Meldpunten niet-acuut

Handvatten voor de inrichting van een zorgvuldige en rechtmatige gegevensverwerking

Inhoudsopgave

1 Inleiding en leeswijzer

In het kader van een sluitende aanpak voor kwetsbare personen is het beleid erop gericht dat gemeenten meldpunten inrichten waar burgers en instanties meldingen kunnen doen over personen die (volgens de melder) waarschijnlijk een niet acute behoefte tot ondersteuning hebben1. Op dit moment wordt op veel plaatsen in Nederland al vormgegeven aan deze meldpunten. In veel gevallen wordt daarbij voortgebouwd op de al bestaande meldpunten OGGZ en de meldpunten Zorg en Overlast. Uitgangspunt is dat niemand tussen wal en schip mag vallen. Dat betekent dat indien iemand wordt gemeld het meldpunt op zoek gaat naar de juiste hulp. Pas als er een instantie of professional is gevonden die de zaak oppakt, beschouwt het meldpunt de melding als afgerond. Bij veel gemeenten is er een beweging zichtbaar dat deze 'meldpunten niet-acuut' en de meldpunten in het kader van de Wet verplichte geestelijke gezondheidszorg (Wvggz) in één meldpunt worden georganiseerd.

De meldpunten niet-acuut hebben tot taak om meldingen te beoordelen, de beller handelingsperspectief te bieden en mensen met een behoefte aan ondersteuning door te geleiden naar de instantie die passende ondersteuning kan bieden, of daarnaartoe kan leiden. Soms kan worden volstaan met een advies aan de melder of gemelde. In andere gevallen wordt doorgeleid naar een andere instantie, of naar een andere afdeling binnen de organisatie waar het meldpunt is onder gebracht, bijvoorbeeld de afdeling bemoeizorg. Waar mogelijk vindt de doorgeleiding zo veel mogelijk plaats na contact met en in overleg met de gemelde persoon. Alle meldpunten checken na enige tijd of de melding kan worden afgesloten. Dat doen zij door bij de vervolginstantie te checken of vervolgacties daadwerkelijk hebben plaats gevonden. Ook checken de meeste bij de melder of gemelde of zij voldoende geholpen zijn.

De meldpunten niet-acuut en gegevensverwerking

Deze handreiking gaat over de juridische basis en de inrichting van de gegevensverwerking in de meldpunten niet-acuut. Welke gegevens mag het meldpunt verwerken en op welke wettelijke basis? Welke gegevens mogen instanties of professionals verstrekken aan het meldpunt ten behoeve van haar taak? Hoe richten we de informatiehuishouding zo in dat deze voldoet aan de eisen van zorgvuldigheid die de burger van de overheid mag verwachten? Waar moeten professionals rekening mee houden als ze hun werkzaamheden in het meldpunt uitvoeren? En wat betekent werken in een meldpunt voor BIG-geregistreerde medewerkers?

Doel van deze handreiking is om de gemeente en de organisatie die de meldpuntfunctie namens de gemeente uitvoert inzicht te geven in:

- De juridische basis voor de gegevensverwerking t.b.v. het meldpunt;
- De organisatieaspecten die van belang zijn bij de inrichting van de gegevensverwerking in het meldpunt;
- Antwoorden op veel gestelde vragen voor projectmanagers en professionals bij het uitvoeren van de meldpunttaak.

Daarnaast zal in deze handreiking aandacht besteed worden aan de samenloop van meldpunten niet- acuut met de meldpunten Wvggz en aan de relatie met bemoeizorg.

1 Deze sluitende aanpak en meldpunten bouwen voort op de aanbevelingen van het schakelteam Personen met verward gedrag. Het kan daarbij gaan om een ondersteuningsbehoefte op het gebied van zorg, hulp en of begeleiding. Deze handreiking gaat niet over meldingen bij crisissituaties of de meldpunten Wet verplichte geestelijke gezondheidszorg.

Complexiteit bij de juridische vormgeving van meldpunten niet-acuut

Bij het schrijven van deze handreiking deed zich de complexiteit voor dat er op dit moment geen specifieke wettelijke regeling is voor het oprichten van meldpunten niet-acuut. De eerdere meldpunten OGGZ vonden hun basis in het betreffende prestatieveld van de Wmo. Echter met de Wmo 2015 is de meldpunttaak niet meer expliciet belegd.2 In zijn brief van 20 september 2018 heeft de staatssecretaris van VWS aan de colleges van burgemeester en wethouders benoemd dat de OGGZ-taak en daarmee ook de bijbehorende meldpunttaak, wel degelijk behoort tot de opdracht aan gemeenten in het kader van de Wmo 2015. Het ontbreken van een expliciete meldpunttaak heeft echter wel gevolgen voor het juridisch kader voor de gegevensverwerking. Om de gegevensverwerkingen die nodig zijn voor het goed vervullen van de meldpunttaak mogelijk te maken, is het nodig om gebruik te maken van de gecombineerde taken en zorgplichten van het college van B&W en de burgemeester. Dit is complex. In hoofdstuk 3 wordt hier uitgebreid op ingegaan.

Leeswijzer

De handreiking kent, naast een algemene introductie over de meldpunten niet-acuut, drie hoofdstukken die elk een andere doelgroep bedienen. Om ervoor te zorgen dat de hoofdstukken afzonderlijk leesbaar zijn, komen sommige onderdelen op meerdere plaatsen terug.

Hoofdstuk 2 bevat een algemene introductie over het meldpunt niet-acuut. In dit hoofdstuk wordt een generiek werkproces geschetst op basis van de ervaringen van de pilots van de meldpunten niet-acuut. Ook is er aandacht voor de samenloop met het meldpunt Wvggz en de relatie met bemoeizorg.

Hoofdstuk 3 bevat een juridische analyse t.b.v. de gegevensverwerking door het meldpunt en de partijen die informatie verstrekken aan het meldpunt. Dit gedeelte richt zich met name op projectleiders, juristen, privacy-officers en Functionarissen Gegevensbescherming van bij het meldpunt betrokken partijen.

Hoofdstuk 4 bevat een uitgebreide Privacy Impact Analyse op basis van de werkwijzen van een tiental meldpunten die betrokken waren bij deze handreiking. Zij geeft inzicht in privacy-risico's bij verschillende werkwijzen en organisatiewijzen en schetst de maatregelen die genomen kunnen worden om de kans op het optreden van die risico's te verkleinen. Dit gedeelte richt zich met name op projectleiders, managers en medewerkers die zich bezighouden met de organisatie en inrichting van de werkprocessen en informatiehuishouding van het meldpunt.

Hoofdstuk 5 biedt praktische tips voor de het inrichten van de gegevensverwerking en voor de zorgvuldige omgang met gegevens tijdens het dagelijkse werk aan de hand van veel gestelde vragen. In paragraaf 5.2 van dit hoofdstuk zijn enkele casussen beschreven die laten zien hoe een zorgvuldige gegevensverwerking er in de praktijk uit kan zien. Dit gedeelte richt zich met name op professionals. Uitgangspunt daarbij is dat de betrokken organisaties hun huiswerk op basis van hoofdstuk 3 en 4 goed hebben gedaan zodat de professionals zich niet bezig hoeven te houden met de juridische aspecten van de gegevensverwerking, maar vooral met zorgvuldige afwegingen ten aanzien van de noodzakelijke gegevensverwerking op basis van de inhoud van de problematiek.

2 Het kabinet heeft het Wetsvoorstel Aanpak Meervoudige Problematiek Sociaal Domein (WAMS) in voorbereiding. Dit wetsvoorstel expliciteert de meldpunttaak voor de colleges van b&w. Daarmee zou er weer een duidelijke juridische basis ontstaan voor de noodzakelijke gegevensverwerking ten behoeve van de meldpunten niet-acuut. De inwerkingtreding van de WAMS wordt voorzien niet eerder dan 1 januari 2022.

2 Meldpunten niet-acuut

2.1 Meldpunten niet-acuut

De primaire taak van het meldpunt niet-acuut is om ervoor te zorgen dat een burger of professional die meldt, of de burger waarover wordt gemeld, een advies krijgt waarmee hij zelf verder kan. Of, indien nodig, ervoor te zorgen dat de juiste instantie of professional actie onderneemt om de gemelde of de melder verder te helpen. Typische activiteiten die daarbij horen zijn risicotaxatie, triage, advisering aan melder of gemelde en indien nodig het doorgeleiden naar de juiste behandelaar of voorziening.

In deze handreiking wordt de meldpuntfunctie onderscheiden van andere activiteiten die er soms wel nauw mee verbonden zijn. Het inzetten van bemoeizorg bijvoorbeeld, wordt gezien als een mogelijke uitkomst van het meldproces, maar niet als onderdeel ervan. Hetzelfde geldt voor het inschakelen van het wijkteam, of het doorgeleiden naar een GGZ-instelling. Dit zijn mogelijke uitkomsten van het meldproces.

In paragraaf 2.2 wordt nader ingegaan op het primaire proces van het meldpunt niet-acuut.

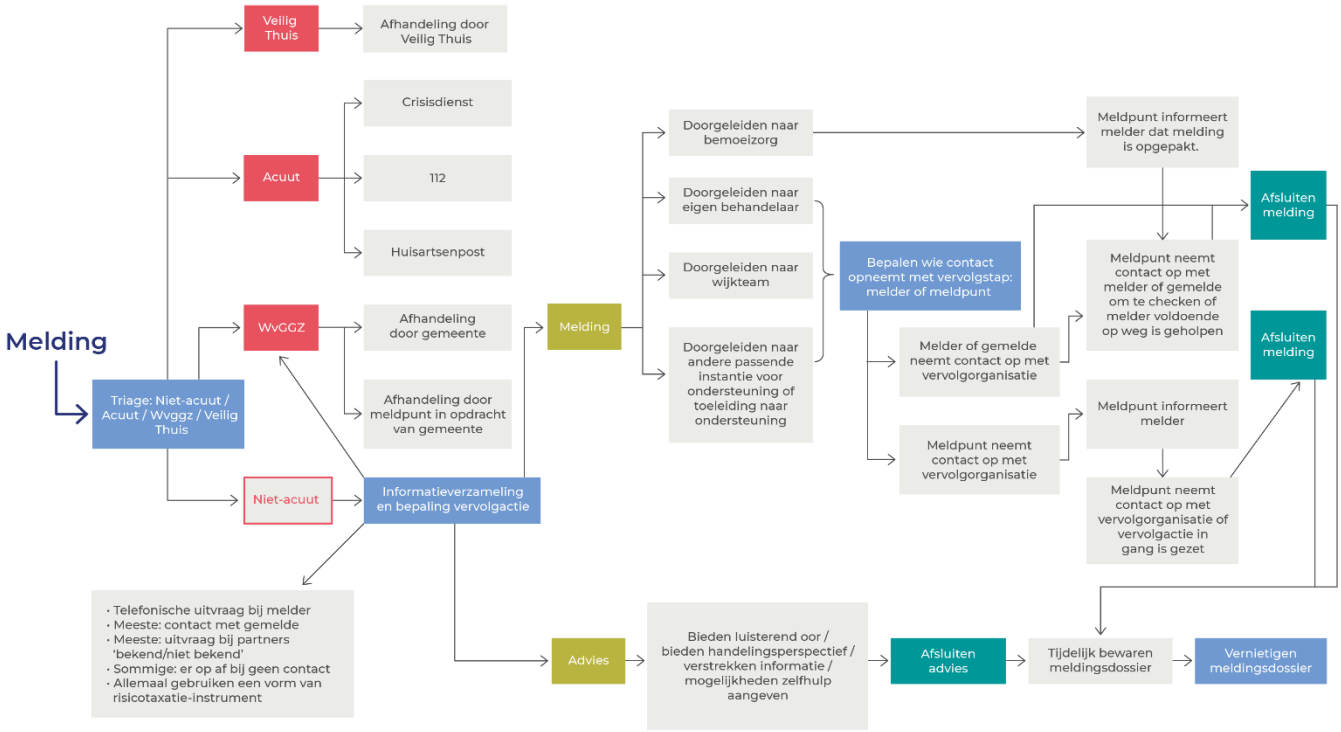
Voor welke burgers is een meld- en adviespunt voor niet-acute hulpbehoefte?
Het gaat om een groep kwetsbare mensen zowel in het sociale domein als in de domeinen zorg en veiligheid. Denk aan dak- en thuislozen, woningvervuilers, multiprobleemgezinnen, chronisch verslaafden, straatprostituees, veelvuldige delict-plegers, mensen met ernstige psychische aandoeningen of verstandelijke beperkingen, vereenzaamde ouderen, mensen die dreigen een gevaar voor zichzelf of voor anderen te vormen en chronisch zieken. Soms veroorzaken zij ook overlast in hun omgeving. Het gaat niet alleen om GGZ-problematiek. Vaak gaat het om mensen die verward raken doordat zij dementeren, een licht verstandelijke beperking hebben, verslaafd zijn of niet goed voor zichzelf kunnen zorgen, waardoor ze hun ziekte (bijvoorbeeld diabetes) verwaarlozen. Een deel van de kwetsbare burgers op wie de meldpunten zich richten, hebben geen duidelijke zorgvraag. Ze hebben te maken met een opeenstapeling van problemen en zijn niet in staat om dit proces te doorbreken.
De term: meldpunt voor personen met verward gedrag dekt dus eigenlijk niet goed de lading. Beter is het om te spreken over meld- en adviespunten niet-acute zorg.

Bron: Handreiking meldpunten niet-acuut

2.2 Generiek werkproces van de meldpunten niet-acuut

In onderstaande paragraaf is een generiek werkproces weer gegeven voor de meldpunten niet-acuut. Dit werkproces wordt daarna nader toegelicht.

Stroomschema meldpunt niet-accuut



Toelichting op het stroomschema

Melding

Het proces start met een melding door iemand die vermoedt dat iemand in zijn omgeving zorg nodig heeft. Bijvoorbeeld een familielid, een buurvrouw of een huurder. Het kan ook een zorgmelding van de politie betreffen, een professional of een persoon die zelf contact opneemt.

Triage niet-acuut/acuut/Wvggz/Veilig Thuis

De eerste stap in het proces is bepalen langs welke route de melding wordt opgepakt. Op basis van informatie van de melder bepaalt de medewerker van het meldpunt of er acuut hulp ingezet moet worden. In dat geval wordt de melding doorgezet naar de crisisdienst, 112 of de huisartsenpost. Bij een crisisdienst kan het bijvoorbeeld gaan om een crisisdienst GGZ, een crisisdienst jeugd of optreden door de Raad voor de Kinderbescherming.

Als uit de informatie blijkt dat het een melding betreft die betrekking heeft op huiselijk geweld of kindermishandeling, wordt de melding door gezet naar Veilig Thuis.

Ook kan het zijn dat de medewerker van het meldpunt tot de conclusie komt dat het eigenlijk gaat om een melding in het kader van de Wvggz. In dat geval wordt de melding doorgezet naar het meldpunt Wvggz. Als het meldpunt niet-acuut en het meldpunt Wvggz in eenzelfde organisatie zijn ondergebracht, dan wordt de melding vanaf dat moment behandeld volgens de juridische kaders van de Wvggz.

In alle andere gevallen wordt de melding behandeld als een melding niet-acuut.

In paragraaf 2.3 wordt nader ingegaan op de samenloop van meldpunten niet-acuut en Wvggz
Niet-acuut: Informatieverzameling en bepaling vervolgactie
Als de melding wordt behandeld als 'melding niet-acuut' gaat deze de volgende stap van het meldproces niet-acuut in: 'Informatieverzameling en bepaling vervolgactie'. In deze processtap gaat een medewerker aan de slag om beter zicht te krijgen op de situatie: Wat is er aan de hand? Zijn er al professionals of instanties betrokken en zo ja welke? Welke is de meest aangewezen professional of instantie die ingeschakeld kan worden om de gemelde of melder verder te helpen door hulp of ondersteuning of door toeleiding naar zorg?

Activiteiten die bij deze fase horen zijn o.a. nadere uitvraag bij de melder, contact opnemen met en informatie vergaren van gemelde, eventueel contact opnemen met reeds betrokken instanties of uitvraag doen bij instanties of zij bekend zijn met gemelde en een rol zien voor zichzelf in het oppakken van de melding. De meeste meldpunten hanteren ook een instrument voor risico-taxatie bij het beoordelen van de situatie en noodzakelijke vervolgroute.

De uitkomst van deze processtap is dat duidelijk wordt wat de beste vervolgroute is. Dat kan zijn dat de melder of gemelde voldoende geholpen is met een advies in de vorm van een luisterend oor, informatie of doorverwijzing waar hij zelf gevolg aan kan geven. Een andere mogelijkheid is dat een andere organisatie wordt ingeschakeld om een vervolgactie in gang te zetten. Dat kan bijvoorbeeld het bemoeizorgteam zijn, het wijkteam van de gemeente, een behandelaar of een andere passende instantie.
Een andere mogelijkheid zou kunnen zijn dat het meldpunt gaandeweg het proces alsnog tot de conclusie komt dat de melding toch moet worden opgepakt in het kader van de Wvggz. In dat geval wordt de melding als het ware overgeheveld en verder behandeld als Wvggz-melding. Op de juridische kant van deze overdracht wordt kort ingegaan in hoofdstuk 3.

Bepalen wie contact opneemt met de vervolgorganisatie
Als duidelijk is welke instantie de vervolgactie gaat ondernemen, kan het meldpunt nog afspreken wie formeel contact opneemt met de vervolgorganisatie: het meldpunt, de gemelde of de melder.

Afsluiten advies of melding, tijdelijk bewaren en vernietigen dossier
De melding wordt afgesloten als betrokkene is geholpen met een advies of als er een organisatie invulling geeft aan een vervolgactie. De meeste meldpunten nemen na een bepaalde periode contact op met de vervolgorganisatie om te checken of de vervolgactie ook is opgepakt. Ze sluiten dan pas af als duidelijk is dat dit is gebeurd. Sommige meldpunten monitoren een melding gedurende een beperkte periode en sluiten de melding pas af als duidelijk is dat de betrokkene - melder of gemelde - is geholpen.

In beide gevallen zal het dossier daarna nog enige tijd worden bewaard voor het geval eenzelfde persoon binnen korte tijd weer meldt of gemeld wordt. Als de vooraf bepaalde bewaartermijn is verstreken en er geen aanleiding is geweest het dossier opnieuw te openen, wordt het dossier vernietigd. In hoofdstuk 4 wordt nader ingegaan op deze bewaartermijnen vanuit het perspectief van zorgvuldige gegevensverwerking en privacy.

Relatie tot lokale overlegtafels en zorg- en veiligheidshuizen
Veel gemeenten kennen overlegtafels voor specifieke doelgroepen of complexe casuïstiek, zoals een jeugdbeschermingstafel en de zorg- en veiligheidshuizen. De aanmelding bij dergelijke tafels is dan geregeld in lokale afspraken. In dit schema wordt ervan uitgegaan dat aanmelding bij dergelijke tafels niet rechtsreeks plaats vindt vanuit het meldpunt, maar dat indien nodig wordt doorgeleid naar een instantie die op basis van de lokale afspraken naar een dergelijke tafel kan doorgeleiden.

2.3 Meldpunten niet-acuut in relatie tot meldpunten Wvggz

Per 1 januari 2020 is de Wet verplichte GGZ in werking getreden. Gemeenten zijn verplicht een meldpunt in te richten waar 'eenieder' een melding kan doen als hij denkt dat iemand geestelijke gezondheidszorg nodig heeft, die mogelijk met verplichte zorg zou moeten verleend. Als zo'n melding wordt gedaan, moet het college van B&W een verkennend onderzoek doen. Indien het college tot de conclusie komt dat het waarschijnlijk nodig is om te komen tot verplichte geestelijke gezondheidszorg, meldt het college de gemelde aan bij de Officier van Justitie voor toeleiding naar de verplichte GGZ. De conclusie kan ook zijn dat er geen reden, of niet voldoende reden is om iemand toe te leiden naar de verplichte GGZ, bijvoorbeeld omdat er nog niet voldoende is geprobeerd om de gemelde te helpen in het kader van vrijwillige zorg, de gemelde inmiddels vrijwillige zorg heeft geaccepteerd, of omdat er andere zorg en ondersteuning nodig is dan GGZ. In dat geval leidt het college de gemelde door naar de aangewezen instantie. Ook kan het zijn dat het college bemoeizorg in zet, om iemand te overtuigen vrijwillige zorg te accepteren.

In veel gemeenten worden het meldpunt Wvggz met het verkennend onderzoek en het meldpunt niet-acuut in eenzelfde meldpunt ondergebracht. Juridisch gezien zijn dit echter twee verschillende taken. Daarom is het belangrijk om bij de vormgeving van het meldpunt goed uit te werken hoe deze twee zich tot elkaar verhouden. Wanneer wordt een melding behandeld volgens het Wvggz-kader en wanneer volgens het kader van het meldpunt niet-acuut. Ook is het belangrijk dat de informatiehuishouding voor beide typen meldingen gescheiden is.

Bij een gecombineerd meldpunt niet-acuut en Wvggz, kunnen zich de volgende situaties voordoen.

a) Een melding komt binnen en bij de triage is direct duidelijk dat het geen Wvggz-melding betreft. In dat geval volgt de melding een van de overige routes: crisis, Veilig Thuis, of niet-acuut.

b) Een melding komt binnen bij het gecombineerde meldpunt en de medewerker komt bij de triage tot de conclusie dat het gaat om een melding in het kader van de Wvggz. Dan wordt de melding verder behandeld volgens het kader van de Wvggz. Dat betekent dat het meldpunt namens het college van B&W start met het verkennend onderzoek.

c) Het is bij de triage nog niet duidelijk of het gaat om een melding in het kader van de Wvggz. In dat geval is het advies om de melding te behandelen als een melding niet-acuut.

In de praktijk zal het regelmatig voorkomen dat een melding die aanvankelijk in behandeling is genomen als 'melding niet-acuut' gaandeweg toch beschouwd moet worden als een melding in het kader van de Wvggz. De uitkomst van het meldproces niet-acuut is dan in feite dat de vervolgactie moet worden opgepakt in het kader van de Wvggz. Juridisch gezien wordt de melding dan doorgeleid naar het meldpunt Wvggz, dat dan alsnog een verkennend onderzoek start. Het meldpunt niet-acuut kan dan de noodzakelijke informatie verstrekken aan het meldpunt Wvggz.[3]

[3] Er verschijnt binnenkort een aparte factsheet over de samenloop meldpunt niet-acuut – meldpunt Wvggz. Over de gegevensverwerking in de meldpunten Wvggz verschijnt ook binnenkort een 'veel gestelde vragen' bij de VNG.

2.4 Meldpunt niet-acuut in relatie tot bemoeizorg

In deze handreiking is er, in overleg met de praktijk, voor gekozen om bemoeizorg en de werkzaamheden van een bemoeizorgteam, niet als onderdeel van het meldproces te beschouwen. Het inzetten van bemoeizorg wordt gezien als een van de mogelijke uitkomsten van het meldproces. Als bemoeizorg moet worden ingezet, kan het meldpunt aan het bemoeizorgteam de informatie overdragen die zij nodig hebben om de bemoeizorg in gang te zetten.

Zie voor bemoeizorg de binnenkort te verschijnen nieuwe handreiking *Gegevensverwerking en bemoeizorg (de bestaande handreiking uit 2014 wordt herzien)*.

3 Juridische aspecten bij het inrichten van een meldpunt niet-acute zorg

3.1 Inleiding

Dit deel van de handreiking gaat in op de juridische aspecten ten aanzien van de gegevensverwerking door het meldpunt niet-acuut en de partijen die informatie verstrekken aan het meldpunt. Dit deel richt zich met name op *projectleiders, juristen, privacy-officers en Functionarissen Gegevensbescherming van bij het meldpunt betrokken partijen.*

De inhoud van dit deel is gebaseerd op de conclusies van een uitgebreide juridische analyse. Het is belangrijk om bij de inrichting van het meldpunt dan ook nauw samen te werken met de juridische afdeling van de gemeente. Als het meldpunt ondergebracht wordt bij een andere organisatie, bijvoorbeeld een GGD, dan is het verstandig om ook een jurist van de GGD hierbij te betrekken, zodat er geen misverstanden ontstaan. De uitgebreide juridische analyse is te vinden op GGD GHOR Kennisnet en staat hier.

Er komen vijf juridische aspecten aan de orde:

1. De juridische basis om meldpunten niet-acuut op te richten voor zover deze basis nodig is om persoonsgegevens te kunnen verwerken;
2. De juridische aspecten bij gegevensverwerking door meldpunten niet-acuut;
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 Algemene verordening gegevensbescherming (AVG).

3.2 De juridische basis om meldpunten niet-acuut op te richten voor zover deze basis nodig is om persoonsgegevens te kunnen verwerken

Er is op dit moment geen specifieke wettelijke regeling voor het oprichten van meldpunten. De meldpunten OGGZ vonden hun basis in het betreffende prestatieveld van de Wmo. Echter met de Wmo 2015, is de meldpunttaak niet meer expliciet belegd.4 Daarmee is er ook geen expliciete juridische basis voor de gegevensverwerking door de meldpunten niet-acuut.
Dit betekent niet dat er geen gegevensverwerking mogelijk is ten behoeve van de meldpunten niet-acuut. Maar het heeft wel meer voeten in de aarde om een goede juridische basis te creëren voor de gegevensverwerking die nodig is. Daarom is het belangrijk om bij de oprichting goed voor ogen te houden welke gegevensverwerkingen mogelijk moeten zijn om het meldpunt goed te laten functioneren.

[4] Op dit moment is wetgeving in voorbereiding om een expliciete juridische basis te creëren voor de noodzakelijke gegevensverwerking ten behoeve van de meldpunten niet-acuut. De inwerkingtreding daarvan wordt op z'n vroegst voorzien 1 januari 2022.

Ontwerpcriteria die vanuit gegevensverwerkingsperspectief aan het meldpunt gesteld kunnen worden zijn:

- Er moet een grondslag zijn conform de AVG artikel 6 lid 1 om gegevens te kunnen verwerken door het meldpunt. Anders is de verwerking van persoonsgegevens niet toegestaan. Daarvoor is het nodig dat in verband met art. 6, lid 3, AVG duidelijk is op basis van welke taak of taken van de betrokken partijen het meldpunt wordt opgericht.
- Het meldpunt moet bijzondere persoonsgegevens waaronder gegevens betreffende de gezondheid en strafrechtelijke gegevens afkomstig van de politie kunnen verwerken. Anders is het niet mogelijk voor het meldpunt om te triageren en door te kunnen geleiden naar de aangewezen instantie. Het meldpunt is immers met name bedoeld voor mensen die zorg of ondersteuning nodig hebben. Het kan daarbij voorkomen dat iemand gemeld wordt door de politie naar aanleiding van een overtreding of verstoring van de openbare orde. Ook moet het mogelijk zijn door te geleiden naar hulp- en zorgverleners.
- Het moet mogelijk zijn om deze gegevens te verwerken en uit te wisselen zonder toestemming van betrokkene. De aard van het meldpunt is immers dat mensen gemeld worden en dus niet altijd vooraf toestemming zullen geven. Ook is het leggen van contact niet altijd mogelijk, terwijl het wel noodzakelijk is om zo snel mogelijk te zorgen dat de meest aangewezen partij aan het werk wordt gezet.
- Dit moet ook mogelijk zijn indien de professional die de meldpunttaken uitvoert, behoort tot een beroepsgroep met een beroepsgeheim zoals geregeld in de wet BIG, de Wgbo, of de jeugdwet. Het meldpunt voert echter geen behandeltaken uit op grond van een medische behandelovereenkomst en verleent geen jeugdhulp.
- In alle gevallen blijft gelden dat de verwerking van persoonsgegevens moet voldoen aan de criteria van noodzaak, subsidiariteit en proportionaliteit van de AVG.

Op basis van bovenstaande ontwerpcriteria vanuit gegevensverwerkingsperspectief komen de volgende modellen voor de oprichting van een meldpunt niet acute zorg in aanmerking:

- Meldpunten met een taak van algemeen belang, formeel ingesteld bij gezamenlijk besluit van het college van B&W en de burgemeester (van één of meerdere gemeenten), uitgevoerd door de gemeente zelf.
- Meldpunten met een taak van algemeen belang, formeel ingesteld bij gezamenlijk besluit van het college van B&W en de burgemeester (van één of meerdere gemeenten) en ondergebracht bij een bij het instellingsbesluit aangewezen partij anders dan gemeente, bijvoorbeeld een GGD. Deze andere partij treedt dan op als uitvoerder namens het college van B&W en de burgemeester.
- Meldpunten met een gecombineerde taak van algemeen belang en (medische) zorgverlening, gezamenlijk opgericht door het college van B&W (van één of meerdere gemeenten) en een GGZ-instelling waar het meldpunt is ondergebracht.

NB. Bij elk van deze modellen blijft het mogelijk dat, naast het besluit tot instelling van het meldpunt, meerdere partijen afspraken maken over bijvoorbeeld de bemensing of de werklocatie van het meldpunt.

3.2.1 Ratio achter deze modellen

Gezien de aard van de werkzaamheden van het meldpunt, de noodzaak om zonder toestemming te kunnen werken, en de sturende rol van de overheid hierin, is de meest aangewezen grondslag voor gegevensverwerking artikel 6, lid 1, sub e, van de AVG: de gegevensverwerking is noodzakelijk voor de uitvoering van een taak van algemeen belang. Om gebruik te kunnen maken van deze grondslag is het noodzakelijk dat het meldpunt wordt opgericht in het kader van taken die wettelijk geregeld zijn.

Meldpunt ingesteld bij besluit van college van B&W en burgemeester

Een besluit tot instellen van een meldpunt kan ten behoeve van deze gecombineerde taken genomen worden door het college van B&W en de burgemeester 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 van B&W betreft het hier de taken uit de materiewetten voor het sociaal domein, te weten de Wmo, Jeugdwet, Participatiewet en Wet gemeentelijke schuldhulpverlening. Voor de burgemeester spelen hierbij diens bevoegdheden ten aanzien van de openbare orde.

Door het besluit tot instelling van een meldpunt voor deze gecombineerde wettelijke taken ontstaat er een juridische basis voor de verwerking van persoonsgegevens op grond van het eerdergenoemde artikel 6 lid 1 sub e van de AVG. Dit betekent tevens dat er geen toestemming nodig is ingevolge de AVG om deze persoonsgegevens te verwerken.

Door de combinatie van taken kan het meldpunt zowel zorgmeldingen, als meldingen vanuit het openbare orde domein waar een zorg- of sociaaldomeinaspect aan zit, verwerken. Ook kan het meldpunt in voorkomende gevallen gezondheidsgegevens dan wel strafrechtelijke gegevens verwerken. Voor de verwerking van gezondheidsgegevens is daarbij de uitzondering op het verbod om deze te verwerken van artikel 30, lid 3, onder a, van de Uitvoeringswet AVG (UAVG) voor maatschappelijke dienstverlening van toepassing. Strafrechtelijke gegevens kunnen dan verwerkt worden omdat dit noodzakelijk is in aanvulling op de verwerking van gezondheidsgegevens conform artikel 33, lid 1, c, van de UAVG. Omgekeerd zullen gezondheidsgegevens bij meldingen door de politie verwerkt kunnen worden omdat dit noodzakelijk is in aanvulling op de verwerking van gegevens van strafrechtelijke aard conform artikel 23, onder c, van de UAVG.

Meldpunt opgericht door het college van B&W en een GGZ-instelling

Voor het college van B&W betreft het hier de taken uit de materiewetten voor het sociaal domein, te weten de Wmo, Jeugdwet, Participatiewet en Wet gemeentelijke schuldhulpverlening. Voor de GGZ-instelling speelt dat het om een instelling voor gezondheidszorg gaat. Het gaat bij meldpunten niet om een behandelovereenkomst zoals bedoeld in de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO). Het kan in bepaalde gevallen wel gaan om medische handelingen zoals bedoeld in de wet BIG. Dit hangt af van de melding en of er bij de gemelde sprake is van bijvoorbeeld een psychische aandoening. Er kan sprake zijn van een medische handeling als de medewerker van het meldpunt diagnose-achtige werkzaamheden verricht of bij een specifiek medisch advies aan de gemelde om bijvoorbeeld contact met een GGZ-behandelaar te zoeken om te bekijken of een GGZ-behandeling nodig of mogelijk is.

Meldpunt ingesteld door colleges van B&W en burgemeesters van meerdere gemeenten

Bij meerdere gemeenten kan een meldpunt, net zoals een GGD, ingesteld worden op basis van de Wet gemeenschappelijke regelingen. Een besluit van de gezamenlijke burgemeesters en colleges is ook mogelijk.

3.2.2 Positie van medewerkers met een BIG-registratie bij de voorgestelde modellen

Voor de professional die BIG geregistreerd is, geldt bij werkzaamheden die in het meldpunt uitgevoerd worden dat er geen sprake is van een medische behandelovereenkomst, maar dat bij medisch

handelen zoals een diagnose of een specifiek medisch advies wel rekening gehouden moet worden met het medisch beroepsgeheim voor zover dat geldt buiten de behandelovereenkomst.

Dat betekent dat zij gegevens uit het meldpuntdossier mogen verstrekken aan anderen, voor zover noodzakelijk is voor de goede uitvoering van de meldpunttaken, bijvoorbeeld om die andere instantie in staat te stellen zorg te gaan verlenen, of toeleiding naar hulp op te starten. Zij hebben daarvoor geen toestemming nodig van de betrokkene. Zij blijven echter gebonden aan de ethische codes van hun beroepsgroep. Dat betekent bijvoorbeeld dat zij de beginselen van goed hulpverlenerschap hanteren: de gemelde zoveel mogelijk betrekken bij het meldproces; voor zover dat mogelijk is met hem bespreken naar welke instantie het beste kan worden doorgeleid; geen gegevens verstrekken aan een andere partij als dat het belang van de gemelde schaadt. Ten aanzien van het verstrekken van inhoudelijk medische gegevens geldt dat hierbij zo veel mogelijk terughoudendheid moet worden betracht.

3.2.3 De verantwoordelijke voor de gegevensverwerking

In juridische zin zijn de meldpunten volgens de hier boven genoemde modellen samenwerkingsverbanden van het college van B&W en de burgemeester en soms van de colleges en burgemeesters van meerdere gemeenten. In de praktijk wordt het meldpunt in uitvoerende zin veelal belegd bij een andere partij. Dit betekent dat er helderheid geschapen moet worden over de verantwoordelijkheid voor de gegevensverwerking.

De AVG biedt daarvoor verschillende mogelijkheden:

- Bij een meldpunt voor een gemeente:
  - Het college van B&W en de burgemeester van een gemeente zijn gezamenlijk verantwoordelijk;
  - Het college van B&W wordt aangewezen als verantwoordelijke;
- In geval van een meldpunt van meerdere gemeenten:
  - De colleges van B&W en de burgemeesters zijn gezamenlijk verantwoordelijk;
  - De colleges van B&W zijn gezamenlijk verantwoordelijk;
  - Het college van B&W en de centrumgemeente zijn gezamenlijk verantwoordelijk;
  - Het college van de centrumgemeente is verantwoordelijk;
- De uitvoerende organisatie (lees een GGD, GGZ-instelling, of andere organisatie dan de gemeente die het meldpunt uitvoert) wordt aangewezen als de verwerkingsverantwoordelijke.

Als algemeen uitgangspunt wordt geadviseerd om één partij aan te wijzen als verwerkingsverantwoordelijke en niet meerdere partijen. Gezamenlijke verwerkingsverantwoordelijkheid, brengt bij de meldpunten waar we het hier over hebben extra en onnodige complexiteit met zich mee bijvoorbeeld als een burger zijn rechten wil uitoefenen of extra afstemming tussen verschillende Functionarissen Gegevensbescherming.

3.3 De juridische aspecten bij het verstrekken van persoonsgegevens door meldpunten niet-acuut

3.3.1 Mogelijkheden om te verstrekken

In het vorige hoofdstuk is de juridische basis voor de gegevensverwerking door het meldpunt geschetst. Een specifieke vorm van het verwerken van persoonsgegevens is het verstrekken van persoonsgegevens door een meldpunt aan derden. Hierbij moet op grond van de AVG met een aantal aspecten rekening gehouden worden:

- Het principe van doelbinding op grond van de AVG van art. 5, lid 1, onder b, en art. 6, lid 4. Artikel 5 lid 1 sub b, bepaalt dat gegevens uitsluitend verwerkt mogen worden voor de doelen waarvoor deze zijn verzameld. Artikel 6 lid 4 bepaalt dat dit ook is toegestaan als de doelen van verdere verwerking verenigbaar zijn met de oorspronkelijke doelen van verzameling, of als deze verdere verwerking bij wet is toegestaan.
- Een geheimhoudingsverplichting of eventuele strikte doelbinding die erop neerkomt dat gegevens enkel verder gebruikt mogen worden voor dezelfde doelen als waarvoor deze eerder verzameld zijn.

Ten behoeve van de taken van het meldpunt komen drie doelen van verstrekken voor:

1. Het verstrekken van gegevens over een gemelde aan derden, om te checken of deze partij reeds betrokken is bij gemelde en of een rol kan spelen bij het verder oppakken van de melding op basis van de eigen taken;
2. Het verstrekken van persoonsgegevens over een gemelde aan derden om deze in staat te stellen de melding verder op te pakken op basis van zijn eigen taken;
3. Verstrekken van gegevens aan de melder in het kader van terugmelding.

<u>Verstrekken voor doelen 1 en 2</u>

In de praktijk zullen meldpunten vooral gegevens verstrekken voor de eerste twee doelen. Waarbij uiteraard de noodzakelijkheidsafweging in acht genomen moet worden. Hierbij speelt het volgende:

- In beide gevallen is de verstrekking van de gegevens noodzakelijk voor de uitvoering van de taken van het meldpunt. Het meldpunt heeft deze gegevens ook in dat kader verzameld. De doelen stemmen dus overeen. Het doelbindingprincipe staat niet in de weg.
- Het meldpunt verstrekt uitsluitend gegevens aan partijen die gezien hun taak ook mogelijkerwijs een taak hebben ten aanzien van de gemelde, of moeten beoordelen of zij wellicht een taak zouden moeten krijgen. Zij mogen deze gegevens verwerken voor hun eigen taak.
- Voor zover het noodzakelijk is daarbij gezondheids- of strafrechtelijke gegevens te verstrekken, zal dit in de regel slechts aan de orde zijn bij partijen die deze gegevens ook nodig hebben en mogen verwerken voor de eigen taken. Denk daarbij aan een instelling voor gezondheidszorg, jeugdhulp of jeugdbescherming, de gemeente of wijkteam in het kader van de wettelijke taken van het college in het sociaal domein, een instelling voor beschermd wonen, Veilig Thuis of de politie. Gezondheidsgegevens mogen aan deze partijen worden verstrekt, maar uitsluitend voor zover dat noodzakelijk is. Vaak zal het meldpunt gegevens van de politie krijgen, met als doel hulp in gang te zetten. Ook deze gegevens mag het meldpunt aan partijen verstrekken, als dit noodzakelijk is voor de taak van het meldpunt, of de andere partij in staat te stellen de melding op te pakken. Er moet wel altijd terughoudendheid betracht worden bij het verstrekken van deze gegevens over gezondheid en gegevens die te maken hebben met strafbare feiten, veroordelingen of veiligheidsmaatregelen.
- Er zijn ook partijen aan wie in de regel geen gezondheidsgegevens en of strafrechtelijke gegevens mogen worden verstrekt. Woningcorporaties mogen bijvoorbeeld slechts gezondheidsgegevens verwerken als dat noodzakelijk is voor aangepaste voorzieningen in een woning. Aanbieders van

algemene voorzieningen in het kader van de Wmo mogen slechts gegevens verwerken die ze van de betrokkene zelf hebben verkregen. Vaak zal verstrekking van gezondheidsgegevens of strafrechtelijke gegevens aan dergelijke partijen ook niet noodzakelijk zijn. Mocht dit noodzakelijk lijken dan is het verstandig te checken of dit kan, of om toestemming te vragen aan betrokkene.
- Uiteraard zal er bij de verstrekking van gegevens altijd rekening moeten worden gehouden met de criteria van noodzaak, subsidiariteit en proportionaliteit van de AVG.

Voor professionals is het moeilijk om te overzien welke partijen wel en welke geen gezondheids- en of strafrechtelijke gegevens mogen verwerken. Daarom is het belangrijk dat de organisaties voor goede werkinstructies zorgen. Bijvoorbeeld door bij de meest voorkomende partijen aan te geven wat daarin wel en niet is toegestaan.

Verstrekken van gegevens aan de melder in het kader van terugmelding
Een derde doel voor het verstrekken van persoonsgegevens door het meldpunt is het informeren van de melder over de afhandeling van de melding.
Het terugmelden aan de melder past bij de goede taakuitoefening van het meldpunt. Echter de melder heeft zelf meestal geen taak meer ten aanzien van gemelde die verband houdt met de melding. Het doel van de verstrekking van gegevens over gemelde is hierdoor in de meeste gevallen niet duidelijk en zal beperkt moeten blijven tot de mededeling 'dat de melding is opgepakt'.

3.3.2 De positie van medewerkers van het meldpunt die vallen onder het beroepsgeheim van de wet BIG, WGBO bij het verstrekken door het meldpunt

In paragraaf 3.2.2 is uitgelegd dat het beroepsgeheim van de wet BIG en de WGBO verstrekking van gegevens niet in de weg staat, als de verstrekking noodzakelijk is voor de goede uitvoering van de werkzaamheden van het meldpunt en het handelen door het meldpunt en de daarbij behorende gegevensverstrekking niet in strijd is met de beginselen van goed hulpverlenerschap.

3.4 De juridische aspecten bij het verstrekken van persoonsgegevens aan meldpunten bij een melding en als antwoord op een informatievraag van het meldpunt

3.4.1 Het melden bij een meldpunt

De meldpunten niet-acuut hebben als uitgangspunt dat eenieder kan melden die zich zorgen maakt over een persoon. Dit kunnen natuurlijke personen of organisaties, bijvoorbeeld de politie of een woningcorporatie, zijn. Er is geen *specifieke* wettelijke regeling voor het verstrekken van persoonsgegevens *aan* meldpunten door partijen.

Burgers kunnen 'als burger' persoonsgegevens verstrekken aan meldpunten. Deze gegevensverstrekkingen vallen niet onder de AVG.

Organisaties zullen zelf moeten beoordelen in welke situaties zij een melding willen doen bij het meldpunt en wat de juridische basis is voor deze melding. Eventueel kunnen op bestuurlijk niveau afspraken gemaakt worden met belangrijke partners, zoals politie, zorgpartijen, of woningcorporaties.

Op hoofdlijnen geldt het volgende:
Als het melden bij het meldpunt past bij de (wettelijke) taken van de organisatie in relatie tot de gemelde, dan kunnen op grond van de AVG artikel 6 lid 4 in principe gegevens verstrekt worden aan

het meldpunt. Bijvoorbeeld een woningcorporatie die bij een huurder signaleert dat er wellicht zorgproblematiek speelt, zou dit kunnen melden op grond van haar zorgplicht artikel 18a lid 1, Woningwet.

Zorgmeldingen van de politie kunnen gemeld worden op grond van bijzondere omstandigheden zoals bedoeld in art. 7, lid 1, of artikel 19 sub c, van de Wet Politiegegevens.

Als een organisatie wil melden, maar de melding niets met de eigen taak te maken heeft, dan zal de organisatie gegevens verstrekken (uitsluitend) voor de taak van het meldpunt en kunnen gegevens verstrekt worden, mits er geen strikte doelbinding rust op de gegevens en er geen wettelijke geheimhoudingsplichten bestaan. Een strikte doelbinding of geheimhoudingsverplichting geldt in de praktijk met name als het gaat om het verstrekken van gegevens over de gezondheid, strafrechtelijke - of politiegegevens.

3.4.2 Het melden bij een meldpunt door professionals met een beroepsgeheim op grond van de wet BIG, WGBO of Jeugdwet

Indien de melder gebonden is aan een beroepsgeheim op grond van de wet BIG, WGBO of Jeugdwet en de melding vloeit voort uit een behandelrelatie met betrokkene dan zal in principe in het kader van die behandeling of de uitvoering van jeugdhulp toestemming gevraagd moeten worden, tenzij er sprake is van een van de in die wetten benoemde uitzonderingsgronden, i.c. vitaal belang, conflict van plichten, respectievelijk 'het goed hulpverlenerschap van de jeugdhulpwerker'.

Dit geldt ook voor BIG-geregistreerd ambulancepersoneel dat bij de hulpverlening signaleert dat er waarschijnlijk ook andere hulp nodig is en dit wil melden bij een meldpunt. Zij zullen dit dan moeten bespreken met de persoon die ze willen melden en toestemming vragen, tenzij er sprake is van een conflict van plichten.

3.5 Het vereiste dat enkel noodzakelijke gegevens verwerkt mogen worden

Uitgangspunt van alle regelgeving over het verwerken van persoonsgegevens is dat deze uitsluitend verwerkt worden voor zover noodzakelijk voor de taak en het doel van de activiteit. In dat verband hanteert de AVG de begrippen *noodzaak*, *proportionaliteit en subsidiariteit*, waarbij proportionaliteit en subsidiariteit onderdeel zijn van de noodzakelijkheidsafweging.

Noodzakelijk betekent dat je niet meer gegevens verwerkt of verstrekt dan noodzakelijk is voor het doel. Er moet dus steeds en op meerdere plekken in het werkproces beoordeeld worden wel gegevens noodzakelijk zijn, gegeven de situatie en te ondernemen vervolgstappen.

Proportioneel betekent dat het middel in verhouding moet staan tot het doel. Hierbij kun je bijvoorbeeld denken aan bewaartermijnen. Is het proportioneel om persoonsgegevens van alle meldingen gedurende lange tijd te bewaren, terwijl voor het overgrote deel van de meldingen een veel kortere periode relevant is. Het lang bewaren staat dan voor de meeste meldingen niet in verhouding tot de aard van de melding en de inbreuk op de privacy. Het is dan beter een kortere bewaartermijn te hanteren en proberen criteria op te stellen voor de uitzonderingen.

Subsidiair betekent dat je eerst beoordeelt of er minder ingrijpende manieren zijn om het doel te bereiken. Bijvoorbeeld: als het ook kan met uitwendige en niet inhoudelijke gegevensgegevens, dan

moet je dat doen. Het gebruik van bijvoorbeeld medisch inhoudelijke persoonsgegevens is dan immers niet noodzakelijk.

De criteria *noodzaak, proportionaliteit en subsidiariteit* zijn open normen. Voor een deel kunnen daarin beleidsmatig keuzes gemaakt worden. Maar veel komt neer op de professionaliteit van de medewerkers.
In de praktijk worden veel verschillende redenen aangevoerd om de noodzakelijkheid van het verwerken en verstrekken van persoonsgegevens te rechtvaardigen. Deze zijn niet allemaal even valide. In onderstaande tabel hebben we er een aantal bij wijze van voorbeeld op een rij gezet.

Noodzakelijkheidsargumenten	
Valide	**Niet valide**
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).	Je weet maar nooit of we de gegevens op een later tijdstip nodig hebben.
Zonder de gegevens kunnen de werkzaamheden of interventie(s) niet uitgevoerd worden (denk aan personalia of (formele) voorwaarden).	Het is handig om te hebben. De gegevens vergemakkelijken de werkzaamheden of interventie.
Zonder de gegevens loopt het fout (denk aan veiligheid en bescherming).	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 zijn nodig om de werkzaamheden op inhoudelijk goede en verantwoorde 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. Bij een meldpunt gaat het er dan om dat de gegevens noodzakelijk zijn om tot een goede beoordeling van de melding te komen en te kunnen bepalen naar welke instantie deze moet worden doorgeleid.	

Bij de valide argumenten kan de vraag ‘is het noodzakelijk’ bij een meldpunt niet-acuut volmondig met ‘ja’ beantwoord worden voor het specifieke doel. Bij de niet valide argumenten ligt dat anders. Bewaren ‘want je weet maar nooit’ kan geen voldoende reden zijn voor een meldpunt om gegevens langdurig te bewaren. Het bewaren van een melddossier zal altijd een specifiek doel moeten dienen. In paragraaf 4.3.3 wordt hier nader op ingegaan. Voor ‘handig om te hebben’ geldt ook dat dit geen voldoende reden kan zijn om gegevens te verzamelen of langdurig te bewaren. Bij het efficiencyargument kan nog sprake zijn van een proportionaliteitsafweging. Als het niet-verstrekken leidt tot onevenredig hoge extra kosten, kan het verwerken van bepaalde gegevens te verantwoorden zijn. Dit zal echter bij een meldpunt niet aan de orde zijn.

3.6 De informatieplicht van de AVG

Op grond van de AVG is het meldpunt verplicht om betrokkene te informeren over de gegevensverwerking. De AVG kent specifieke bepalingen ten aanzien van de informatieplicht voor de situatie waarin de gegevens van een ander dan de betrokkene zelf zijn gekregen. Dit zal bij de meldpunten in eerste instantie het geval zijn. Deze bepalingen staan in artikel 14 van de AVG.
Kort gezegd komt dit op het volgende neer:
De betrokkene wordt tenminste binnen een maand na de melding geïnformeerd over de gegevensverwerking of zodra het meldpunt zelf contact opneemt met betrokkene.

Het informeren kan achterwege of uitgesteld worden als:

- De betrokkene al geïnformeerd is, bijvoorbeeld door de melder, of direct geïnformeerd zal worden door vervolgorganisatie die de melding op pakt;
- Als het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, bijvoorbeeld omdat men geen contact kan krijgen met de gemelde;
- Het informeren ertoe leidt dat de werkzaamheden van het meldpunt onmogelijk worden of ernstig in het gedrang komen. In dat geval moet wel bepaald worden wanneer betrokkene wel geïnformeerd wordt, bijvoorbeeld door de vervolgorganisatie die de melding op pakt;
- Op grond van de UAV artikel 41 lid 1, mag het informeren achterwege blijven als dit nodig is ter bescherming van de betrokkene of van de rechten en vrijheden van anderen. Ook in dit geval moet wel bepaald worden wanneer betrokkene wel geïnformeerd wordt, of dat de vervolgorganisatie dit doet.

Het meldpunt zal in haar beleid inzichtelijk moeten maken in welke situaties ze gebruik maakt van de uitzonderingsgronden, eventueel afspraken moeten maken met vaste partners over wie de gemelde op welke wijze informeert en moeten zorgen voor begrijpelijke informatie voor betrokkenen op de website en eventueel een folder.

4 Privacy Impact Analyse op de werkwijze van meldpunten niet-acuut

4.1 PIA-systematiek

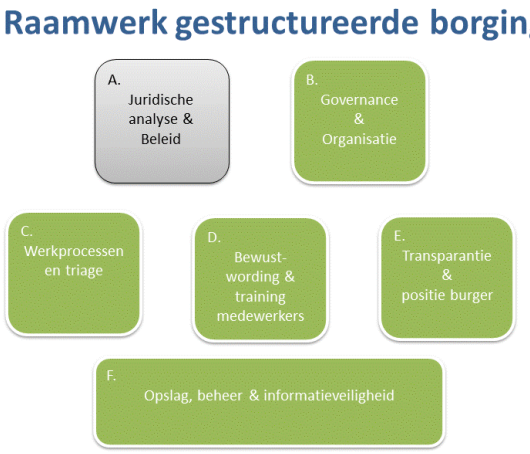
Een zorgvuldige omgang met gegevens van burgers begint bij een goede inrichting van de informatiehuishouding. De manier waarop een meldpunt is georganiseerd, het werkproces dat wordt gevolgd en de wijze waarop gegevens worden geregistreerd, heeft een grote invloed op de risico's die er bestaan voor de privacy van de burger. Ook de manier waarop de interactie met de burger plaats vindt en de manier waarop medewerkers worden geïnstrueerd en getraind, speelt een belangrijke rol.

De PIA-systematiek biedt een manier van kijken waarbij uitgaande van de bestaande organisatie en werkwijze privacy-risico's in kaart worden gebracht en maatregelen worden aangereikt om de kans dat de risico's optreden ook zo klein mogelijk te houden. Voor deze handreiking maken wij gebruik van de opzet van de Privacy Impact Assessment (PIA) voor de gemeentelijke informatiehuishouding voor de decentralisaties sociaal domein, die het kabinet in 2014 liet uitvoeren. Deze neemt niet de gegevensverwerkingen als uitgangspunt, maar de organisatiewijzen. Daarmee biedt die goed zicht op de aspecten waar bij het inrichten van de organisatie rekening kan worden gehouden.

In dit hoofdstuk wordt achtereenvolgens gekeken naar:

- Governance en organisatie
- Werkprocessen en triage
- Bewustwording en training van medewerkers
- Transparantie en de positie van de burger
- Opslag, beheer en informatieveiligheid

Het veld juridische analyse en beleid is reeds behandeld in hoofdstuk 3.



Governance en organisatie: In dit onderdeel van de PIA-analyse wordt gekeken naar de risico's die samenhangen met de wijze waarop het meldpunt is georganiseerd. Daarbij wordt gekeken naar bestuurlijke afspraken en overeenkomsten en hoe het meldpunt is gepositioneerd ten opzichte van andere taken van de organisatie.

Werkprocessen en triage: In dit onderdeel van de PIA-analyse wordt gekeken naar de privacy-risico's die samenhangen met het gekozen werkproces en de wijze waarop in het werkproces afwegingen worden gemaakt ten aanzien van de noodzakelijkheid van de te verwerken gegevens. Er wordt

gekeken naar inhoudelijke routes van een melding en overdrachtsmomenten naar andere organisaties. Voor het werkproces maken we gebruik van het generieke werkproces zoals beschreven in hoofdstuk 2.

Bewustwording en training van medewerkers: In dit onderdeel van de PIA-analyse wordt aandacht besteed aan het belang van training en bewustwording van medewerkers in het meldpunt en partnerorganisaties van het meldpunt.

Transparantie en positie van de burger: In dit onderdeel van de PIA-analyse wordt gekeken naar de privacy-risico's die samenhangen met de wijze waarop de positie van de burger, zowel melder als gemelde, is geborgd in de werkwijze. Het gaat dan om bijvoorbeeld de wijze waarop de burger zijn rechten inzake de AVG kan uitoefenen. Maar ook over de manier waarop de burger geïnformeerd wordt tijdens de behandeling van de melding.

Opslag, beheer en informatieveiligheid: In dit onderdeel van de PIA-analyse besteden we aandacht aan de privacy-risico's die samenhangen met de meer technische en beheers-aspecten van informatievoorziening. Waar worden gegevens opgeslagen? Hoe is de toegang tot gegevens geregeld? Voldoet de informatiebeveiliging?

In de volgende paragrafen gaan we op al deze aspecten verder in.

4.2 Governance en organisatie: privacy-risico's en aanbevelingen

Algemene toelichting
Op het gebied van de organisatie laten de meldpunten verschillende varianten zien. Een aantal aspecten springen eruit vanuit het oogpunt van gegevensverwerking en privacy.

Een eerste aspect dat in beeld komt is de positionering van het meldpunt. De meeste meldpunten zijn ondergebracht bij een organisatie die ook nog andere taken uitvoert. Meestal bij een GGD, soms bij een GGZ-instelling en in een enkel geval bij de gemeente of een andere organisatie. Voor zover bekend zijn er geen situaties waarbij het meldpunt niet-acuut een zelfstandige organisatie is, met uitsluitend de meldpuntfunctie als taak.

Een tweede aspect is de mate van integratie van de meldfunctie niet-acuut met andere meldfuncties, zoals een crisismeldpunt en per 1 januari 2020 de meldfunctie Wvggz.

Een derde aspect is de mate waarin het meldpunt zelf ook andere taken uitvoert dan de meldpuntfunctie zoals beschreven in hoofdstuk 2 of in haar werkwijze 'overige activiteiten' heeft geïntegreerd zoals procesregie of deelname aan een zorgoverleg.

De keuzes die op de bovengenoemde aspecten gemaakt worden, kunnen specifieke privacy-issues met zich meebrengen. In dit hoofdstuk gaan wij nader in op die mogelijke keuzes, de specifieke privacy-risico's en de maatregelen om die risico's te vermijden.

Daarnaast gaan we aan het eind van deze paragraaf in op afspraken tussen organisaties die betrokken zijn bij het meldpunt.

4.2.1 Het meldpunt uitbesteed aan een andere organisatie

In hoofdstuk 3 zijn verschillende modellen gepresenteerd om het meldpunt juridisch te organiseren op een manier dat er voldoende grondslag bestaat om de gegevens te verwerken die noodzakelijk zijn voor de werkzaamheden in het meldpunt niet-acuut. De meeste meldpunten zullen worden uitbesteed aan een andere organisatie, meestal een GGD en soms een GGZ. Dit betekent dat de organisatie die de taken uitvoert dit doet namens het samenwerkingsverband van college van B&W en de burgemeester en niet op eigen titel.

Privacy-risico's

Bij het uitbesteden van de meldpuntfunctie doen zich verschillende risico's voor:

- Onduidelijkheid over wie de verantwoordelijke is voor de gegevensverwerking: het college of de organisatie waar het meldpunt is onder gebracht;
- Onduidelijkheid over wie de taken van de verantwoordelijke voor de gegevensverwerking uitvoert;
- Onduidelijkheid over welk beleid ten aanzien van gegevensverwerking en privacy geldt: dat van de gemeente of dat van de organisatie die het meldpunt uitvoert;
- De bevoegdheidsverlening voor het uitvoeren van de taken van het college is niet goed geregeld.

Aanbevelingen

- De meldpuntfunctie is een specifieke taak die vraagt om een apart beleidsdocument van de gemeente voor de omgang met gegevensverwerking en privacy. Verwijs in de opdrachtverlening voor het meldpunt naar dit beleidsdocument. Maak voor het opstellen eventueel gebruik van deze handreiking.
- Maak in de opdrachtverstrekking afspraken over wie in uitvoerende zin invulling geeft aan de werkzaamheden van de verantwoordelijke voor de gegevensverwerking en maak de wijze waar op dit gebeurt onderdeel van het beleidsdocument. Denk daarbij in ieder geval aan de volgende zaken:
  - Informatieplicht aan de betrokkene(n);
  - De wijze waarop betrokkene(n) hun rechten inzake de AVG kunnen uitoefenen;
  - De procedure rond datalekken;
- Vraag de juristen van de gemeente(n) zorg te dragen voor de juiste bevoegdheidsverleningen.

4.2.2 Het meldpunt als onderdeel van een organisatie die ook andere taken uitvoert

De meeste meldpunten zijn ondergebracht bij een organisatie die ook andere taken uitvoert, zoals hulpverlening, behandeling of bemoeizorg. Het gaat dan om organisaties zoals een GGD of GGZ-instelling, die vanuit hun andere taken beschikken over de kennis en expertise om tot een goede beoordeling van de situatie te komen juist waar het gaat om zorg- en sociale problematiek. Raakvlakken en schijnbare overlap in taken zijn hier het meest ingewikkeld. Bijvoorbeeld tussen de meldpunttaak en bemoeizorg.

Een ander aspect dat hier een rol kan spelen is dat medewerkers soms volledig zijn vrij gesteld voor de meldpunttaak, soms vervullen ze in deeltijd ook andere taken binnen de organisatie.

Privacy-risico's

Bij deze positionering van het meldpunt doen zich een aantal privacy-risico's voor:

- Vermenging van taken en juridische kaders of verwarring daarover waardoor:
  - Het voor de meldpuntmedewerker niet duidelijk is dat er verschillende regels gelden voor de gegevensverwerking bij het uitvoeren van de meldpuntfunctie en die voor andere taken en dat niet duidelijk is aan welke regels hij zich moet houden bij het uitoefenen van de meldpuntfunctie;

- Vermenging van de gegevenshuishoudingen: de gegevenshouding van de meldpuntfunctie is niet goed gescheiden van die voor andere taken, waardoor niet duidelijk waarvoor gegevens wel of niet gebruikt mogen worden en welke regels van toepassing zijn;
- Het voor andere medewerkers in de organisatie niet duidelijk is dat de meldpuntfunctie een andere taak is en dat gegevens die voor die taak verzameld zijn niet zomaar gebruikt mogen worden voor andere taken van de organisatie;
- Het voor partijen die bevraagd worden niet duidelijk is vanuit welke taak ze bevraagd worden en welke regels voor haar van toepassing zijn bij het verstrekken van informatie.

Aanbevelingen

- Zorg voor een goede afbakening van de meldpunttaak ten opzichte van de andere taken in de organisatie, o.a. door:
  - Te beschrijven welke activiteiten en 'producten' wel tot de meldpunttaak behoren en welke niet;
  - Een duidelijke functiescheiding tussen de meldpunttaak en andere taken, zodat medewerkers weten wanneer het kader voor de meldpunttaak geldt en wanneer het kader voor andere taken.
- Stel een beleidsdocument op voor de gegevensverwerking en privacy ten behoeve van de meldpunttaak aan de hand van de thema's in deze handreiking.
- Maak op basis van de afbakening een werkinstructie voor de medewerkers van het meldpunt zodat ze weten welke werkzaamheden onder de meldpunttaak vallen, welke niet, en wat dat betekent voor de gegevensverwerking. Maak daarbij duidelijk dat de meldpunttaak een aparte taak is en dat dit betekent dat zij gegevens waar over de organisatie vanuit andere taken beschikt, niet zomaar mogen gebruiken voor de meldpunttaak. Geef aan welke regels hiervoor gelden, op basis van het juridisch kader in hoofdstuk 3.
- Maak onderdeel daarvan dat voor partijen bij wie informatie wordt opgevraagd altijd duidelijk is in het kader van welke taak dat gebeurt, zodat deze kunnen beoordelen op basis van hun eigen kaders of zij gegevens kunnen verstrekken voor de betreffende taak.
- Zorg dat binnen de organisatie andere medewerkers weten dat de meldpuntfunctie een aparte taak is en dat zij niet zomaar gebruik kunnen maken van gegevens die voor de meldpunttaak zijn verzameld. Indien vanuit de meldpuntfunctie wordt doorgeleid naar een van de andere taken in de organisatie vergt dit dezelfde afweging ten aanzien van de te verstrekken gegevens als bij doorgeleiding naar een externe organisatie. Geef inzicht in de regels die daarvoor gelden. Maak daarbij gebruik van het juridisch kader in hoofdstuk 3.

Toelichting

Veel meldpunten zijn ondergebracht bij een instelling die ook bemoeizorg levert of medische behandelingen doet. Juridisch gezien zijn dit verschillende taken met elk een eigen juridisch kader voor de gegevensverwerking. In hoofdstuk 3 is aangegeven dat de meldpunttaak valt onder de wettelijke taken van het college van B&W en de burgmeester. Gegevens die in het kader van deze taak verzameld worden mogen in principe zonder toestemming van betrokkene verstrekt worden aan anderen, voor zover dat noodzakelijk is voor de meldpunttaak. Bijvoorbeeld omdat de betreffende partij hulp moet gaan verlenen, of moet gaan toeleiden naar hulp. Wat dit betekent voor BIG-geregistreerde professionals staat uitgebreider toegelicht in paragraaf 3.2.2.

Als binnen de organisatie ook medische behandelingen worden uitgevoerd, dan zal dit in de regel gebeuren op basis van een medische behandelovereenkomst. Op de informatie die verzameld wordt in het kader van een behandeling is het medisch beroepsgeheim van toepassing.

Die verschillende taken en juridische kaders kunnen tot verwarring leiden onder medewerkers. Daarom is het belangrijk dat een organisatie waar meerdere taken aan de orde kunnen zijn, goed afbakent welke activiteiten onder welke taak en dus onder welk kader voor gegevensverwerking vallen. Dat zij zorgdraagt voor gescheiden informatiehuishoudingen en voor goede werkinstructies voor de medewerkers zodat deze weten hoe te handelen bij de uitvoering van de verschillende taken.

4.2.3 Meldpunt niet-acuut gecombineerd met andere meldpunten in één organisatie

Sommige meldpunten fungeren als gecombineerd meldpunt voor niet acute zorg en meldpunt voor acute of crisissituaties. Bij de meeste meldpunten is het voornemen ook het meldpunt voor de Wvggz onder te brengen bij het meldpunt niet-acuut. De achterliggende gedachte is dat voor de triage die in al deze meldpuntfuncties een belangrijke rol speelt vergelijkbare kennis en expertise nodig is.
Ook ontstaat hierdoor een grotere herkenbaarheid en toegankelijkheid voor de burger. Juridisch gezien is er echter sprake van verschillende taken. Complicerende factor hierbij is dat bij veel meldingen wellicht pas later in het werkproces blijkt wat voor type melding het is. De wetgever heeft deze samenloop van meldfuncties vooralsnog niet voorzien, waardoor niet geheel duidelijk is hoe deze taken zich tot elkaar kunnen verhouden.

Privacy-risico's

Bij de combinatie van meerdere meldfuncties in een meldpunt doen zich verschillende risico's voor:

- Onduidelijkheid over het type melding dat gemeld wordt en daardoor:
  - Onduidelijkheid of verwarring bij de meldpuntmedewerker over de regels die gevolgd moeten worden bij het behandelen van een melding;
  - Onduidelijkheid bij partijen die bevraagd worden in het kader van de melding over het type melding en welke regels voor haar van toepassing zijn bij het beantwoorden van de vraag van het meldpunt;
- Bij verschillende typen meldingen over dezelfde persoon:
  - Vermenging van dossiers, bijvoorbeeld het niet-acuut dossier en het Wvggz dossier;
  - Onduidelijkheid of en zo ja welke gegevens in het kader van het ene type melding gebruikt mogen worden voor de behandeling van een ander type melding.

Aanbevelingen

- Stel een werkinstructie op voor medewerkers om in de eerste triage een keuze te maken voor het type melding en de omgang met gegevens als eenmaal een keuze is gemaakt voor het type melding.
- Onderdeel daarvan is dat aan partijen bij wie informatie opgevraagd wordt in het kader van het behandelen van de melding altijd geïnformeerd worden in het kader van welk type melding ze bevraagd worden.
- Geef in de werkinstructie aan hoe u wilt dat medewerkers omgaan met het gebruik van gegevens uit het ene melddossier t.b.v. het andere melddossier, bijvoorbeeld als een Wvggz-melding bij nader inzien toch een 'melding niet-acuut' blijkt te zijn.
- Houdt bij de inrichting van de informatiehuishouding rekening met het feit dat elk type melding een eigen dossier kent en dat duidelijk moet zijn welke informatie bij welk type melding hoort.

Toelichting

Zie paragraaf 2.3 voor een toelichting op de samenloop van een meldpunt niet-acuut en een meldpunt Wvggz.

4.2.4 Andersoortige taken uitgevoerd binnen het meldpunt niet-acuut

Sommige meldpunten voeren onder de vlag van het meldpunt ook taken uit die verder gaan dan advies, triage en doorgeleiden van een melding. Het gaat dan bijvoorbeeld om deelname aan een zorgoverleg of het vervullen van de procesregie bij complexe casuïstiek. Soms voert een meldpunt activiteiten uit die vergelijkbaar zijn met bemoeizorg. Naarmate een meldpunt meer verschillende activiteiten uitvoert die ook onder een andere taak zouden kunnen vallen, kunnen zich specifieke risico's voordoen vanuit het perspectief van privacy en de verwerking van persoonsgegevens.

Privacy-risico's en aanbevelingen

In deze situatie doen zich dezelfde risico's voor als in de situatie waarbij een meldpunt is ondergebracht in een organisatie die ook andere taken uitvoert. Echter omdat ze allemaal als werkzaamheden van het meldpunt worden gezien, doen de risico's zich in versterkte mate voor met name voor de partijen die bevraagd worden door het meldpunt. De aanbevelingen in de situatie dat een meldpunt is ondergebracht in een organisatie die ook andere taken uitvoert, zijn ook hier van toepassing.

Toelichting

Als een meldpunt andersoortige taken uitvoert, zijn de doelen voor de gegevensverwerking verschillend. De meldpunttaak heeft primair tot doel om door te geleiden naar de juiste instantie. Het inschakelen van bemoeizorg kan een logische uitkomst zijn van het meldproces, maar kent een ander specifiek doel: 'toeleiden naar zorg' van iemand die zorgmijdend is. De informatie in een bemoeizorgdossier zal daarom in de regel uitgebreider zijn, meer gevoelige informatie bevatten en een langere periode beslaan, dan nodig is voor een melddossier.

Het voeren van procesregie op een integraal plan kent weer een ander doel. Hier is het doel niet de doorgeleiding, of toeleiding, maar het coördineren van samenwerking tussen partijen. Hier wordt in de regel ook meer en gevoelige informatie uitgewisseld tussen partijen en over een langere periode, dan in het kader van sec de meldfunctie noodzakelijk is.

Bij deelname aan een zorgoverleg kunnen meerdere doelen aan de orde zijn. De betrokkenheid van het meldpunt zou vooral moeten zijn: beoordelen welke partij naar aanleiding van de melding het beste aan de slag kan.

De verschillen in doelen betekenen dat de gegevens die voor het een verzameld zijn, niet zomaar voor het ander gebruikt mogen worden. Daarom is het belangrijk dat medewerkers weten welke activiteiten tot welke taak behoren en dat er duidelijk onderscheid gemaakt wordt met betrekking tot de gegevensverwerking zowel met betrekking tot het verstrekken als het vastleggen van gegevens.

Bij gegevensdeling in het kader van casus- of zorgoverleggen zijn in het kader van de zorg- en veiligheidshuizen spelregels ontwikkeld om te voorkomen dat gevoelige persoonsgegevens onnodig verspreid raken onder de deelnemers van een overleg. Deze zijn toepasbaar op elke vorm van casusoverleg. Deze spelregels zijn:

- Het doel van het overleg is duidelijk en er nemen alleen partijen deel die nodig zijn voor het doel van het overleg. Een doel kan zijn: bepalen wie een casus oppakt, of komen tot een integraal plan.

De zeggenschap over gegevens die worden ingebracht blijft bij de degene die deze heeft ingebracht.

- Partijen die tijdens een overleg kennisnemen van gegevens van een andere partij, mogen deze niet automatisch gebruiken voor eigen taken en werkzaamheden.
- Partijen die gegevens uit het overleg willen gebruiken voor eigen taken en werkzaamheden, mogen dit uitsluitend doen indien degene die deze heeft ingebracht dit goed vindt, en alleen voor de doelen waarvoor deze ze wil verstrekken. Vuistregel is dat enkel partijen die een interventie (gaan) doen gegevens 'mee naar huis nemen' voor het uitvoeren van de afgesproken interventie.
- Elke partij beoordeelt steeds op basis van de voor hem geldende kaders of het mogelijk is om gegevens te verstrekken.

4.2.5 Afspraken met andere organisaties

Alle meldpunten hebben een aantal partners waar ze veel meldingen van ontvangen, partners die veel in beeld zijn als er informatie opgevraagd moet worden in het kader van de behandeling van een melding, of die vaak in beeld zijn als partij waarnaar wordt doorgeleid. Daarnaast is het meldpunt in sommige regio's nog onderdeel van een breder samenwerkingsconvenant in het kader van overlast of OGGZ. Het verschaft de medewerkers van het meldpunt en de medewerkers van partijen waar vaak mee samen gewerkt veel duidelijkheid als op bestuurlijk niveau afspraken gemaakt worden over de samenwerking, in het bijzonder over de gegevensverwerking. Een convenant of protocol is niet noodzakelijk als grondslag voor de gegevensverwerking, maar kan wel helpen om duidelijkheid te creëren en de samenwerking in de praktijk soepel te laten verlopen.

In deze paragraaf geven we daarvoor een aantal aandachtspunten mee.

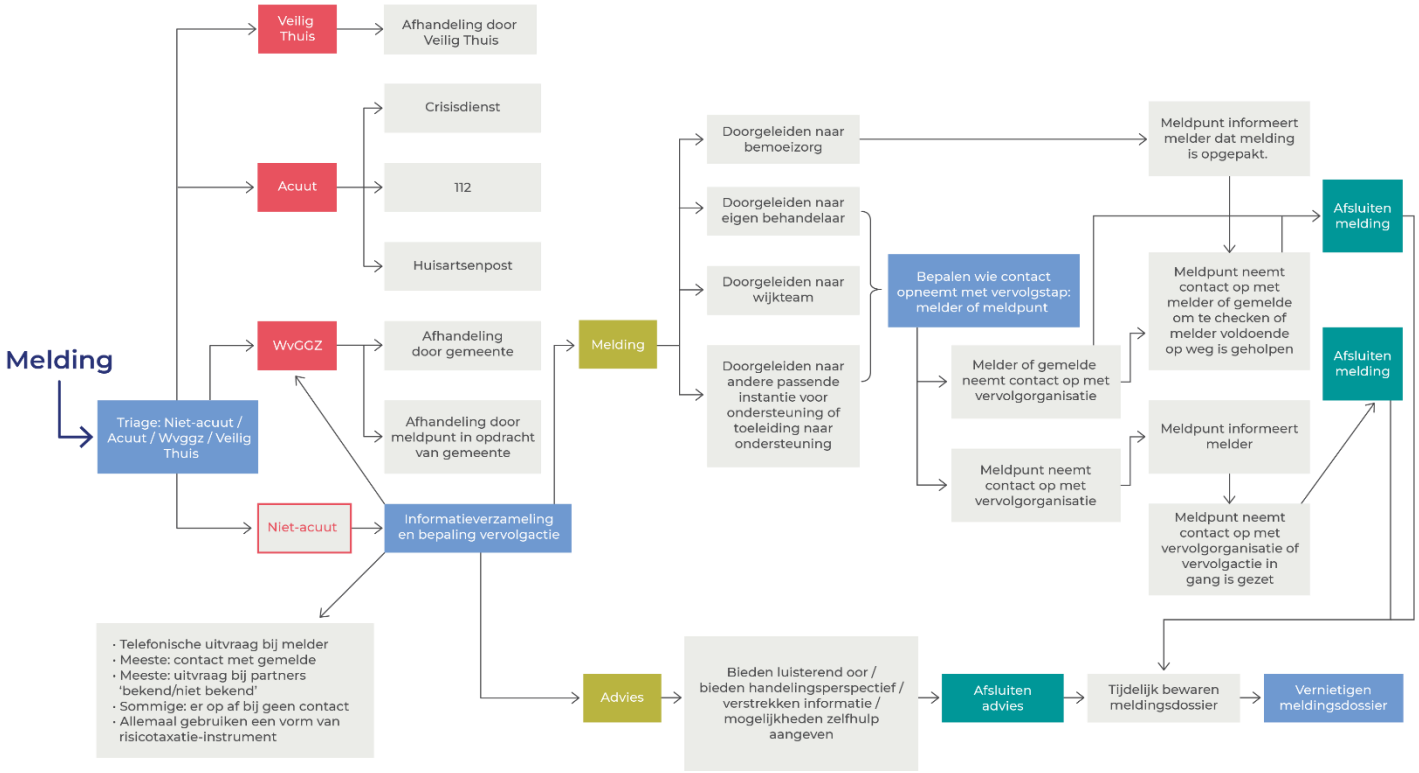
Aandachtspunten bij samenwerkingsafspraken

- Maak in het convenant duidelijke onderscheid tussen de verschillende taken die er in het kader van de samenwerking worden uitgevoerd. Benoem daarbij bijvoorbeeld het onderscheid tussen de meldpunttaak, de bemoeizorgtaak en andere taken;
- Benoem in het convenant ook de taken van andere partijen die aan de orde kunnen zijn bij bijvoorbeeld het doorgeleiden van meldingen;
- Maak in het privacy-protocol onderscheid tussen de regels die op gaan voor het uitwisselen van gegevens met betrekking tot de verschillende taken. Baseer de regels voor de meldpuntfunctie daarbij op deze handreiking, die voor bemoeizorg op de handreiking bemoeizorg, en die voor bijvoorbeeld het meldpunt Wvggz en het verkennend onderzoek op de te verschijnen handreiking daar over.

4.3 Werkprocessen en triage

Algemene toelichting

Voor het generieke werkproces van het meldpunt 'niet-acuut' gaan we uit van het werkproces zoals geschetst in paragraaf 2.2.



Vanuit het perspectief van gegevensverwerking doen zich een aantal risico's voor. Sommige zijn standaardrisico's die inherent zijn aan het werken met gegevens, andere hangen samen met inhoudelijke keuzes ten aanzien van het werkproces die verschillende meldpunten maken.

De kern van het werkproces van een meldpunt is triage. Alle informatieverzameling staat in het teken van het verhelderen, routeren en indien noodzakelijk doorgeleiden van een melding zodat de persoon in kwestie – melder of gemelde – geholpen is met een advies, een instantie aan de slag gaat om de noodzakelijke hulp, zorg of ondersteuning te bieden, of om toe te leiden naar hulp, zorg of ondersteuning. In het werkproces van de meldpunten zijn een aantal processtappen te herkennen die elk een andere mate van gegevensverwerking vragen en waarin afwegingen gemaakt worden ten aanzien van het opvragen en verstrekken van informatie.

De eerste stap is de triage als de melding binnen komt. Op basis van de informatie van de melder wordt bepaald welk type melding het betreft: acuut, niet-acuut, Wvggz of anders.

De tweede stap is de informatieverzameling en bepaling vervolgroute. Hierin wordt de melding verder verkend om een goed beeld van de situatie te krijgen. Er wordt contact gezocht met de gemelde, gecheckt op bekendheid bij het meldpunt en indien nodig worden partijen benaderd die mogelijk al een betrokkenheid hebben bij de melder of gemelde. Op basis van het beeld dat zo ontstaat wordt de juiste vervolgroute bepaald: advies, of doorgeleiding naar een specifieke instantie.

De derde stap is de 'melding'. Hier wordt bepaald naar welke instantie wordt doorgeleid en welke gegevens noodzakelijk zijn om te verstrekken bij de overdracht en wie contact opneemt met de vervolgorganisatie: de melder, de gemelde of het meldpunt.

De vierde stap is de terugmelding aan de melder. Hier vindt een afweging plaats welke informatie verstrekt kan worden aan de melder met betrekking tot de afhandeling va de melding.
Tot slot is er de beslissing ten aanzien van bewaren en vernietigen. Hierin wordt bepaald in welke categorie de melding hoort en welke bewaartermijn daarbij hoort.

Een aspect waarin verschillen te zien zijn bij de meldpunten is de activiteiten die zij uitvoeren t.b.v. de processtap 2 'informatieverzameling en bepaling vervolgactie'. Met name als het niet mogelijk blijkt contact te leggen met de gemelde. Sommige meldpunten geleiden bij 'geen contact' door naar een wijkteam, of als de situatie daar aanleiding toe geeft naar een bemoeizorgteam. Andere gaan zelf 'eropaf' om het contact te leggen, soms zelfs langduriger, waarbij het tegen bemoeizorg aanzit.

Een tweede aspect dat speelt vanuit het oogpunt van gegevensverwerking zijn de bewaartermijnen, en de doelen van het bewaren van het meldingdossier. De omgang met bewaartermijnen laat een grote variëteit zien. Sommige hanteren een termijn van 1, 2 of 5 jaar. Anderen sluiten aan bij bewaartermijnen van de behandeltaken van de organisatie en hanteren 15 jaar. Sommige maken onderscheid bij de bewaartermijnen afhankelijk van de problematiek en het gekozen vervolgtraject. Anderen hanteren één termijn voor alle meldingen.

Alle meldpunten geven aan dat het enige tijd bewaren van een meldingdossier van belang is om te kunnen signaleren of een persoon vaker meldt, of gemeld wordt, omdat dat wellicht een indicatie kan zijn van zwaardere problematiek.

4.3.1 Privacy-risico's bij het generieke werkproces

In het generieke werkproces doen zich een aantal privacy-risico's voor die inherent zijn aan het werken met gegevens.

Privacy-risico's

- De doelen van de verschillende processtappen zijn niet concreet genoeg beschreven waardoor niet duidelijk is en ook geen duidelijke afweging gemaakt kan worden, welke gegevens in een bepaalde stap van het proces noodzakelijk zijn. Hierdoor bestaat het risico dat veel meer gegevens verzameld worden dan noodzakelijk.
- Er zijn geen duidelijke werkinstructies voor de professional over het verzamelen en vastleggen van gegevens in het melddossier, waardoor hier veel meer gegevens in terecht komen, dan uiteindelijk noodzakelijk blijken voor de triage en doorgeleiding.
- Bij het doorgeleiden van een melding naar een andere instantie, vindt geen of onvoldoende afweging plaats welke gegevens noodzakelijk zijn voor de betreffende partij, waardoor meer gegevens worden verstrekt dan noodzakelijk.
- Alle drie bovenstaande situaties kunnen er ook toe leiden dat er te grote voorzichtigheid ontstaat, waardoor er minder gegevens verwerkt worden dan voor een goede taakuitvoering noodzakelijk is, terwijl het wel mogelijk zou zijn om die gegevens te verwerken of verstrekken.

Aanbevelingen

- Zorg voor concrete doelomschrijvingen bij elke processtap die richting geven aan de afwegingen ten aanzien van gegevensverwerking.
- Bij verschillende activiteiten in een processtap: formuleer eventueel een doel per activiteit.
- Zorg voor werkinstructies over het verzamelen en vastleggen van gegevens.
- Neem in de werkinstructies op dat er bij het doorgeleiden altijd een afweging moet plaats vinden ten aanzien van de noodzakelijke gegevensverstrekking aan de instantie die de vervolgacties in gang gaat zetten. Overweeg met 'vaste partners' afspraken te maken over de te verstrekken gegevens bij het doorgeleiden van meldingen.

Toelichting op doelformuleringen

Het formuleren van doelen per processtap is een belangrijke voorwaarde om medewerkers in staat te stellen een noodzakelijkheidsafweging te maken over het vastleggen en verstrekken van gegevens. De doelomschrijving bij de triage van de melding zou kunnen zijn: bepalen of het een melding betreft in het kader van acuut, niet-acuut, Wvggz of een ander meldpunt. De doelomschrijving bij de stap 'informatieverzameling en bepaling vervolgactie' zou kunnen zijn: beter zicht krijgen op de gemelde situatie en bepalen welke instantie het beste ingeschakeld kan worden naar aanleiding van de melding. Onderdeel van de doelomschrijving van de stap 'meldpunt neemt contact op met vervolgorganisatie' zou kunnen zijn: de beoogde instantie in staat stellen om de juiste actie te ondernemen. Als een meldpunt zelf 'er-op-af' gaat omdat er telefonisch geen contact gelegd kan worden, is het belangrijk om het doel hiervan helder te omschrijven en af te bakenen.

Toelichting werkinstructie afweging noodzakelijke gegevensverwerking

Onderdeel van de werkinstructie kan zijn, dat de medewerker steeds aan het eind van een processtap bepaalt welke informatie noodzakelijk is om te vast te leggen en welke niet. Als de melding afgehandeld kan worden met een advies of doorverwijzing, is het niet nodig heel uitgebreid informatie vast te leggen. Bij het verkennen van een melding in gesprek met de gemelde of de uitvraag bij partnerorganisaties, zullen in de regel meer gegevens verzameld en uitgewisseld worden dan uiteindelijk nodig blijken. Dit is inherent aan het verkennen van een melding. Op het moment dat de situatie helder is en de vervolgactie duidelijk, zal vaak blijken dat een deel van de verzamelde informatie niet relevant is. Uitgangspunt zou moeten zijn dat deze dan ook niet vastgelegd wordt in het

melddossier of weer verwijderd wordt om te voorkomen dat deze vervolgens onnodig wordt verstrekt bij het doorgeleiden naar de vervolgorganisatie.
In paragraaf 3.5 is een tabel opgenomen met voorbeelden van valide en niet valide argumenten bij het bepalen van de noodzaak om gegevens vast te leggen of niet.

4.3.2 Gegevensverwerking bij terug melden aan de melder

Een onderdeel van het proces is het terug melden aan degene die heeft gemeld, zodat deze weet dat er actie wordt ondernomen. Bij het bepalen van welke informatie wordt teruggekoppeld, maken de alle pilots onderscheid tussen een burger die meldt en een professional of instantie die meldt.
In de situatie dat een burger meldt, blijft de terugmelding beperkt tot de mededeling 'de melding is opgepakt'. Bij professionals of instanties, wordt afhankelijk van de partij die meldt, bepaalt hoeveel informatie wordt terug gemeld.

Privacy-risico's

- Bij het terug melden kunnen zich verschillende risico's voor doen:
- Bij terug melden aan een meldende burger: de melder krijgt gevoelige gegevens over de persoonlijke situatie van de gemelde. Hierdoor kan de privacy van de gemelde onevenredig geschaad worden, met een risico van stigmatisering, risico's voor de veiligheid of risico bijvoorbeeld voor de rechtspositie van de gemelde.
- Bij het terug melden aan een professional of instantie:
  - Dezelfde risico's als hierboven;
  - Het risico dat deze gegevens ontvangt en vastlegt die niet noodzakelijk voor zijn taken in relatie tot de betrokkene;
  - Het risico dat deze gegevens ontvangt waar hij geen grondslag voor heeft, dit geldt met name ten aanzien van gegevens over de gezondheid of strafrechtelijke gegevens;
  - Het risico dat de professional of instantie deze gegevens vastlegt en voor andere doelen gaat gebruiken dan waarvoor ze zijn verstrekt.

Aanbevelingen

- Bij terug melden aan een meldende burger: door slechts terug te melden 'dat de melding wordt opgepakt' zonder verdere inhoudelijke informatie, wordt dit risico voorkomen.
- Bij terug melden aan een professional of instantie:
  - Overweeg of het mogelijk is om de terugmelding te doen in overleg met de gemelde;
  - Maak een afweging omtrent de terug te melden informatie. Neem daarin mee: of het gezien de taak van de meldende instantie en zijn betrokkenheid bij de gemelde noodzakelijk is om meer informatie te verschaffen en of de meldende instantie bepaalde gegevens zoals gezondheidsgegevens mag verwerken of niet;
  - Neem in de werkinstructie op dat bij een terugmelding altijd wordt vermeld dat deze informatie niet voor andere doeleinden mag worden gebruikt;
  - Maak eventueel een overzicht van welk type professional of instantie welke informatie krijgen bij een terugmelding;
  - Maak afspraken met instanties die regelmatig melden over informatie in de terugmelding en over de strikte doelbinding op het gebruik van die informatie.

Toelichting

Belangrijkste doel van regelgeving rond gegevensverwerking en privacy is het beschermen van de persoonlijke levenssfeer van mensen. Daarom moet bij het terug melden aan burgers die melden altijd terughoudendheid betracht worden, ook al omdat niet op voorhand bekend is hoe de relatie tussen

melder en gemelde is. Er kan immers sprake zijn van belangen of conflicten die niet bekend zijn bij het meldpunt.

Voor professionals of instanties die melden, geldt in principe dezelfde terughoudendheid, voor zover zij geen directe betrokkenheid hebben bij de gemelde vanuit een eigen taak. Zij zijn dan niet anders dan een burger die meldt.

Voor zover een meldende professional of instantie wel een betrokkenheid heeft bij de gemelde vanuit een eigen taak, is het bij de terugmelding van belang om af te wegen welke gegevens noodzakelijk zijn om te verstrekken gezien deze betrokkenheid. Stel je zelf daarbij de vraag: wat is het doel van het verstrekken van meer informatie dan 'de melding is opgepakt'. En verzeker je ervan dat de informatie niet voor andere doeleinden wordt gebruikt. Immers instanties kunnen ook meerdere belangen hebben in hun relatie tot de gemelde.

Professionals en instanties mogen uitsluitend bijzondere persoonsgegevens zoals gezondheidsgegevens of strafrechtelijke gegevens verwerken voor hun taak, als dat bij wet is geregeld. Als dat niet is geregeld mogen ze bijvoorbeeld geen informatie ontvangen dat een melding wordt opgepakt door de GGZ.

Beide zijn zaken die een medewerker van het meldpunt moeilijk kan overzien. Daarom is het belangrijk dat het meldpunt afspraken maakt met organisaties waar veel mee wordt samen gewerkt over het gebruik van informatie die ze van het meldpunt krijgen. Ook is het belangrijk dat de meldpuntorganisatie de medewerkers inzicht geeft in welke organisaties bepaalde gegevens wel of niet mogen ontvangen.

4.3.3 Bewaartermijnen en signalering

De wet geeft geen duidelijke bewaartermijnen voor het melddossier. Het melddossier is géén medisch behandeldossier en ook geen 'toeleidingdossier'. De bewaartermijnen die gelden voor die taken zijn hier dus niet van toepassing. Dat betekent dat voor het melddossier de AVG van toepassing is. Deze hanteert een open norm: 'niet langer dan noodzakelijk'. De bewaartermijn moet beperkt zijn en onderbouwd worden. Duidelijk moet zijn met welk doel het dossier wordt bewaard en de gekozen bewaartermijn noodzakelijk is. Elk meldpunt zal hieraan zelf beleidsmatig invulling moeten geven.

Privacy-risico's

- Bij het bewaren van het melddossier kunnen zich verschillende risico's voor doen:
  Het is onduidelijk hoe lang het melddossier wordt bewaard en met welk doel. Het bewaren is dan onrechtmatig;
- Het melddossier wordt langer bewaard dan noodzakelijk gezien het doel waarvoor het wordt bewaard;
- Het melddossier wordt korter bewaard dan noodzakelijk gezien het doel waarvoor het wordt bewaard.

Aanbevelingen

- Leg in het beleid van het meldpunt vast hoe lang het melddossier wordt bewaard nadat de melding is afgesloten en met welk doel dit gebeurt. Onderbouw de gekozen periode en geef aan wanneer en hoe deze wordt geëvalueerd en bijgesteld;
- Maak eventueel onderscheid in bewaartermijnen op basis van het type problematiek of de gekozen vervolgroute;
- Leg in het beleid vast of en zo ja in welke gevallen er een uitzondering kan worden gemaakt op de bewaartermijn en voor hoe lang de bewaartermijn maximaal verlengd kan worden;
- Zorg in geval van uitzonderingen dat de burger hier over wordt geïnformeerd;
- Laat geen open eindjes bestaan: zorg dat van elk dossier duidelijk is wanneer het vernietigd moet worden of wanneer de bewaartermijn opnieuw beoordeeld moet worden.

Toelichting

De meeste meldpunten geven aan dat het enige tijd bewaren van een melddossier van belang is om te kunnen signaleren of een persoon vaker meldt, of gemeld wordt. Dat kan immers een indicatie zijn van zwaardere problematiek en relevant zijn in het kader van de doorgeleiding. Indien een persoon binnen korte tijd vaker meldingen doet, kan dat ook een indicatie zijn van een probleem bij de melder. Op basis hiervan kan een duidelijk doel geformuleerd worden voor het enige tijd bewaren van het melddossier. Leg de handelswijze ten aanzien van de bewaartermijnen vast in het privacy-beleid van het meldpunt.

Het bewaren van melddossiers voor het genereren van beleids- en managementinformatie is geen rechtmatig doel. Hiervoor kan immers volstaan worden met het geanonimiseerd bewaren van de karakteristieken van meldingen. Ook voor evaluatie of leerdoeleinden is het niet nodig om de melddossiers op persoonsniveau te bewaren. Dossiers kunnen ontdaan van persoonsgegevens bewaard worden. Maar bij voorkeur wordt er gewerkt met samengestelde casussen die niet tot personen herleidbaar zijn.

Benadering ten aanzien van bewaartermijnen

De bewaartermijn moet beperkt zijn en onderbouwd worden. Duidelijk moet zijn met welk doel het dossier wordt bewaard en de gekozen bewaartermijn noodzakelijk is.

Een eerste stap in de benadering is om onderscheid te maken op basis van het gekozen vervolgtraject. Voor een melding die leidt tot een (zelfhulp)advies kan wellicht een minder lange bewaartermijn gelden dan voor andere meldingen. Een melding die leidt tot het inzetten van bemoeizorg moet wellicht langer bewaard worden dan een melding die wordt doorgezet naar het wijkteam in het kader van toeleiding sociaal domein.

Een tweede stap is om in de bewaartermijn onderscheid te maken tussen het ‘dicht zetten’ van het melddossier en het vernietigen. In die benadering wordt het dossier bijvoorbeeld 6 maanden na afhandeling ‘dicht gezet’ en een jaar na afhandeling vernietigd. Dit betekent dat het melddossier na 6 maanden niet meer kan worden ingezien, maar dat wel zichtbaar is dat de persoon eerder gemeld is of eerder een melding heeft gedaan. Als dan in de periode tussen 6 maanden en een jaar een nieuwe melding komt, kan het melddossier opnieuw toegankelijk gemaakt worden, bijvoorbeeld door de manager van het meldpunt. Daarna gaat de bewaartermijn opnieuw lopen. Deze handelwijze biedt een balans tussen het beschermen van de privacy van de burger en de noodzaak om bij nieuwe meldingen de eerdere informatie toch weer te kunnen gebruiken.

Een derde stap is het benoemen van criteria om een uitzondering te maken op de in het beleid vastgelegde bewaartermijn. Dat betekent dat er ruimte gecreëerd wordt voor de professionele afweging om in een concrete situatie een langere bewaartermijn te hanteren. Zo'n professionele beslissing zal dan altijd onderbouwd moeten worden. Het is belangrijk dat er geen open einde bestaat. Duidelijk zal moeten zijn hoe lang de bewaartermijn verlengd wordt of na maximaal hoeveel tijd een nieuwe beoordeling moet volgen.

De praktijk
De genoemde periodes van 6 maanden en 1 jaar in deze toelichting zijn arbitrair. In de praktijk hanteren meldpunten vaak een periode van 5 jaar voor meldingen die zijn doorgeleid naar bemoeizorg. En van 1 jaar voor meldingen die tot een advies hebben geleid.
Vanuit oogpunt van bescherming van de privacy van de burger verdient het tenminste aanbeveling om in ieder geval de dossiers na een veel kortere periode, bijvoorbeeld respectievelijk een jaar en een half jaar 'dicht te zetten'

4.4 Inrichten van informatiesystemen: opslag, toegang, beheer, informatieveiligheid

Algemeen
De meeste meldpunten niet-acuut zitten 'in huis', of maken onderdeel uit van een organisatie die ook andere taken uitvoert, vaak een GGD, maar het kan ook de gemeentelijke organisatie zijn. Het meldpunt maakt dan meestal gebruik van het informatiesysteem, de technische en beheersmatige faciliteiten van deze organisatie: opslag, toegangsbeheer, informatiebeveiliging. In paragraaf 4.2.2 is al aandacht besteed aan een aantal specifieke risico's. In deze paragraaf gaan we hier nader op in met betrekking tot de inrichting van de informatiesystemen, informatiebeveiliging en datalekken.

4.4.1 Opslag, toegang en beheer van het melddossier indien het meldpunt werkt op de informatiesystemen van een organisatie die ook andere taken uitvoert

Privacy-risico's
Als een meldpunt niet-acuut gebruik maakt van het informatiesysteem van de organisatie waar het is onder gebracht, doen zich verschillende privacy-risico's voor:

- Vermenging van de gegevenshuishoudingen: de gegevenshouding van de meldpuntfunctie is niet goed zijn gescheiden van die voor andere taken, waardoor:
  - Medewerkers toegang hebben tot gegevens terwijl ze dat niet mogen hebben;
  - Gegevens die thuishoren in het meldpuntdossier ten onrechte terecht komen in of gekoppeld worden aan dossiers die voor andere taken zijn aangelegd en vice versa;
  - Verkeerde bewaartermijnen worden gehanteerd ten aanzien van het meldpuntdossier.

Deze risico's treden in gelijke mate op als het meldpunt door de gemeente zelf wordt uitgevoerd of is ondergebracht bij een andere organisatie.

Aanbevelingen

- Zorg voor een goede scheiding in de informatiehuishouding voor de meldpuntfunctie en de andere taken, o.a. door een apart meldpuntdossier in te richten. Indien vanuit de meldpuntfunctie wordt doorgeleid naar een van de andere taken in de organisatie vergt dit dezelfde afweging ten aanzien van de te verstrekken gegevens als bij doorgeleiding naar een externe organisatie.
- Besteed bij het beheer o.a. aandacht aan:
  - Afspraken over het autorisatiebeleid ten aanzien van de melddossiers. Uitgangspunt daarbij dat uitsluitend meldpuntmedewerkers toegang hebben tot het melddossier;
  - De rol van de leidinggevende van het meldpunt bij het toekennen en intrekken van autorisaties;
  - Het beleid ten aanzien van gegevensverwerking en privacy van het meldpunt, o.a. met betrekking tot het bewaren en vernietigen van de melddossiers.

4.4.2 Informatieveiligheid

Het ligt voor de hand dat op de informatiehuishouding in het meldpunt het informatieveiligheidsbeleid toegepast wordt van de organisatie waar het meldpunt is onder gebracht.

Privacy-risico's

Hierbij kan zich het volgende risico voordoen:

- De normen voor informatieveiligheid van de organisatie waar het meldpunt is onder gebracht zijn minder zwaar dan de normen die gesteld moeten worden aan de gegevens die het meldpunt verwerkt. Denk daarbij met name aan de verwerking van gezondheidsgegevens en strafrechtelijke gegevens. Aangezien de meeste meldpunten zijn ondergebracht bij een GGD of GGZ-instelling is de kans dat de hier onder genoemde risico's zich voordoen klein.

Aanbevelingen

- Sluit voor de informatiebeveiliging aan bij de normen die reeds gebruikt worden door de verwerkingsverantwoordelijke. Voor het college op de gemeente, is dat de Baseline Informatiebeveiliging Overheid, voor de GGD en de GGZ is dat NEN 7510. Deze zijn voldoende voor de gegevens die in een meldpunt niet-acuut aan de orde zijn.

4.5 Transparantie en de positie van de burger

Algemene toelichting

Een burger heeft het recht om te weten dát er gegevens over hem worden verwerkt, en wat dat voor hem of haar betekent. Ook heeft de burger rechten en moet deze weten hoe hij van zijn rechten gebruik kan maken. Dit geldt zowel voor de gemelde als de melder. Daarnaast is transparantie over het gebruik van persoonsgegevens tijdens de werkzaamheden een belangrijk uitgangspunt van de AVG. Bij de meldpunten niet-acuut zal de gemelde veelal niet op de hoogte zijn van de melding en soms ook moeilijk bereikbaar. Des te belangrijker is het dat er goed wordt nagedacht over de wijze waarop de burger toch geïnformeerd wordt en zijn rechten kan uitoefenen.

Het informeren van de burger kent twee aspecten:

1. De formele informatieplicht aan de burger inzake de AVG
2. ransparantie over de gegevensverwerking tijdens het meldproces

Privacy-risico's

Ten aanzien van de rechten van de burger en de transparantie doen zich verschillende risico's voor:

- Burgers worden tijdens het dienstverleningsproces te weinig of niet geïnformeerd ten aanzien van hun rechten en plichten in het kader van gegevensverwerking;
- Er zijn geen of ingewikkelde processen en procedures ingericht voor de situatie waarin een burger gebruik wil maken van zijn of haar rechten met betrekking tot bezwaar, inzage of correctie, waardoor deze rechten slechts met grote moeite geëffectueerd kunnen worden;
- Medewerkers zijn niet op de hoogte van de rechten van burgers met betrekking tot privacy en gegevensverwerking en de daarvoor ingerichte processen, waardoor zij de burger niet adequaat kunnen informeren en ondersteunen bij het uitoefenen van hun rechten;
- Voor medewerkers is niet duidelijk hoe zij de burger tijdens het proces op de hoogte moeten houden van de stappen die worden gezet en de gegevens die zij daarvoor willen verwerken. De burger kan dan niet weten welke persoonsgegevens er over hem worden verwerkt, waarom en met wie informatie wordt gedeeld. Hij kan daardoor ook niet effectief gebruik maken van zijn rechten.

Aanbevelingen
- Besteed in het beleid van het meldpunt aandacht over de wijze waarop invulling gegeven wordt aan de informatieplicht en aan het principe van transparantie tijdens het meldproces. Verwerk dit ook in de werkinstructies voor de medewerkers. Besteed daarbij aandacht aan:
  - Onderscheid tussen melder en gemelde;
  - Het moment van informeren van de gemelde en hoe te handelen als gemelde niet geïnformeerd kan worden;
  - De wijze waarop de gemelde geïnformeerd wordt tijdens het behandelen van de melding.
- Richt processen en procedures zo in, dat burgers die gebruik willen maken van hun rechten laagdrempelig en snel geholpen kunnen worden.

Toelichting
T.a.v. de melder
Tijdens de melding kan deze geïnformeerd worden dat zijn naam en contactgegevens worden vastgelegd, met welk doel en voor hoe lang. Ook kan gecheckt worden of melder bezwaar heeft tegen het kenbaar maken van zijn naam aan de gemelde. Eventueel kan verwezen worden naar informatie op de site van het meldpunt.

T.a.v. de gemelde
Uitgangspunt is dat de gemelde zo spoedig mogelijk wordt geïnformeerd over het feit dat hij is gemeld, bijvoorbeeld als het meldpunt contact opneemt met de gemelde om de situatie te bespreken. De medewerker kan dan aangeven of, en zo ja welke gegevens worden vastgelegd, en bespreken wat de vervolgstappen zijn, welke informatie nodig is en waarom.

Als het niet mogelijk is om dit te bespreken, bijvoorbeeld omdat de gemelde niet te bereiken is, of niet aanspreekbaar, is het belangrijk dat wordt vastgelegd waarom gemelde niet kan worden geïnformeerd en aan te geven wanneer dat wel gebeurt.

4.6 Training en bewustwording van medewerkers

Algemene toelichting
Zorgvuldige omgang met persoonsgegevens is in belangrijke mate een organisatievraagstuk. Zonder goede inrichting van de werkprocessen en de daarvoor noodzakelijke gegevensverwerking kunnen professionals niet goed invulling geven aan de regelgeving rond gegevensverwerking. Het in de praktijk invulling geven aan een zorgvuldige omgang met gegevens is een onderdeel van professionele kwaliteit en vraagt om instructie, training en bewustwording.

Een specifiek onderdeel van professionele kwaliteit op het snijvlak van inhoud en privacyregelgeving is de dossiervoering. Welke informatie neem je op in een dossier, en welke niet?

4.6.1 Kennis met betrekking tot beleid en werkinstructies

Privacy-risico's

Bij te weinig aandacht voor training en bewustwording van medewerkers kunnen zich verschillende risico's voordoen:

- Door gebrekkige kennis over het beleid en de werkinstructies wordt de zorgvuldige omgang met persoonsgegevens onvoldoende intrinsiek onderdeel van de dagelijkse professionele praktijk. Daardoor is de kans groot dat onnodig of bovenmatig gegevens uitgevraagd en geregistreerd worden en/of dat er onvoldoende aandacht is voor de rechten van de burger. De burger loopt daarmee het risico dat zijn of haar privacy wordt geschonden;
- Omgekeerd kan het betekenen dat medewerkers zich te veel laten belemmeren in hun werk door onnodige angst de privacyregels te schenden, waardoor probleemsituaties te laat of pas in een laat stadium zichtbaar worden en kunnen worden aangepakt;
- Door gebrek aan kennis in de organisatie over privacy en gegevensverwerking in relatie tot de dienstverlening in het sociaal domein, wordt de kwetsbaarheid van medewerkers vergroot. Bij complexe of zwaarwegende afwegingen ten aanzien van de omgang met gegevens, kunnen medewerkers bijvoorbeeld niet terugvallen op deskundige ondersteuning;
- De risico's die zich voordoen door gebrekkige kennis bij de medewerkers van het meldpunt, kunnen zich ook voordoen als kennis bij belangrijke samenwerkingspartners van het meldpunt ontbreekt. Organisaties kunnen dan te terughoudend zijn in het verstrekken van informatie aan het meldpunt of willen veel meer informatie dan noodzakelijk in het kader van hun vervolgacties.

Aanbevelingen

- Besteed in training en opleiding van medewerkers aandacht aan het thema privacy en gegevensverwerking, het beleid ten aanzien van gegevensverwerking in het meldpunt, de afspraken met samenwerkingspartners en de rechten van betrokkene(n);
- Stel werkinstructies op voor medewerkers, met name voor het maken van afwegingen ten aanzien van de gegevensverwerking in de verschillende processtappen en ten aanzien van de rechten van de burger;
- Overweeg om specifieke expertise te organiseren in de organisatie, om medewerkers te adviseren bij lastige afwegingen in het kader van privacy en gegevensverwerking;
- Maak afspraken met samenwerkingspartners over het informeren van hun medewerkers over de afspraken rond gegevensverwerking en de wijze waarop de privacy van burgers in het meldpunt is geborgd;
- Organiseer het leren, bijvoorbeeld door periodiek in werkoverleg vraagstukken die zich in de praktijk hebben voorgedaan te bespreken en tot goede werkafspraken te komen.

4.6.2 Kwaliteit van dossiers

Dossiervoering is een belangrijk aspect van professionele kwaliteit. Het dossier vormt de basis voor een goede inhoudelijk beoordeling van de situatie. Bewuste afwegingen ten aanzien van de informatie die in een dossier wordt opgenomen is ook een belangrijke voorwaarde om de privacy van burgers te waarborgen.

Privacy-risico's

Als medewerkers onvoldoende getraind zijn in dossiervoering doen zich een aantal risico's voor:

- Medewerkers nemen veel meer informatie op in het dossier dan noodzakelijk is, gezien de functie van het meldpunt. Bijvoorbeeld omdat emailwisselingen met derden integraal zijn opgenomen in het dossier;
- Medewerkers zijn juist te voorzichtig en nemen daarom te weinig informatie op in het dossier, waardoor de vervolginstantie of een collega die de casus overneemt niet goed geïnformeerd kan worden;
- Er ontstaan 'schaduwdossiers' onder het mom van persoonlijke werkaantekeningen omdat men gehoord heeft dat deze niet tot het dossier behoren;
- In het dossier is niet duidelijk van wie de informatie afkomstig is, de melder, de gemelde, een naaste of een professionele instantie;
- In het dossier is geen duidelijk onderscheid tussen feiten en meningen of interpretaties door de medewerker of door de bron van de informatie;
- Er blijft na afsluiting onnodig meer inhoudelijke en gevoelige informatie achter in het dossier dan noodzakelijk is voor het doel van het bewaren.

Aanbevelingen
- Besteed in trainingen aandacht aan de kwaliteit van dossiervoering;
- Neem in de werkinstructie op dat de medewerker aan het eind van elke processtap steeds een afweging maakt op basis van het beeld dat is ontstaan en de geplande vervolgstappen welke informatie noodzakelijk is om te behouden en welke verwijderd kan worden;
- Neem in de werkinstructie expliciet op dat emailverkeer niet integraal in de dossiers opgenomen wordt, maar alleen de essentie van de emailwisseling;
- Besteed aandacht aan het fenomeen 'persoonlijke werkaantekeningen' en maak duidelijk dat dit niet mag leiden tot 'schaduwdossiers';
- Houd periodiek, bijvoorbeeld een of twee keer per jaar, een 'schouw' op dossiers, bij voorkeur geanonimiseerd, om samen te leren en tot betere dossiervoering te komen;
- Stel richtlijnen op voor het opschonen van het dossier bij afsluiting van een melding. Geef daarin aan welke gegevens noodzakelijk zijn om te bewaren en waarom en welke informatie vernietigd kan worden. Verwerk de richtlijnen in werkinstructies voor de medewerkers.

Toelichting

Persoonlijke werkaantekeningen

Werkaantekeningen zijn aantekeningen die een professional maakt uitsluitend voor persoonlijk gebruik. Het kan bijvoorbeeld gaan om veronderstellingen die hij of zij nog wil toetsen of verifiëren alvorens deze in het dossier op te nemen. Een gevaar hiervan is dat de persoonlijke werkaantekeningen uitgroeien tot een schaduwdossier waar de betrokkene geen weet van heeft en waarover hij dus ook zijn rechten niet kan uitoefenen.

De kern van deze werkwaantekeningen is echter dat ze persoonlijk zijn. Zij kunnen dus geen rol spelen in formele besluitvorming. Daarvoor zouden ze eerst toegevoegd moeten worden aan het reguliere dossier. Ook mogen de persoonlijke werkaantekeningen niet verstrekt worden aan anderen ten behoeve van hun eigen taakuitvoering.

5 Uitvoering van de meldpuntfunctie: veel gestelde vragen en voorbeelden voor de professional

Dit hoofdstuk bevat enkele praktische handvatten voor medewerkers van het meldpunt. Ze zijn gegoten in de vorm van veel gestelde vragen.

5.1 Veel gestelde vragen en antwoorden

1. **In onze regio is het meldpunt ondergebracht bij de GGD. In andere regio's bij de GGZ. En in andere regio's bij de gemeente. Maakt dit verschil voor de gegevensverwerking?**
   Nee. Voor de gegevensverwerking is in de eerste plaats bepalend welke (wettelijke) taak wordt uitgevoerd. De werkzaamheden van het meldpunt vinden hun wettelijke basis in de taken van het college van B&W in het sociaal domein en die van de burgemeester op het gebied van openbare orde en veiligheid. Als zij de meldpunttaak hebben uitbesteed aan een andere organisatie, voert deze organisatie de taken uit namens hen en gelden voor de gegevensverwerking de regels die vanuit de hun taken daaraan gesteld worden. Dat betekent bijvoorbeeld dat de grondslag voor de gegevensverwerking artikel 6 eerste lid onder e van de AVG is: de gegevensverwerking is noodzakelijk voor de uitvoering van een taak van algemeen belang of de uitoefening van openbaar gezag.

   Praktisch betekent dit onder andere dat het meldpunt gegevens mag verwerken en ook mag verstrekken aan andere partijen als dat noodzakelijk is voor het goed uitvoeren van de meldpunttaak. Bijvoorbeeld als de melding wordt doorgeleid naar het wijkteam, dan mag het meldpunt de gegevens verstrekken die het wijkteam nodig heeft om aan de slag te gaan. Daarbij is het wel belangrijk dat steeds een afweging wordt gemaakt welke gegevens noodzakelijk zijn om te verstrekken.

2. **Ik ben een BIG-professional en ben dus gehouden aan het beroepsgeheim. Wat betekent dat voor mijn werk als meldpuntmedewerker?**
   Voor de professional die BIG geregistreerd is geldt bij werkzaamheden in het meldpunt uitgevoerd worden dat er geen sprake is van een medische behandelovereenkomst, maar dat wel rekening gehouden moet worden met het medisch beroepsgeheim voor zover dat geldt buiten de behandelovereenkomst.

   Dat betekent dat zij gegevens uit het melddossier mogen verstrekken aan anderen, voor zover noodzakelijk is voor de goede uitvoering van de meldpunttaken, bijvoorbeeld om die andere instantie in staat te stellen zorg te gaan verlenen, of toeleiding naar hulp op te starten. Zij hebben daarvoor geen toestemming nodig van de betrokkene. Zij blijven gebonden aan de ethische codes van hun beroepsgroep. Dat betekent bijvoorbeeld dat zij de beginselen van goed hulpverlenerschap hanteren: de gemelde zoveel mogelijk betrekken bij het meldproces; voor zover dat mogelijk is met hem bespreken naar welke instantie het beste kan worden doorgeleid; geen gegevens verstrekken aan een andere partij als dat het belang van de gemelde schaadt. Ten aanzien van het verstrekken van inhoudelijk medische gegevens geldt dat hierbij zo veel mogelijk terughoudendheid moet worden betracht.

3. **Ons meldpunt doet zowel de meldingen niet-acuut als de meldingen Wvggz. Waar moeten we dan rekening mee houden?**
   In veel gemeenten worden het meldpunt Wvggz met het verkennend onderzoek, en het meldpunt niet-acuut in eenzelfde meldpunt ondergebracht. Juridisch gezien zijn dit echter twee verschillende taken. Daarom is het belangrijk om bij de vormgeving van het meldpunt goed uit te werken hoe deze twee zich tot elkaar verhouden. Wanneer een melding behandeld wordt volgens het Wvggz-kader, en wanneer volgens het kader van het meldpunt niet-acuut. Ook is het belangrijk dat de informatiehuishouding voor beide typen meldingen gescheiden is.

Bij een 'gecombineerd meldpunt niet-acuut en Wvggz', kunnen zich de volgende situaties voordoen.

a) Een melding komt binnen en bij de triage is direct duidelijk dat het geen Wvggz-melding betreft. In dat geval volgt de melding een van de overige routes: crisis, Veilig Thuis of niet-acuut.

b) Een melding komt binnen bij het gecombineerde meldpunt en de medewerker komt bij de triage tot de conclusie dat het gaat om een melding in het kader van de Wvggz, dan wordt de melding verder behandeld volgens het kader van de Wvggz. Dat betekent dat het meldpunt namens het college van B&W start met het verkennend onderzoek.

c) Het is bij de triage nog niet duidelijk of het gaat om een melding in het kader van de Wvggz. In dat geval is het advies om de melding te behandelen als een melding niet-acuut.

In de praktijk zal het regelmatig voorkomen dat een melding die aanvankelijk in behandeling is genomen als 'melding niet-acuut' gaandeweg toch beschouwd moet worden als een melding in het kader van de Wvggz. De uitkomst van het meldproces 'niet-acuut' is dan in feite dat de vervolgactie moet worden opgepakt in het kader van de Wvggz. Juridisch gezien wordt de melding dan doorgeleid naar het meldpunt Wvggz, dat dan alsnog een verkennend onderzoek start. Het meldpunt niet-acuut kan dan de noodzakelijke informatie verstrekken aan het meldpunt Wvggz.5 In paragraaf 2.3 wordt nader ingegaan op de samenloop van het meldpunt niet-acuut en het meldpunt Wvggz. Het is goed om bij de samenloop van een meldpunt niet-acuut en een meldpunt Wvggz in het achterhoofd te houden dat het in juridische zin om twee verschillende taken gaat. Dat betekent bijvoorbeeld dat als een melding 'niet-acuut' toch een melding Wvggz blijkt te zijn en je wilt verder in het Wvggz-kader, er juridisch gezien sprake is van een overdracht van het meldpunt niet-acuut aan het meldpunt Wvggz. Zie ook paragraaf 4.2.3 voor de inrichtingsvereisten bij samenloop van meldpunten.

4. **In onze organisatie is het melddossier gescheiden van de andere dossiers zoals bemoeizorg. Waarom is dat?**
   De taak van het meldpunt is juridisch gezien een andere dan bijvoorbeeld een medische behandeling. De eerste taak wordt uitgevoerd namens het college van B&W en de burgemeester, de tweede door een medisch behandelaar meestal op basis van een behandelovereenkomst met betrokkene. Het feit dat beide taken in dezelfde organisatie worden uitgevoerd, wil niet zeggen dat de dossiers samengevoegd kunnen worden. Dan zouden alle meldpuntmedewerkers toegang hebben tot behandelgegevens die niet relevant zijn voor de meldpunttaak. Omgekeerd zouden behandelaars dan toegang krijgen tot meldpuntgegevens ook als die niks met de behandeling te maken hebben. Dat staat op gespannen voet met de privacy van de burger.

5. **Welke informatie mag ik verstrekken aan een instantie die de vervolgacties op gaat pakken?**
   De organisatie die de vervolgacties gaat oppakken mag je de informatie verstrekken die deze nodig heeft voor het invulling geven aan die vervolgacties. Het is wel belangrijk dat je daarin steeds een afweging maakt welke informatie die organisatie nodig heeft. Het zal meestal niet nodig zijn om het hele dossier door te sturen. Maar als er bemoeizorg ingezet moet worden is het waarschijnlijk noodzakelijk om meer informatie door te geven, dan als het wijkteam langs moet gaan omdat er wellicht een Wmo-voorziening nodig is.

Verstrekken van gezondheidsgegevens en strafrechtelijke gegevens

Er zijn ook partijen die geen gegevens over gezondheid of strafrechtelijke gegevens mogen verwerken. Aan deze partijen mag je dergelijke gegevens dus ook niet verstrekken. Bij vraag 9 gaan we nader in op het verstrekken van gegevens over gezondheid en strafrechtelijke gegevens.

6. **Als de GGD van de gemeente opdracht heeft gekregen als meldpunt te fungeren. Heeft de gemeente als opdrachtgever een onbeperkt recht op informatie?**
   Nee. 'De gemeente' bestaat in dit geval niet. Van belang is in welk kader en met welk doel de gemeente gegevens wil opvragen. Ook als het college van B&W optreedt als verwerkingsverantwoordelijke en de GGD namens het college de meldpunttaak uitvoert, kan het college niet vrijelijk over deze gegevens beschikken. Als de gemeente gegevens wil opvragen met betrekking tot een specifiek persoon, zal zij aan moeten geven voor welke taak zij deze gegevens wil gebruiken en welke gegevens noodzakelijk zijn. Het meldpunt zal moeten beoordelen of zij in dat geval gegevens voor dat doel kan verstrekken. Dit uitgangspunt geldt ook binnen de gemeente zelf, als bijvoorbeeld afdelingen onderling gegevens willen uitwisselen. Dit geldt ook ten aanzien van gegevens die een meldpunt Wvggz verzamelt in het kader van een verkennend onderzoek.

   Wel kan het zo zijn dat de gemeente besluit om de meldpunttaak anders te organiseren. Bijvoorbeeld als zij deze zelf uit wil gaan voeren, of aan een andere partij uitbesteden. Als het college van B&W, of de burgemeester en b&w gezamenlijk optreden als verwerkingsverantwoordelijke dan kunnen zij de GGD vragen om de melddossiers over te dragen. Als de uitvoerende organisatie de verantwoordelijke is voor de gegevensverwerking, dan kan dit alleen als dit eerder contractueel is afgesproken. Dit is een van de redenen waarom het van belang is om het melddossier te scheiden van andere taken.

   Tot slot is er nog de mogelijkheid dat 'de gemeente' persoonsgegevens van het meldpunt wil gebruiken om beleidsonderzoek te verrichten. De gemeente zal dan aan moeten geven op basis waarvan zij vindt dat zij de gegevens voor dat doel mag gebruiken. En als de uitvoerende organisatie de verwerkingsverantwoordelijke is, zal zij daar een eigen oordeel over moeten vormen. In alle gevallen is het van belang dat er een duidelijk onderzoeksplan ligt, met waarborgen voor de privacy van de betrokkenen, zoals pseudonimisering of anonimisering. De resultaten van het onderzoek mogen niet tot personen herleidbaar zijn.

7. **Hoe weet ik welke gegevens noodzakelijk zijn om te verwerken of verstrekken?**
   In de praktijk worden veel verschillende redenen aangevoerd om de noodzakelijkheid van het verwerken en verstrekken van persoonsgegevens te rechtvaardigen. Deze zijn niet allemaal even valide. In onderstaande tabel hebben we een aantal op een rij gezet.

Noodzakelijkheidsargumenten	
Valide	**Niet valide**
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)	Je weet maar nooit of we de gegevens op een later tijdstip nodig hebben.
Zonder de gegevens kunnen de werkzaamheden of interventie(s) niet uitgevoerd worden (denk aan personalia of (formele) voorwaarden)	Het is handig om te hebben. De gegevens vergemakkelijken de werkzaamheden of interventie.
Zonder de gegevens loopt het fout (denk aan veiligheid en bescherming)	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 zijn nodig om de werkzaamheden op inhoudelijk goede en verantwoorde 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. Bij een meldpunt gaat het er dan om dat de gegevens noodzakelijk om tot een goede beoordeling van de melding te komen en te kunnen bepalen naar welke instantie deze moet worden doorgeleid.	

Bij de valide argumenten kan de vraag ‘is het noodzakelijk’ bij een meldpunt niet-acuut volmondig met ‘ja’ beantwoord worden voor het specifieke doel. Bij de niet valide argumenten ligt dat anders. Bewaren ‘want je weet maar nooit’ kan geen voldoende reden zijn voor een meldpunt om gegevens langdurig te bewaren. Het bewaren van een melddossier zal altijd een specifiek doel moeten dienen. In paragraaf 4.3.3 wordt hier nader op ingegaan. Voor ‘handig om te hebben’ geldt ook dat dit geen voldoende reden kan zijn om gegevens te verzamelen of langdurig te bewaren. Bij het efficiency argument kan nog sprake zijn van een proportionaliteitsafweging. Als het niet-verstrekken leidt tot onevenredig hoge extra kosten, kan het verwerken van bepaalde gegevens te verantwoorden zijn. Dit zal echter bij een meldpunt niet aan de orde zijn.

8. **Welke gegevens mag ik aan de melder verstrekken om hem te informeren dat de melding is opgepakt?**
   Belangrijkste doel van regelgeving rond gegevensverwerking en privacy is het beschermen van de persoonlijke levenssfeer van mensen. Daarom moet bij het terug melden aan burgers die een melding hebben gedaan altijd terughoudendheid betracht worden, ook al omdat niet op voorhand bekend is hoe de relatie tussen melder en gemelde is.
   Er kan immers sprake zijn van belangen, of conflicten die niet bekend zijn bij het meldpunt. In principe meld je daarom niet meer terug dan de mededeling dat de melding is opgepakt. Vind je het noodzakelijk om meer informatie te verstrekken, stel je zelf dan de vraag: wat is het doel van het verstrekken van meer informatie dan 'de melding is opgepakt'.

   Voor professionals of instanties die melden, geldt in principe dezelfde terughoudendheid, voor zover zij geen directe betrokkenheid hebben bij de gemelde vanuit een eigen taak. Zij zijn dan niet anders dan een burger die meldt.

   Als een meldende professional of instantie wel een betrokkenheid heeft bij de gemelde vanuit een eigen taak, is het bij de terugmelding van belang om af te wegen welke gegevens noodzakelijk zijn om te verstrekken gezien deze betrokkenheid. Daarbij speelt hetzelfde type afweging als bij de informatieverstrekking aan een vervolgorganisatie.

Er zijn twee belangrijke zaken om in de gaten te houden als je meer informatie wilt verstrekken aan de melder:

1. Verzeker je ervan dat de informatie niet voor andere doeleinden wordt gebruikt. Immers instanties kunnen ook meerdere belangen hebben in hun relatie tot de gemelde.
2. Professionals en instanties mogen uitsluitend bijzondere persoonsgegevens zoals gezondheidsgegevens of strafrechtelijke gegevens verwerken voor hun taak, als dat bij wet is geregeld. Als dat niet is geregeld mogen ze bijvoorbeeld geen informatie ontvangen dat een melding wordt opgepakt door de GGZ.

Beide zijn zaken die je als medewerker van het meldpunt moeilijk kunt overzien. Daarom is het belangrijk dat het meldpunt afspraken maakt met organisaties waar veel mee wordt samen gewerkt over het gebruik van informatie die ze van het meldpunt krijgen. Ook is het belangrijk dat de meldpuntorganisatie de medewerkers inzicht geeft in welke organisaties bepaalde gegevens wel of niet mogen ontvangen. Bij vraag 9 gaan we nader in op het verstrekken van gegevens over gezondheid en strafrechtelijke gegevens.

9. **Wanneer moet ik de gemelde informeren dat hij is gemeld?**
   Als je gegevens gaat vastleggen over gemelde, is het nodig om hem zo snel mogelijk daarover te informeren. Het meest natuurlijke moment is om dat te doen als je contact opneemt met gemelde om de situatie te bespreken. Ook is het belangrijk hem op de hoogte te houden van vervolgstappen de je gaat ondernemen en of je bijvoorbeeld gegevens op wilt vragen bij anderen. Er zullen altijd situaties zijn waarin het niet mogelijk blijkt om iemand te informeren, of waarin het duidelijk is dat betrokkene geen flauw idee heeft wat hij met die informatie moet of er niet voor open staat. De AVG kent een uitzonderingsbepaling voor het informeren voor situaties waarin het niet mogelijk blijkt om iemand te informeren, of waarin het duidelijk is dat betrokkene geen flauw idee heeft wat hij met die informatie moet of er niet voor open staat. Als daardoor het doel van de verwerking in dit geval het bieden van hulp, ongedaan wordt gemaakt, kan het informeren achterwege blijven. Leg je afwegingen vast en kijk of je iemand op een later moment alsnog kunt informeren.

10. Verstrekken van strafrechtelijke en of gezondheidsgegevens

Professionals en instanties mogen uitsluitend bijzondere persoonsgegevens zoals gezondheidsgegevens of strafrechtelijke gegevens verwerken voor hun taak, als dat bij wet is geregeld. Als een partij geen gezondheidsgegevens mag verwerken, betekent dat bijvoorbeeld dat deze geen informatie mag ontvangen dat een melding wordt opgepakt door de GGZ.

Als vuistregel kun je hanteren dat je gegevens over gezondheid of strafrechtelijke gegevens uitsluitend verstrekt ten behoeve van zorg, hulpverlening of begeleiding, of in het kader van toeleiding naar voorzieningen in het sociaal domein. Uiteraard uitsluitend als dat noodzakelijk is in het kader van de activiteit die ze gaan ondernemen en ze daarvoor deze gegevens mogen verwerken.

Als medewerker van het meldpunt valt dit moeilijk te overzien. Daarom is het belangrijk dat het meldpunt afspraken maakt met organisaties waar veel mee wordt samen gewerkt over het gebruik van informatie die ze van het meldpunt krijgen. Ook is het belangrijk dat de meldpuntorganisatie de medewerkers inzicht geeft in welke organisaties bepaalde gegevens wel of niet mogen ontvangen.

11. Hoe lang mogen we het melddossier bewaren na afsluiting van de melding?

De wet geeft geen duidelijke bewaartermijnen voor het melddossier. Het melddossier is géén medisch behandeldossier en ook geen 'toeleidingdossier'. De bewaartermijnen die gelden voor die taken zijn hier dus niet van toepassing. Dat betekent dat voor het melddossier de AVG van toepassing is. Deze hanteert een open norm: 'niet langer dan noodzakelijk'. De bewaartermijn moet beperkt zijn en onderbouwd worden. Duidelijk moet zijn met welk doel het dossier wordt bewaard en de gekozen bewaartermijn noodzakelijk is. Elk meldpunt zal hieraan zelf beleidsmatig invulling moeten geven.

In de toelichting bij paragraaf 4.3.3 hebben we stappen aangereikt tot een beleid te komen rond het bewaren van melddossiers.

12. Welke gegevens mogen bewaard worden in het dossier na afsluiting van de melding

Tijdens het behandelen van een melding wordt er informatie verzameld om een goed beeld te krijgen van de situatie en om zicht te krijgen op welke instantie de meest aangewezen organisatie is om de melding verder op te pakken. Je krijgt waarschijnlijk meer informatie dan je uiteindelijk nodig hebt voor het doorgeleiden van de melding, maar vaak kun je dat pas beoordelen als het plaatje helder is.
In die gevallen is het belangrijk om bij het afsluiten van de melding het dossier op te schonen en een beoordeling te maken welke informatie relevant is om te bewaren en welke niet. De wet geeft hier geen harde criteria voor. Daarom is het van belang dat het meldpunt hier beleid op maakt en werkinstructies opstelt.
Bij vraag 6 zijn een aantal valide en niet valide argumenten op een rij gezet om gegevens al dan niet te verwerken of te bewaren.

13. Is het verplicht een convenant en privacy-protocol op te stellen met samenwerkingspartners van het meldpunt?

Het verschaft de medewerkers van het meldpunt en de medewerkers van partijen waar vaak mee samen gewerkt veel duidelijkheid als op bestuurlijk niveau afspraken gemaakt worden over de samenwerking, in het bijzonder over de gegevensverwerking. Een convenant of protocol is niet noodzakelijk als grondslag voor de gegevensverwerking, maar kan wel helpen om duidelijkheid te creëren en de samenwerking in de praktijk soepel te laten verlopen.

14. Hoe moet het meldpunt omgaan met anonieme meldingen?

Werkwijze die het meldpunt nu hanteert

- Uitgangspunt is dat altijd de naam en contactgegevens van de melder worden geregistreerd. Eventueel kan de melder aangeven dat hij anoniem wil blijven voor de gemelde.
- Als de melder anoniem wil blijven en de situatie lijkt schrijnend of urgent, dan neemt het meldpunt de melding toch in behandeling of schakelt een van de hulpdiensten in.
- Als het onduidelijk is wordt de melding als signaal geregistreerd. Als er binnen afzienbare tijd meer meldingen komen wordt alsnog actie ondernomen.

Reflectie
Het meldpunt volgt een genuanceerde benadering.

Voor wat betreft het eerste uitgangspunt
Het uitgangspunt bij de eerste bullet is in lijn met de regeling die ook in de WAMS wordt voorgesteld. Daar wordt ervan uitgegaan dat een melding niet anoniem kan zijn om de volgende redenen:

- Het kan voor een goede behandeling van de melding noodzakelijk zijn om contact op te nemen met de melder.
- We willen voorkomen dat melden misbruikt wordt om mensen dwars te zitten.
  Daarnaast kan het zo zijn dat als iemand vaak 'loze meldingen' doet de persoon zelf een probleem heeft en niet de gemelde(n). Dat is ook een reden om de gegevens van de melder wel te willen registreren.

Voor wat betreft het tweede uitgangspunt
Het tweede uitgangspunt is inhoudelijk verstandig. Als een situatie schrijnend lijkt of urgent, ga je op z'n minst checken of iemand wellicht hulp nodig heeft. Eventueel kun je ook de wijkagent vragen polshoogte te nemen. Als je dit uitgangspunt hanteert, is het wel van belang dat je daarop beleid formuleert en (achteraf) motiveert waarom je actie hebt ondernomen. Zodat je later in evaluatieve zin kunt bezien of het beleid aanpassing behoeft. Vanuit de AVG zijn dan de volgende punten van belang:
Informatieplicht: je informeert de gemelde dat er een melding over hem is gedaan, dat zijn gegevens zijn geregistreerd, hoe lang ze worden bewaard en hoe hij zijn rechten kan uitoefenen;

Noodzakelijkheidsprincipe en bewaren: als blijkt dat het een loze melding is geweest, is er geen rechtmatige grond om de gegevens langer te bewaren. In dat geval vernietig of anonimiseer je de gegevens alsnog.

Bij twijfel: Als er twijfel blijft bestaan zou je de melding aan kunnen houden. Onder de volgende voorwaarden:

- Je motiveert waarom en met welk doel je de melding aanhoudt en dus de gegevens registreert;
- Je koppelt een termijn aan herbeoordeling of de melding nog moet worden aangehouden, opnieuw opgepakt moet worden of kan worden afgesloten.

De termijn voor herbeoordeling kan niet te lang zijn. Je kunt daar beleidsmatig keuzes in maken. Die zul je moeten motiveren. En ook regelmatig evalueren.

- Als bij herbeoordeling blijkt dat het toch een loze melding was, vernietig of anonimiseer je de gegevens alsnog en informeert de betrokkene.

Voor wat betreft het derde uitgangspunt
Het derde uitgangspunt is vanuit de AVG bezien problematisch. Je gaat immers een melding over een persoon registreren zonder dat je de persoon daarvan in kennis stelt. Dat is in strijd met de informatieplicht van de AVG. Maar het past ook niet bij het zorgvuldig handelen van een overheid om meldingen over burgers te registreren zonder dat de burger daar weet van heeft.

De AVG stelt dat je de betrokkene informeert als je gegevens over hem vast legt. Niet informeren kan alleen als daar hele goede redenen voor zijn. Bijvoorbeeld omdat het de situatie erger maakt, of ertoe zou leiden dat er helemaal geen hulp verleend kan worden. Maar die uitzonderingsgronden kunnen hier niet worden ingeroepen, aangezien de gemelde situatie niet als schrijnend en urgent is beoordeeld.

Aanbeveling
Op grond van de AVG is het noodzakelijk om altijd contact op te nemen met de gemelde en hem te informeren over de melding de registratie van gegevens en wat dat betekent.
Vervolgens kun je dezelfde werkwijze hanteren als hier boven bij schrijnende situaties.

5.2 Voorbeelden

In deze paragraaf worden een paar voorbeelden beschreven van praktijksituaties, gevolgd door een korte reflectie vanuit het perspectief van gegevensverwerking

Voorbeeld 1: Bezorgde ouders bellen naar het meldpunt over hun zoon

Ouders bellen meldpunt met zorgen omtrent hun zoon van 30. Daarbij vertellen ze het volgende:
De ouders hebben hun zoon uit huis gezet en hij verblijft nu bij een vriend in een andere gemeente. Ze hebben hem uit huis gezet omdat ze er zelf aan onder door gingen. Ze hadden hem een ultimatum gesteld omtrent zijn gedrag en drugsgebruik. Daar kon hij zich niet aan houden. Vervolgens hebben de ouders hem de deur gewezen.

Op zijn 14de is bij de zoon *pddnos* en *adhd* gediagnosticeerd. Hij is ook angstig en suïcidaal geweest en daarvoor ook bekend geraakt bij de GGZ. Op dit moment gebruikt hij drank en drugs met name ketamine en cannabis. Hij is eerder ook depressief gediagnosticeerd. Ouders denken dat hij dat nu weer is. Hij heeft geen behandelaar meer op dit moment.

De zoon wil absoluut geen hulp. Het lukt hem niet om werk te krijgen of om een uitkering aan te vragen. Hij heeft een sociaal netwerk van vrienden, waar hij nu ook verblijft, maar ouders denken dat dit geen goede plek voor hem is. Ze zien hem achteruitgaan maar hebben er geen grip meer op.

De ouders willen hem best laten weten dat ze met de GGD hebben gebeld.

Hoe heeft het meldpunt de melding opgepakt?

De ouders zijn op het meldpunt uitgenodigd voor een gesprek. Hen is uitgelegd wat de mogelijkheden zijn. Vervolgens is afgesproken dat de ouders melden aan hun zoon dat het meldpunt hem wil ondersteunen. De ouders hebben de contactgegevens van het meldpunt doorgegeven aan de zoon.

Het meldpunt heeft geen gegevens opgevraagd van andere instellingen.

Nadat de zoon contact met het meldpunt heeft opgenomen, heeft het meldpunt met zijn toestemming de ouders laten weten dat ze met de zoon aan de slag gaan. Inhoudelijk heeft het meldpunt niks aan de ouders gezegd.

Met zijn toestemming heeft het meldpunt vervolgens gegevens opgevraagd bij de GGZ en de huisarts. Op basis van die informatie is de zoon uiteindelijk via de huisarts doorgeleid naar verslavingszorg.

Reflectie vanuit het perspectief van gegevensverwerking

Vanuit het perspectief van gegevensverwerking spelen een aantal vragen, waaronder:
- Moet het meldpunt de zoon informeren over de gegevensverwerking?
- Mag het meldpunt de gezondheidsgegevens van de zoon vastleggen die de ouders verstrekken?
- Had het meldpunt ook zonder toestemming van de zoon gegevens op mogen vragen bij zorgverleners?
- Welke gegevens mag het meldpunt vastleggen in het melddossier?

Moet het meldpunt de zoon informeren?
Ja, dat moet binnen een redelijke termijn. Bij voorkeur de eerste keer dat contact wordt gelegd en voordat gegevens worden verstrekt aan anderen. De handelswijze van het meldpunt is prima. Het meldpunt laat de ouders de zoon informeren dat ze hem hebben gemeld bij het meldpunt en vragen de zoon zichzelf te melden. Dat doet hij en op dat moment kan het meldpunt hem informeren.

Als het niet mogelijk was geweest om de zoon te bereiken, had het meldpunt toch gewoon aan de slag gekund. De AVG kent een uitzonderingsbepaling voor het informeren voor situaties waarin het niet mogelijk blijkt om iemand te informeren, of waarin het duidelijk is dat betrokkene geen flauw idee heeft wat hij met die informatie moet of er niet voor open staat. Als daardoor het doel van de verwerking in dit geval het bieden van hulp, ongedaan wordt gemaakt, kan het informeren achterwege blijven. Leg je afwegingen vast en kijk of je iemand op een later moment alsnog kunt informeren.

Mag het meldpunt de gezondheidsgegevens van de zoon vastleggen die de ouders verstrekken?
Ja, dat mag. Het meldpunt mag in het kader van haar meldpunttaak gezondheidsgegevens verwerken. Ze heeft daarvoor niet eerst toestemming nodig van de zoon zelf. Wel moet ze steeds beoordelen welke gegevens noodzakelijk zijn in het kader van de melding.

Had het meldpunt ook zonder toestemming van de zoon gegevens op mogen vragen bij zorgverleners?
Ja, dat had het meldpunt mogen doen, als dat noodzakelijk was geweest om te kunnen bepalen naar wie de melding moet worden doorgeleid. Wel is het uitgangspunt dat het meldpunt eerst probeert contact te zoeken met de betrokkene en zijn medewerking te verkrijgen. Ook zullen zorgverleners terughoudender zijn in het verstrekken van gegevens aan het meldpunt als niet duidelijk is of de betrokkene daar toestemming voor heeft gegeven. Zorgverleners zullen zich bijvoorbeeld beperken tot de mededeling: ‘stuur hem maar door naar mij’, of ‘ik zal contact met hem zoeken’, zonder verder in details te treden.

Welke gegevens mag het meldpunt vastleggen in het melddossier?
Het meldpunt mag de gegevens vastleggen die noodzakelijk zijn om de melding te kunnen beoordelen en door te geleiden naar de juiste instantie. De gegevens in de beschrijving lijken in dat opzicht niet bovenmatig. Daarnaast mag het meldpunt de uitkomst van het meldproces vast leggen en de afspraak die met de instantie waarnaar wordt doorgeleid, is gemaakt.

Voorbeeld 2: Politiemelding over vrouw die uit de trein is gehaald

De politie kreeg een melding dat de NS op het station een dame uit de trein heeft gehaald die geen ID-bewijs kon tonen. Ook wilde zij geen gegevens opgeven en begon zij te gillen op het perron.
De politie is ter plaatse gegaan en heeft een gesprek gevoerd met betrokkene. Mevrouw gaf de politie haar gegevens op en deze bleken juist te zijn.

Betrokkene komt de laatste tijd veel in politiemeldingen voor en zou vaak verward zijn.
Naar de politie ter plaatse reageerde zij normaal en zij kregen niet de indruk dat zij in een psychose zat.
De politie heeft de gegevens overgegeven aan de NS. Betrokkene heeft een bekeuring gekregen en daarna is zij op de trein gezet. De politie heeft een zorgmelding opgemaakt.

Hoe heeft het meldpunt de melding opgepakt?
Melding is eerder bij het meldpunt bekend geweest en destijds overgedragen aan een GGZ-aanbieder. Het meldpunt neemt naar aanleiding van de melding contact op met de GGZ. De GGZ heeft de vrouw nog in behandeling. De GGZ zal contact opnemen met de vrouw en melden dat er een melding is gemaakt door de politie die is doorgezet naar het meldpunt.
Het meldpunt sluit de casus direct weer af.

Reflectie vanuit het perspectief van gegevensverwerking
Vanuit het perspectief van gegevensverwerking spelen een aantal vragen, waaronder:
- Had het meldpunt de gegevens van de eerdere melding nog mogen hebben en had ze die mogen gebruiken?
- Mag het meldpunt direct contact opnemen met de GGZ-aanbieder zonder eerst contact te hebben met de vrouw zelf?
- Had het meldpunt ook breder informatie mogen inwinnen?
- Heeft de GGZ niet te veel gegevens verstrekt aan het meldpunt?

Had het meldpunt de gegevens van de eerdere melding nog mogen hebben en had ze die mogen gebruiken?
Het meldpunt mag het melddossier een beperkte tijd bewaren als dat een duidelijk doel dient dat verband houdt met de meldpunttaken. Belangrijk is wel dat het meldpunt een redelijke bewaartermijn hanteert en duidelijk specificeert met welk doel ze het melddossier bewaart. Uiteraard moet dat doel passen bij de meldpunttaak. Daarbij kun je denken aan: kunnen signaleren als iemand vaker wordt gemeld, omdat dat kan betekenen dat er meer aan de hand is en het noodzakelijk is de meldingen in samenhang te kunnen beoordelen. Een ander doel kan zijn om snel door te kunnen verwijzen naar een instantie waarnaar reeds eerder is doorverwezen. Dat voorkomt dat er onnodig een nieuwe uitvraag plaats hoeft te vinden. Daarmee kan een onnodige inbreuk op de privacy van de burger worden voorkomen.

Het meldpunt had de laatste tijd vaker meldingen over de vrouw gehad. Het is aannemelijk dat ze het melddossier nog mochten hebben en voor dit doel mochten gebruiken.

Er is geen wettelijk vastgestelde bewaartermijn voor het melddossier. De AVG zegt 'niet langer dan noodzakelijk'. Meldpunten zullen hier zelf beleid op moeten ontwikkelen en de bewaartermijn onderbouwen.

Mag het meldpunt direct contact opnemen met de GGZ-aanbieder zonder eerst contact te hebben met de vrouw zelf?
Het meldpunt heeft geen toestemming nodig van de vrouw om contact te zoeken met de GGZ-aanbieder. In de regel heeft het wel de voorkeur om eerst contact te zoeken met betrokkene zelf als dat mogelijk is. In dit geval was de GGZ-aanbieder echter al bekend en kon het meldpunt rechtstreeks contact opnemen.

Had het meldpunt ook breder informatie mogen inwinnen?
Nee, niet zonder meer. In dit geval leverde het contact zoeken met de GGZ-aanbieder de minste inbreuk op de privacy van betrokkene op. Alleen als het contact met de GGZ-aanbieder niks had opgeleverd, of daar aanleiding toe had gegeven, had het meldpunt breder informatie kunnen inwinnen om te bepalen welke andere instantie het beste in actie kon komen.

Heeft de GGZ niet te veel gegevens verstrekt aan het meldpunt?
Nee. Er is slechts gedeeld dat betrokkene nog in behandeling was en dat de GGZ-aanbieder de zaak verder zou oppakken. Daarmee heeft GGZ-aanbieder niet meer informatie verstrekt aan het meldpunt dan nodig was om het meldpunt in staat te stellen om te beoordelen of doorgeleiden naar de GGZ-aanbieder de beste oplossing was.

Voorbeeld 3: Politiemelding

De politie neemt contact op met het meldpunt en vertelt het volgende verhaal:

"Betrokkene heeft sardientjes gestolen bij een supermarkt. De sardientjes hadden een waarde van 84 cent. Meneer vertelde dat hij zijn zoon deze week 250 euro had gegeven. Hij zei dat hij zijn zoon wel vaker geld gaf als hij in geldnood zat. Zijn zoon is ZZP'er en heeft een gezin. Ik vroeg hem of hij vindt dat zijn zoon misbruik maakt van hem. Betrokkene zei dat dit wel zo voelde. Hij zei dat hij het voor zijn kleinkinderen deed. Doordat hij zijn zoon geld gaf, had hij zelf nog maar weinig te besteden.

Op het politiebureau heeft betrokkene zijn ontlasting laten gaan in zijn broek. Betrokkene vertelde geen hulp te krijgen met bijvoorbeeld boodschappen doen of met zijn financiën. Gezien het hele verhaal en met name over het mogelijke misbruik van de 'goedheid' van betrokkene door zoonlief voor de zekerheid deze zorgmelding."

Hoe heeft het meldpunt de melding opgepakt?
Naar aanleiding van de melding is een medewerker van het meldpunt op huisbezoek gegaan om de situatie te bespreken. Client wilde graag hulp voor zijn financiën. Met toestemming aangemeld bij wijkteam.

Reflectie vanuit het perspectief van gegevensverwerking
Vanuit het perspectief van gegevensverwerking spelen een aantal vragen, waaronder:
- Heeft de politie niet te veel informatie verstrekt?
- Is het huisbezoek niet een te grote inbreuk op de privacy van betrokkene gezien de aard van de meldpunttaak?
- Heeft het meldpunt toestemming nodig om iemand aan te melden bij het wijkteam?
- Welke informatie mag het meldpunt aan het wijkteam door geven?

Heeft de politie niet te veel informatie verstrekt?
De beschrijving van de politie is feitelijk. Zij lijken relevant om het meldpunt een eerste beeld te geven van de situatie.

Is het huisbezoek niet een te grote inbreuk op de privacy van betrokkene gezien de aard van de meldpunttaak?
Het meldpunt kan op verschillende manieren de informatie verzamelen die nodig is om een melding goed door te geleiden. Mensen uitnodigen voor gesprek of op bezoek gaan, horen daarbij. De aard van de melding en de mogelijkheden om met iemand in contact te komen, zijn daarbij leidend. In dit geval oordeelde het meldpunt dat het belangrijk was om zelf de situatie van betrokkene te zien en zo beter te kunnen doorverwijzen.

Heeft het meldpunt toestemming nodig om iemand aan te melden bij het wijkteam?
Nee, niet per se. Het hoort bij de taak van het meldpunt om ervoor te zorgen dat de juiste instantie aan de slag gaat naar aanleiding van een melding. Tegelijkertijd: als iemand aan geeft geen hulp te willen, dan moet je goede argumenten hebben om iemand toch door te verwijzen naar een instantie die hulp of zorg komt bieden. Als de man in kwestie had aangegeven het weliswaar moeilijk te vinden, de situatie met zijn zoon, maar verder geen hulp te wensen, dan had het voor de hand gelegen de wil van de betrokkene te respecteren. Alleen als het vermoeden zou zijn dat de man in psychische nood zat, of als er meer meldingen komen van diefstal of overlast, is het voorstelbaar dat of het wijkteam of het bemoeizorgteam wordt ingeschakeld om de betrokkene proberen te verleiden tot het aanvaarden van hulp.

Welke informatie mag het meldpunt aan het wijkteam door geven?
Het meldpunt geeft alleen de gegevens door die het wijkteam nodig heeft om in actie te komen. In dit geval lijkt de context van de diefstal, de problemen met de zoon, en het ‘ongelukje’ met de ontlasting niet relevant voor het wijkteam. Er kan waarschijnlijk volstaan worden met het doorgeven van de contactgegevens van meneer en dat hij graag in aanmerking wil komen voor hulp met zijn financiën. Het is wel van belang om betrokkene te laten weten dat er slechts beperkt gegevens door gegeven worden om zijn privacy te waarborgen en dat het aan hem zelf is om eventueel meer context te geven aan het wijkteam als hij dat nodig vindt.

Colofon

Uitgave van GGD GHOR Nederland.
Dit project is mogelijk gemaakt door

ZonMw

Auteurs

Leon Sonnenschein en **Eric Schreuders** (Net2Legal) met bijdragen van:

Angelique Moonen, meldpunt Signaal Noord Limburg
Jos Mevis, meldpunt midden Limburg
Kim Franx, meldpunt GGD Flevoland
Klaas Verhoeven, meldpunt GGD Gelderland-Zuid
Marijke Schrier, meldpunt GGD Hollands Noorden
Peter Haima, meldpunt GGD Drenthe
Sylvia Commandeur, GGD GHOR Nederland
Trudi Peters, GGD GHOR Nederland

Versie augustus 2020.