert en daarbij tevens informeert over het feit dat het meldpunt eerder gegevens over de melding verwerkt heeft, dan zou het afzonderlijk AVG-informeren (wellicht helemaal) niet nodig zijn. Of een dergelijke handelwijze mogelijk is, is echter onzeker omdat in art. 14, lid 3, onder c, AVG ook geregeld is dat het informeren plaats moet vinden uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt aan een andere ontvanger. Het is duidelijk dat de partij die gegevens van het meldpunt ontvangt om een vervolgactie uit te voeren een ontvanger is zoals hier is bedoeld. Informeren moet dan plaatsvinden op het moment van verstrekken aan de partij voor de vervolgactie en dit moment kan samenvallen met het moment waarop de partij die de vervolgactie doet de betrokkene informeert. Het is echt wat onduidelijk of er bij de situaties dat partijen tijdens het onderzoek om aanvullende informatie gevraagd wordt ook sprake is van verstrekken aan een ontvanger omdat die partijen enkel 'vraag-gegevens' krijgen en deze veelal enkel voor het beantwoorden zullen gebruiken en mogelijk niet zullen gebruiken voor hun eigen werkzaamheden. Hierbij speelt natuurlijk ook of het op basis van deze redenering niet informeren van de betrokkene nog wel behoorlijk en zorgvuldig is. Het gebruiken van deze situatie om niet te informeren wordt dan ook ten zeerste afgeraden.

Het afzonderlijk AVG-informeren is in ieder geval nodig als er geen vervolgacties komen en er door het meldpunt tijdens het behandelen van de melding geen contact geweest is met de betrokkene. Naar verwachting zullen dergelijke situaties niet vaak voor komen. Dit informeren is nodig uiterlijk binnen één maand na de ontvangst van de melding of op het moment dat één van de situaties zoals bedoeld in art. 41, lid 1, UAvg niet meer van toepassing is. In het meldingendossier dient gemotiveerd vastgelegd te worden waarom een dergelijke uitzondering voor het niet-informeren aanwezig is.

In art. 41, lid 1, UAvg gaat het om de volgende situaties waarbij het informeren van de betrokkene (zolang de uitzondering van toepassing is) achterwege kan blijven. Met **vette** tekst is aangegeven welke situaties bij meldingen aan de orde zouden kunnen zijn.
De uitzonderingen zijn:

a. de nationale veiligheid
b. landsverdediging;
c. de openbare veiligheid;
d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, **met inbegrip van** monetaire, budgettaire en fiscale aangelegenheden, **volksgezondheid en sociale zekerheid**;
f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of

Toelichting: bij de bescherming van de rechten en vrijheden van anderen kan het bijvoorbeeld gaan om de bescherming van de melder of de goede taakuitvoering van de werkzaamheden van het meldpunt zelf. De taakuitvoering van het meldpunt zelf zal spelen als het informeren de uitvoering van die werkzaamheden teveel en onevenredig zou belemmeren. Een voorbeeld hierbij is de situatie dat aangenomen kan worden dat een betrokkenen zodra deze weet krijgt van de melding zal vertrekken c.q. zich 'onvindbaar' zal maken of zich zal (gaan) onttrekken aan zorg- en hulpverlening.

j.de inning van civielrechtelijke vorderingen.

Partijen die persoonsgegevens aan meldpunten verstrekken, kunnen op eenzelfde wijze als de meldpunten gebruik maken van de hierboven weergegeven uitzonderingen op de informatieplicht van art. 41, lid 1, AVG. Deze partijen behoeven ook niet aan de informatieplicht te voldoen als ze de betrokkene niet kunnen bereiken of als ze geen contactinformatie voor de betrokkene hebben (vgl. art. 11, lid 1, AVG waarin bepaald is dat indien de doeleinden waarvoor een verwerkingsverantwoordelijke persoonsgegevens verwerkt, niet of niet meer vereisen dat hij een betrokkene identificeert, hij niet verplicht is om, uitsluitend om aan deze verordening te voldoen, aanvullende gegevens ter identificatie van de betrokkene bij te houden, te verkrijgen of te verwerken.).

Zodra de komende WAMS-wetgeving er zal zijn en daarbij ook het door het meldpunt verkrijgen en verstrekken van gegevens uitdrukkelijk regelt, zal de AVG informatieplicht van art. 14 AVG vervallen. Dit omdat in art. 14, lid 5, onder c, AVG geregeld is dat de informatieplicht van art. 14 AVG niet van toepassing is als het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen. Bij de passende maatregelen valt de denken aan een geheimhoudingsverplichting die op de ontvangen gegevens rust. Ook is het daarbij van belang om het werkproces in te richten zoals in deze rapportage wordt aangegeven en het feit dat partijen die een vervolgactie ondernemen alsnog over de eerdere verwerking door het meldpunt kunnen informeren.
De informatieplicht van art. 13 AVG voor de situaties wanneer de persoonsgegevens bij de betrokkene zelf worden verzameld zal ook bij de komende WAMS-wetgeving blijven bestaan.