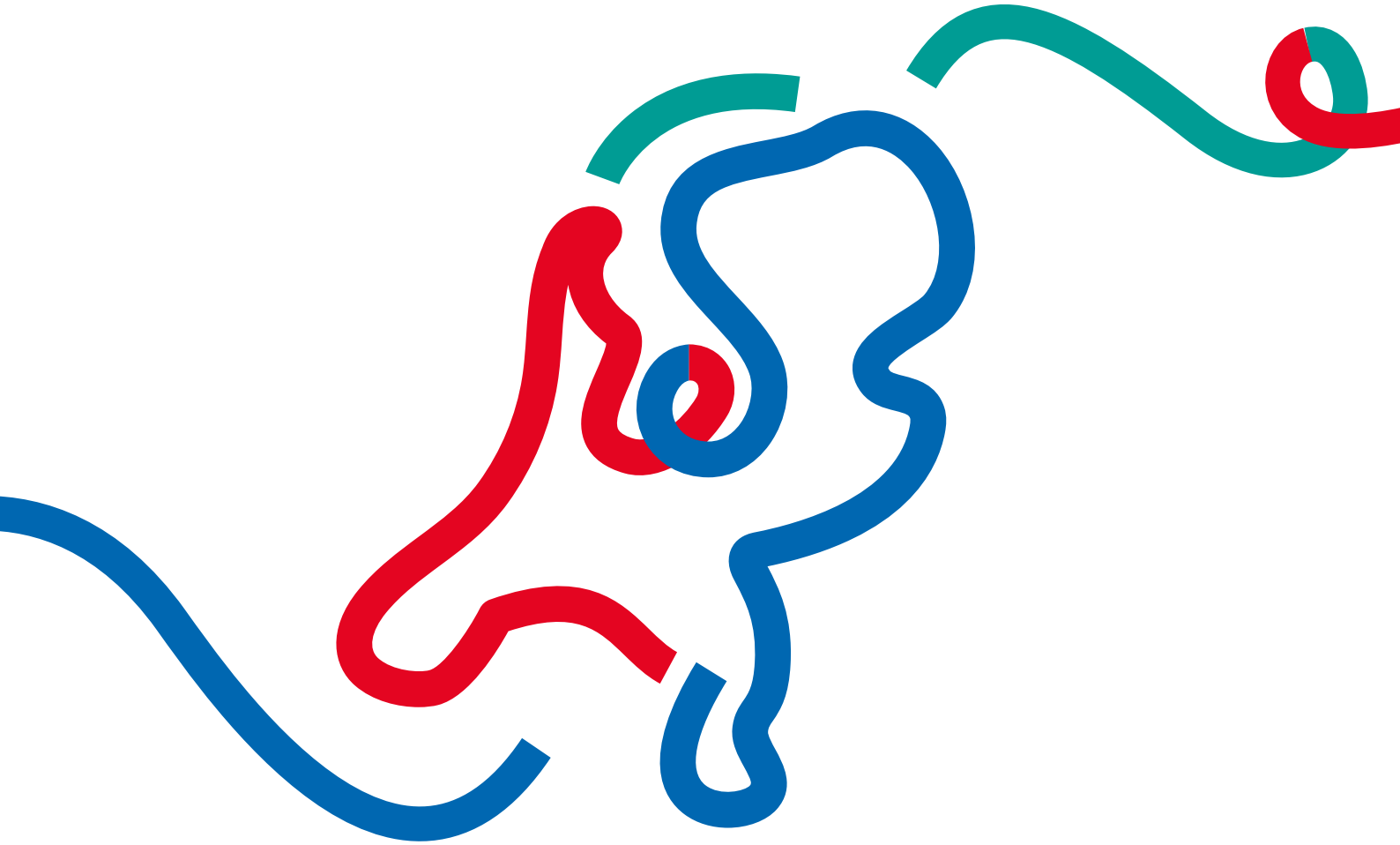
PLATFORM SOCIAAL DOMEIN

Gegevensdeling in sociaal, zorg- en veiligheidsdomein.



VOOR KENNIS,
INZICHT EN ADVIES

Colofon

Auteurs
Léon Sonnenschein en Hans Versteeg
Eindredactie
Mariska Kruijff (TBA Amsterdam)

Voor deze publicatie is met toestemming gebruik gemaakt van concepten en figuren die ontleend zijn aan Eric Schreuders van Net2Legal. Met name het stappenplan in paragraaf 3.5. en de weergave van het generieke werkproces in figuur 3 in paragraaf 4.3.
November 2023

Inhoudsopgave

1. Inleiding

1.1 Doel en doelgroep

Met de meeste burgers in Nederland gaat het gelukkig goed. Zij leiden hun leven op eigen kracht, of met relatief eenvoudige ondersteuning van de overheid en zorgverleners. Een deel van de bevolking lukt dat niet. Door problemen op één of meerdere leefgebieden kunnen deze mensen de grip op hun leven kwijtraken. Zij hebben dan behoefte aan ondersteuning en begeleiding van verschillende instanties om hun bestaan weer op orde te krijgen. Soms is de mix van problemen enorm complex. Denk aan een verslavingsproblematiek die gepaard gaat met strafbare feiten en ernstige overlast. In zo'n situatie is samenwerking tussen partijen uit het sociaal, zorg- en veiligheidsdomein onontbeerlijk.

Om effectief te kunnen samenwerken, moeten partijen gegevens over personen kunnen uitwisselen. Maar: mag dat wel? Bij veel professionals leeft het idee dat er 'vanwege de privacy' niets mogelijk is. Gegevensuitwisseling tussen partijen uit verschillende domeinen is inderdaad complex. Dit komt onder andere door:

- De verschillende doelen van de organisaties. Waar de één huisvesting biedt, levert de ander zorg aan een cliënt en probeert een derde te beoordelen of er sprake is van ontwrichtende criminaliteit.
- Gefragmenteerde regelgeving. Er bestaat helaas geen expliciet juridisch kader voor het uitwisselen van gegevens bij samenwerking tussen de verschillende domeinen.
- Historisch gegroeide fragmentatie van het veld.

De vraag is hoe een gecoördineerde aanpak tussen het sociaal, zorg- en veiligheidsdomein gerealiseerd kan worden.

Voorop staat dat samenwerking en gegevensdeling tussen die domeinen echt **noodzakelijk** is voor de aanpak van de problematiek. Deze handreiking is een hulpmiddel om die noodzaak te onderbouwen. Bovendien wordt beschreven hoe je dat rechtmatig, zorgvuldig en met respect voor de burger kunt doen. Het is voornamelijk een organisatievraagstuk. Want alleen met een goede juridische en organisatorische bedding, kunnen de professionals aan de slag. Het is aan beleidsmakers, juristen en privacy-officers om die bedding vorm te geven.

Deze handreiking is daarom primair geschreven voor deze **doelgroepen**:

1. Beleidsadviseurs van de ketenpartners: zij organiseren de gecoördineerde samenwerking en stellen de inhoud van de samenwerkingsconvenanten op én zien toe op zorgvuldige samenwerking in de praktijk.
2. Juristen en privacy-officers van de ketenpartners: zij beoordelen de juridische grondslag onder de samenwerking en adviseren over de juridische precisering van eventuele convenanten of protocollen.

Deze handreiking kan uiteraard ook interessant zijn voor uitvoerende professionals die benieuwd zijn naar de wijze waarop de samenwerking en gegevensdeling is ingericht, of voor bestuurders of managers die richting geven aan de organisatie en de samenwerking.

De **organisaties** waar het om gaat, zijn bijvoorbeeld: gemeenten, (jeugd) zorginstellingen, sociale wijkteams, woningbouwverenigingen, politie en justitie. In wisselende samenstellingen komen zij elkaar tegen bij verschillende **problematieken**. Denk aan personen met verward gedrag, huiselijk geweld, criminele jeugdgroepen, mensenhandel etc.

(On)mogelijkheden
Samenwerking en gegevensdeling mogelijk maken, staat in deze handreiking centraal. We moeten af van het idee dat er 'vanwege de privacy' niets mag. Dat wil niet zeggen dat gegevensuitwisseling altijd haalbaar of nodig is. Na de juiste toepassing van de hier beschreven aanpak, zal in veel gevallen blijken dat samenwerking en informatie-uitwisseling niet noodzakelijk, niet proportioneel of zelfs onwettig is. Er kan dan geen, of slechts zéér beperkte, informatie tussen organisaties worden uitgewisseld. Die uitkomst biedt dan in ieder geval duidelijkheid voor de uitvoerend professionals. Vervolgens kan er naar andere oplossingen worden gezocht.

1.2 Het belang van privacy

De mogelijkheid om in eigen omgeving helemaal zichzelf te zijn. Zo definieert Van Dale het begrip privacy. Door je ongevraagd met iemands privéleven te bemoeien, schend je die privacy. Mensen kiezen er soms voor om dingen over zichzelf geheim te houden. Als die kennis toch in de openbaarheid komt, kan dat leiden tot schaamte of verlegenheid. De privacywetgeving beschermt mensen daartegen.

Oneigenlijk gebruik van persoonsgegevens brengt nog meer risico's met zich mee. Het kan leiden tot vooroordelen, stigmatisering en/of uitsluiting. Zo kan iemand, op grond van zijn afkomst of overtuigingen, onterecht met een bepaalde groep of bepaald gedrag geassocieerd worden. Ook daartegen biedt de privacywetgeving bescherming. Wanneer hier onzorgvuldig mee om wordt gegaan, heeft dat soms (ernstige) financiële, materiële en psychische gevolgen. Mensen die op onterechte gronden worden verdacht van fraude of een ander strafbaar feit, kunnen te maken krijgen met 'omgekeerde bewijslast'. Ze moeten dan zelf ineens aantonen onschuldig te zijn. De affaires bij de Belastingdienst (de kinderopvangtoeslagenaffaire en het misbruik van het fraudesignaleringssysteem) laten zien tot welke vreselijke situaties dit kan leiden.

Organisaties
Ook voor de betrokken organisaties kan oneigenlijk gebruik van persoonsgegevens grote gevolgen hebben. De Autoriteit Persoonsgegevens legt hoge boetes op voor schending van de AVG (Algemene Verordening Gegevensverwerking). Gedupeerde burgers kunnen op hun beurt een forse schadeclaim indienen. Daarnaast leidt een privacyschending bijna altijd tot een groot verlies aan vertrouwen. Dit raakt niet alleen de betrokken organisatie, maar ook de persoonlijke relatie tussen hulpverlener en cliënt. En een beschadigde vertrouwensrelatie is niet snel hersteld.

Organisaties dienen zeer zorgvuldig met de persoonsgegevens van hun cliënten om te gaan. De manier waarop, is voor een belangrijk deel in de privacywetgeving vastgelegd. Partijen zouden ook vanuit een intrinsieke motivatie zorgvuldig en respectvol met de gegevens van hun cliënten moeten omgaan. Niet alleen omdat de wet dat voorschrijft. Maar vooral ook uit respect voor de grondrechten van de betrokken cliënt en ter bescherming van de (vaak broze) vertrouwensrelatie tussen hulpverlener en cliënt.

1.3 Afbakening en methodiek

Deze handreiking gaat over de manier waarop samenwerking en gegevensdeling in het sociaal, zorg- en veiligheidsdomein mogelijk gemaakt kunnen worden, binnen de voorwaarden die de privacywetgeving daaraan stelt. Het gaat hierbij nadrukkelijk om het oplossen van complexe problematiek waarbij samenwerking tussen verschillende partijen noodzakelijk is.

Verschillende perspectieven

Bij complexe problematiek komen zorg- en veiligheidsvraagstukken samen. Aan de ene kant heeft de betrokken persoon zorg nodig, aan de andere kant vormt hij een bedreiging zijn voor zijn eigen veiligheid of die van anderen. De zorgsector richt zich hoofdzakelijk op het welzijn of de gezondheid van de betrokken persoon. Terwijl de partijen in het veiligheidsdomein ervoor moeten zorgen dat de omgeving veilig blijft, criminaliteit vermindert of dat overlast stopt. Deze verschillende verantwoordelijkheden leiden soms tot verschillende perspectieven op de situatie en kunnen de samenwerking compliceren.

Methode

In deze handreiking staan vier vragen centraal:

1. **Welke vormen van samenwerking zijn er en hoe bepaal je wat de juiste 'tafel' is voor een gecoördineerde samenwerkingsaanpak?**
2. **Hoe zorg je voor een goede juridische basis onder de samenwerking en de gegevensdeling aan en tussen de verschillende tafels?**
3. **Hoe organiseer je de samenwerking aan de verschillende tafels zorgvuldig en zoveel mogelijk eenduidig voor de professionals?**
4. **Hoe zorg je dat de samenwerking met respect voor de betrokken cliënt en met respect voor de andere ketenpartners wordt ingevuld?**

Dit levert een methode op om systematisch tot een goede samenwerking en zorgvuldige gegevensdeling te komen. Deze methode kan vervolgens op diverse vraagstukken worden toegepast. Denk aan de aanpak van criminele jeugdgroepen, de re-integratie van ex-gedetineerden, de ondersteuning van mensen met verward of onbegrepen gedrag etc.

De precieze uitwerking en juridische onderbouwing hangt sterk af van de inhoud van die aanpak, de betrokken ketenpartners en de juridische basis waarop die partijen hun werk doen. Maar de methode om tot de beschrijving van die aanpak te komen is in alle gevallen vergelijkbaar. Ook de wijze waarop de samenwerking zorgvuldig georganiseerd kan worden en de manier waarop het respect voor de betrokken cliënt geborgd kan worden, zijn vergelijkbaar.

Met behulp van deze handreiking ben je in staat te onderbouwen waarom samenwerking en gegevensuitwisseling noodzakelijk zijn voor het oplossen van een maatschappelijk vraagstuk. Bovendien weet je hoe je dat rechtmatig, zorgvuldig en met respect voor de burger kunt organiseren.
De beschreven methodiek is niet vrijblijvend. Laat je een schakel weg, dan is het risico groot dat de gegevensverwerking onzorgvuldig plaatsvindt en daarmee onrechtmatig is.

Waar gaat deze handreiking niet over?
Deze handreiking gaat nadrukkelijk niet over hoe gegevensverwerking binnen de organisaties zelf georganiseerd wordt. De focus ligt bij gegevensverwerking tussen meerdere organisaties en hoe zij privacy en gegevensverwerking goed kunnen borgen in een samenwerkingsverband of overlegtafel. Daarnaast gaat deze handreiking niet specifiek in op de eisen vanuit de AVG, bijvoorbeeld hoe een DPIA kan worden uitgevoerd of hoe je binnen de organisatie een goed privacybeleid kunt ontwikkelen. Over de implementatie van de specifieke AVG-vereisten in (overheids)organisaties is elders volop informatie beschikbaar[1].

1.4 Opbouw van de handreiking

Het uitgangspunt van deze handreiking is dat gegevensverwerking rechtmatig, zorgvuldig en met respect voor de burger moet zijn. Die kernthema's komen veelvuldig terug.

De handreiking richt zich in hoofdstuk 2 op de **maatschappelijke opgaven** in het sociaal, zorg- en veiligheidsdomein. Het belang van een goede onderbouwing van de noodzaak tot samenwerking wordt toegelicht. Waarom moeten verschillende partijen samenwerken om een doel te bereiken? Hoe zien die samenwerkingen er in de praktijk uit? De versnippering van het veld in het sociaal, zorg- en veiligheidsdomein komt ook aan bod. Er bestaan verschillende vormen van samenwerking en gegevensdeling (knooppunten). Hoe bepaal je welk knooppunt voor welk doel het meest geëigend is?

Gegevensdeling of gegevensverwerking?
Formeel spreek je altijd van gegevensverwerking. Deze term wordt ook in de AVG gehanteerd.

Gegevensverwerking is het containerbegrip voor een flink aantal activiteiten ('verwerkingen') m.b.t. persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, raadplegen en verspreiden of verstrekken. Gegevensdeling is dus een specifieke vorm van het verwerken van gegevens.

Hoofdstuk 3 gaat in op de juridische basis om gegevens rechtmatig te mogen delen. Daarnaast wordt relevante wet- en regelgeving besproken en komen enkele belangrijke vereisten uit de AVG aan bod.

Hoofdstuk 4 concentreert zich op de organisatieaspecten rondom het delen van persoonsgegevens in het sociaal, zorg- en veiligheidsdomein. Het beantwoordt de vraag hoe het werkproces ingericht kan worden, zodat de gegevensverwerking ook zorgvuldig is. We bespreken een methode om de samenwerking en de werkprocessen te organiseren en structureren, zodat persoonsgegevens op een zorgvuldige manier worden gedeeld.

Hoofdstuk 5 biedt concrete handvaten hoe de inzichten uit de vorige hoofdstukken in praktijk kunnen worden uitgevoerd, in de vorm van een stappenplan. In dit laatste hoofdstuk worden ook de werkafspraken en vuistregels benoemd die ervoor kunnen zorgen dat gegevensuitwisseling met respect voor de burger plaatsvindt.

[1] Zie bijvoorbeeld www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/ voor een rijke verzameling van handreikingen, werkdocumenten en checklists over de AVG en informatiebeveiliging. De producten zijn ontwikkeld voor gemeenten, maar zijn in het algemeen voor alle overheidsorganisaties goed toepasbaar.

1.5 Achtergrond en verantwoording

De in deze handreiking beschreven aanpak is gebaseerd op het 'Handvat 'Gegevensuitwisseling bij samenwerking rond casuïstiek in het zorg- en veiligheidsdomein'[2]. Die publicatie is ontwikkeld in opdracht van de landelijke Stuurgroep Zorg en Veiligheid en is een gezamenlijk product van diverse (koepels van) organisaties in het zorg- en veiligheidsdomein[3].

Het handvat is ontstaan vanuit een wens bij alle betrokken organisaties om tot een werkbare en praktische aanpak te komen rondom complexe problematiek in het zorg- en veiligheidsdomein. Het uitgangspunt was dat er een juridisch onderbouwde aanpak gewenst was, die samenwerking en gegevensdeling mogelijk maakt.
Een harde randvoorwaarde daarbij was dat de samenwerking en de wijze van gegevensdeling voor alle partijen aanvaardbaar moet zijn en moet passen binnen de wettelijke kaders en de verantwoordelijkheden van de verschillende partijen.

De aanpak is in eerste instantie ontwikkeld voor de zorg- en veiligheidshuizen (ZVH-en). In dit domein is ook de meeste ervaring opgedaan met de aanpak. De afgelopen jaren is de uitwerking in alle ZVH-en geïmplementeerd. Alle ZVH-en gebruiken inmiddels een samenwerkingsconvenant en privacyprotocol die op het handvat zijn gebaseerd. De casus- en procesregisseurs van de ZVH-en zijn ook getraind in de werkwijze.

Maar de aanpak is de afgelopen jaren ook toegepast bij de totstandkoming van handreikingen of werkwijzen in diverse anderen domeinen. Zo zijn er momenteel domein-specifieke handreikingen beschikbaar voor bemoeizorg, kindermishandeling en huiselijk geweld, de aanpak mensenhandel, re-integratie van ex-gedetineerden, de groepsaanpak van criminaliserende jongeren, de aanpak van personen met verward of onbegrepen gedrag, de inrichting van een meldpunt zorg & overlast, de ketenveldnorm levensloopfunctie en de beveiligde intensieve zorg[4].

Leergang

Naast de voorliggende handreiking, is de leergang 'Privacy en gegevensdeling zorg en veiligheid: Zo doe je dat!' ontwikkeld. Deze is ook gebaseerd op het gedachtegoed van het handvat, en gemaakt in opdracht van de landelijke Stuurgroep Zorg en Veiligheid. De leergang moet een bijdrage leveren aan een goede infrastructuur om casuïstiek op te pakken op het snijvlak van zorg en veiligheid, door een goede inrichting van de gegevensverwerking bij samenwerking[5].

[2] Handvat gegevensuitwisseling in het zorg- en veiligheidsdomein, versie 2.3, november 2021, zie www.zorgenveiligheidshuizen.nl/informatie-uitwisselen-in-veiligheidshuizen.
[3] De opstellers van het Handvat zijn: het ministerie van Justitie en Veiligheid, Reclassering Nederland, de Politie, de VNG, de Nederlandse GGZ, het Openbaar Ministerie, de Dienst Justitiële Inrichtingen, het Leger des Heils, Jeugdzorg Nederland, SVG Verslavingsreclassering, de Raad voor de Kinderbescherming, Slachtofferhulp Nederland, Aedes, Halt en de samenwerkende zorg- en veiligheidshuizen.
[4] Voor een volledig overzicht van de diverse domein-specifieke handreikingen zie: www.samenvoorzorgenveiligheid.nl.
[5] Voor meer informatie over de leergang zie www.samenvoorzorgenveiligheid.nl.

2. Maatschappelijke opgave en de AVG

Vraag 1. Welke vormen van samenwerking zijn er en hoe bepaal je wat de juiste ‘tafel’ is voor een gecoördineerde samenwerkingsaanpak?

De Algemene Verordening Gegevensverwerking (AVG) en andere relevante regelgeving bevatten weinig expliciete bepalingen voor de gegevensuitwisseling bij samenwerking in het sociaal, zorg- en veiligheidsdomein. De AVG sluit het echter ook niet uit.

Belangenafweging
De AVG stelt regels voor de bescherming van persoonsgegevens bij het verwerken daarvan (artikel 1). Bij het recht op bescherming moet rekening gehouden worden met de functie van bescherming van persoonsgegevens in de samenleving. Daarbij dient een afweging te worden gemaakt met andere grondrechten (grond 4 bij artikel 1). Denk hierbij aan grondrechten zoals onaantastbaarheid van het lichaam, volksgezondheid en bestaans- en sociale zekerheid. Zo’n belangenafweging is bijvoorbeeld een zwaarwegend maatschappelijk belang ten opzichte van de bescherming van de persoonlijke levenssfeer.

De AVG stelt ook dat overheden hun gegevensverwerking moeten kunnen baseren op een wettelijke taak. Voor andere partijen kunnen andere taken aan de orde zijn. Voor de GGZ bijvoorbeeld: het bieden van geestelijke gezondheidszorg op basis van een overeenkomst. In alle gevallen zal de gegevensuitwisseling mede ten dienste moeten staan van de eigen taakuitoefening.

Onderbouwing samenwerking door de partijen
De inrichting van de gegevensverwerking bij samenwerking begint met de belangenafweging. Hoe zwaar weegt het belang van de maatschappelijke opgave en de noodzaak voor samenwerking, ten opzichte van het belang van de bescherming van de persoonlijke levenssfeer? Waarom is dat maatschappelijk belang zo groot dat het persoonlijk grondrecht moet wijken, zij het zo min mogelijk? Het antwoord op die vraag is een wezenlijk onderdeel van de onderbouwing van de legitimiteit en rechtmatigheid van de gegevensverwerking bij samenwerking.

Onderbouwing deelname aan samenwerking
Een tweede onderdeel van die onderbouwing is dat elke deelnemende organisatie afzonderlijk moet kunnen beargumenteren waarom die partner is in de samenwerking:
- Hoe past deelname aan de samenwerking bij de eigen taak van de organisatie?
- Hoe kan de organisatie vanuit haar taak bijdragen aan de maatschappelijke opgave?
- Hoe draagt de samenwerking bij aan de eigen taak van de organisatie?

Pas als deze vragen zijn beantwoord, heeft het zin om verder na te denken over de juridische aspecten van de gegevensverwerking bij samenwerking (hoofdstuk 3), het organiseren van een zorgvuldige gegevensverwerking (hoofdstuk 4) en handvatten voor de uitvoering (hoofdstuk 5).

Bij ad hoc samenwerking zitten deze afwegingen vaak impliciet verscholen in de inhoud van de problematiek. Bij het inrichten van meer permanente samenwerkingsstructuren zullen deze vragen op bestuurlijk niveau beantwoord moeten worden en een vertaling moeten krijgen naar de praktijk. We lichten dat in de volgende paragrafen toe:

2.1 De noodzaak van samenwerking

Bij samenwerking in het sociaal, zorg- en veiligheidsdomein is er in de regel sprake van een zwaarwegend belang. Maar die moet wel afgewogen worden tegen het belang van de privacyschending. Die afweging en waarom je dan toch gaat samenwerken, vergt per type problematiek een goed onderbouwde afweging. En op uitvoeringsniveau moeten professionals steeds een proportionaliteitsafweging maken.

Samenwerking is geen doel op zich. Samenwerking staat in dienst van een maatschappelijke opgave: het oplossen van ernstige probleemsituaties op het gebied van overlast, criminaliteit of veiligheid van personen. Samenwerking is noodzakelijk, omdat de oorzaak van die probleemsituaties mede gelegen is in sociale en of zorgproblematiek. Om de probleemsituatie te kunnen lossen, is de inzet van verschillende partijen vereist.

Daarbij gaan altijd twee doelen hand in hand:

- Zorgen dat het beter gaat met de persoon of het gezin, en
- Zorgen dat veiligheidsrisico's, ernstige overlast en criminaliteit verminderen. Enerzijds een combinatie van zorg, hulp en ondersteuning, en anderzijds de inzet van handhaving en bestuurs- of strafrechtelijke maatregelen.

Het doel van de samenwerking is nóóit eenzijdig handhaving, opsporing of vervolging. Als dat zo zou zijn, is er geen rol voor de zorg- en sociaal domeinpartners.

Taken, bevoegdheden en verantwoordelijkheden
Problemen hangen met elkaar samen. Interventies en hulpaanbod kunnen elkaar versterken of juist tegenwerken. Uitgangspunt is dat elke partij bijdraagt aan het oplossen van de probleemsituatie vanuit zijn eigen taken, bevoegdheden en verantwoordelijkheden.

Gemeente: Het college van B&W kan aan de oplossing van een probleemsituatie bijdragen. Bijvoorbeeld door passende jeugdhulp of schuldhulpverlening in te zetten, of personen met een psychische kwetsbaarheid of een verslaving beschermd wonen of maatschappelijke opvang bieden. De burgemeester kan besluiten tot een crisisopname in een GGZ-instelling als een situatie onhoudbaar wordt, maar met het achterliggende doel dat zorgverlening op gang komt voor een duurzame oplossing.

Woningcorporaties: Woningcorporaties hebben een taak om ervoor te zorgen dat voldoende betaalbare huurwoningen beschikbaar zijn voor mensen met een laag inkomen. Zij bieden ook woonruimte aan mensen met een psychische kwetsbaarheid, maar hebben tevens de taak om de leefbaarheid en veiligheid in de complexen die zij beheren te bevorderen.

Politie: De politie heeft een taak in de handhaving van de openbare orde, handhaving van de rechtsorde en het bieden van hulpverlening.

GGZ: De GGZ heeft als taak geestelijke gezondheidszorg te verlenen aan mensen met een psychiatrische aandoening. In de meeste gevallen gebeurt dat vrijwillig (op verwijzing door een arts), soms in de vorm van verplichte zorg na een rechterlijke beslissing. Het waar mogelijk voorkomen dat inzet van verplichte zorg nodig is, is daarbij ook een van de achterliggende doelen.

Helderheid aan eigen medewerkers
Ketenpartners moeten binnen hun eigen organisatie helderheid verschaffen aan de medewerkers over:
- De reden van de samenwerking, in relatie tot de eigen taak;
- De juridische basis voor het verwerken van gegevens in de samenwerking;
- Afwegingen die medewerkers moeten maken bij het delen van gegevens.

Voorbeeld

Een gemeente signaleert veel meldingen van overlast door mensen met psychische en psychosociale problematiek. De politie moet vaak in actie komen. Regelmatig lopen problemen zo hoog op dat de woningbouwvereniging geen uitweg ziet en over wil gaan tot huisuitzetting.

Zelfstandig kan de woningcorporatie via een gang naar de rechter dergelijke bewoners wellicht uit huis zetten en de overlast voor de buren verminderen. Daarmee wordt de psychische aandoening van deze bewoners echter niet opgelost en wordt de problematiek (en overlast) elders misschien wel groter. De burgemeester heeft bevoegdheden in het kader van openbare orde en de wet woonoverlast. Maar ook daarmee worden de problemen van deze doelgroep niet echt opgelost.

De gemeente concludeert: negeren van de problematiek is geen optie. Als partijen ieder voor zich blijven opereren, wordt het probleem niet opgelost. Het zal alleen maar leiden tot maatschappelijk ongewenste (ernstige overlast) en onaanvaardbare situaties (dakloosheid van kwetsbare mensen, verergering van de psychische problematiek). Mede op aandringen van de woningcorporatie, neemt de gemeente het initiatief om tot samenwerking te komen tussen woningcorporatie, politie, GGZ en de gemeente (in casu de burgemeester). Uitgangspunt is, dat door samenwerking de problematiek van overlastgevende inwoners mogelijk kan worden aangepakt. Als de juiste hulpverlening van de grond komt, zou de overlast kunnen verminderen en huisuitzettingen minder snel nodig zijn. Ook kunnen andere oplossingen in beeld komen, zoals beschermd wonen, die beter passen bij de specifieke situatie van de betrokkenen. De doelen en taken van de beoogde partners kunnen elkaar zo versterken, in plaats van dat ze elkaar in de weg zitten. Op basis daarvan worden afspraken gemaakt die passen bij ieders taak en rol.

De woningbouwvereniging heeft bijvoorbeeld geen zorgtaak, maar kan wel signalen afgeven richting de zorgpartners bij vermoedens van psychische problematiek. Naar aanleiding van signalen kan de GGZ contact zoeken met een inwoner en passende zorg in gang zetten. De GGZ hoeft de woningcorporatie niet te informeren over wat er met iemand aan de hand is. De GGZ ziet echter wel het belang van afstemming met de corporatie en politie. Bijvoorbeeld als dat leidt tot beter contact tussen hen en de cliënt, waardoor huisuitzetting en negatieve gevolgen voor de gezondheid van een cliënt kunnen worden voorkomen. De GGZ geeft aan binnen de grenzen van het beroepsgeheim steeds te zullen zoeken naar mogelijkheden om die afstemming vorm te geven. Daarbij vraagt ze ook begrip dat dat in sommige gevallen niet zal lukken. De gemeente ontwikkelt met beoogde samenwerkingspartners een aanpak om die er in voorziet dat in individuele gevallen samenwerking tot stand komt.

Bovenstaand voorbeeld laat zien hoe partners, door dicht bij hun eigen taak te blijven, toch samenwerking kunnen zoeken. Het plan om eventueel samen te gaan werken vormt een belangrijke eerste stap voor de juridische onderbouwing van de noodzakelijke gegevensuitwisseling. Die begint namelijk bij het vaststellen van de maatschappelijke opgave, het belang en de noodzaak voor samenwerking, en hoe deze samenhangt met de taken van de individuele partners.

2.2 Samenwerking in de praktijk

In de praktijk krijgt samenwerking op het snijvlak van het sociaal, zorg- en veiligheidsdomein vorm rond het behandelen van casuïstiek. Overlegstructuren ontstaan vaak van onderop en gedreven door de inhoud van de problematiek. Afwegingen over de ernst van de problematiek en de noodzaak voor samenwerking vinden aanvankelijk ad hoc en impliciet plaats.

Voorbeeld

Een schuldhulpverlener merkt dat het niet uitmaakt welke afspraken hij met zijn cliënt maakt. De cliënt komt de afspraken niet na en de schulden blijven oplopen. De schuldhulpverlener weet dat zijn cliënt een alcoholverslaving heeft en hij vermoedt dat de cliënt een lichte verstandelijke beperking heeft. Er is ook steeds vaker sprake van agressie richting omwonenden. De wijkagent komt regelmatig tussenbeide.

Deze conflicten lijken de gemoedstoestand van de cliënt geen goed te doen. Er lijkt sprake van een vicieuze cirkel. De schuldhulpverlener concludeert dat de schulden nooit opgelost gaan worden als niet eerst óók de verslaving en de LVB-problematiek worden geadresseerd. De verwachting is dat dan ook de agressie zal verminderen. De schuldhulpverlener zoekt daarom contact met de verslavingszorg en het maatschappelijk werk, met als mededeling: “ik heb jullie hulp nodig om mijn taak – het oplossen van de problematische schulden – goed te kunnen uitvoeren.”

Voor privacy-juristen is het in dergelijke situaties lastig om de situatie goed te duiden. Er is immers geen sprake van een ‘rechttoe rechtaan’ taakuitvoering en er zijn geen bepalingen die de samenwerking expliciet ondersteunen. Maar vanuit AVG-perspectief wordt wel een aantal belangrijke afwegingen gemaakt. In de ogen van de schuldhulpverlener is er sprake van een ernstige probleemsituatie. Er is sprake van samenhang in problematiek. En als hij geen samenwerking zoekt, lost hij de schulden niet op. In dat geval bereikt hij dus niet het doel van zijn taak. Zijn conclusie: samenwerking met verslavingszorg en maatschappelijk werk is noodzakelijk voor de goede uitoefening van mijn taak.

Het betreft vrijwillige hulpverlening, geen sanctionering of gedwongen hulp. Voor de schuldhulpverlener is er dus ook niet direct aanleiding om te veronderstellen dat hij de belangen van de cliënt onevenredig schaadt met het zoeken van samenwerking.
In ad hoc situaties zie je dat professionals vaak impliciet goede afwegingen maken, die ook te verantwoorden zijn vanuit de AVG. Maar als het overleg structureel wordt, volstaat dit impliciete karakter van de afwegingen niet meer. Dan slaat ook de twijfel toe bij professionals: mogen wij overleggen? Waar moeten wij ons precies aan houden als het gaat om gegevensverwerking? De AVG stelt ook dat de deelnemende partijen moeten kunnen aantonen waarom ze vinden dat ze gegevens mogen uitwisselen in de samenwerking. Dan ontstaat de noodzaak om afspraken te maken op beleids- en bestuurlijk niveau. Ook moet aan de professionals duidelijk worden gemaakt op basis waarvan ze kunnen samenwerken en gegevens mogen uitwisselen, en waarover ze op casuïstiekniveau afwegingen moeten maken.

De afwegingen over de noodzaak van de samenwerking moeten expliciet gemaakt worden en vertaald worden naar handvatten voor de praktijk. Onder andere door een duidelijke doelformulering en criteria die richting geven aan vragen als:

- Voor welk type casuïstiek is deze overlegtafel bedoeld?
- Wanneer is er voldoende aanleiding om een casus in behandeling te nemen en hebben we daar criteria voor?
- Wat is het gezamenlijke doel en hoe verhoudt zich dat tot de taken en doelen van de afzonderlijke partners?

2.3 Knooppunten: meldpunten en overlegtafels

De samenwerking, zoals in deze publicatie beschreven, verloopt bijna altijd via 'knooppunten'. Een knooppunt is een plek waar partijen uit de verschillende domeinen samenkomen en persoonsgegevens met elkaar uitwisselen. Altijd in het kader van een vooraf expliciet gespecifieerd doel.

We onderscheiden twee typen knooppunten: meldpunten en overlegtafels.

- Een meldpunt heeft als kerntaak om meldingen, bijvoorbeeld over woonoverlast of huiselijk geweld, in ontvangst te nemen, te onderzoeken en door te geleiden naar de meest aangewezen instantie om in actie te komen.
- Een overlegtafel is de plek waar organisaties elkaar ontmoeten om de samenwerking te organiseren rond individuele casussen.

De meeste meldpunten zijn georganiseerd om één specifieke (wettelijke) taak uit te voeren. De meldpunten niet-acute zorg, het meldpunt Veilig Thuis, of een meldpunt Wvggz (verplichte zorg vanwege een psychische aandoening) zijn hier voorbeelden van.

De meeste overlegtafels zijn georganiseerd rond een bepaalde maatschappelijke opgave, doelgroep of situatie. Het gaat hierbij om domein-overstijgende problematiek, zoals een tafel voor notoire overlastgevers, een tafel voor woonoverlast, of het zorg- en veiligheidshuis. Het doel van de overlegtafel is om de samenwerking rond concrete casussen te organiseren. Met vaste stappen: beoordelen of samenwerking in een specifiek geval nodig is, welke partijen daarbij nodig zijn, en een plan van aanpak om tot verbetering van de situatie te komen.

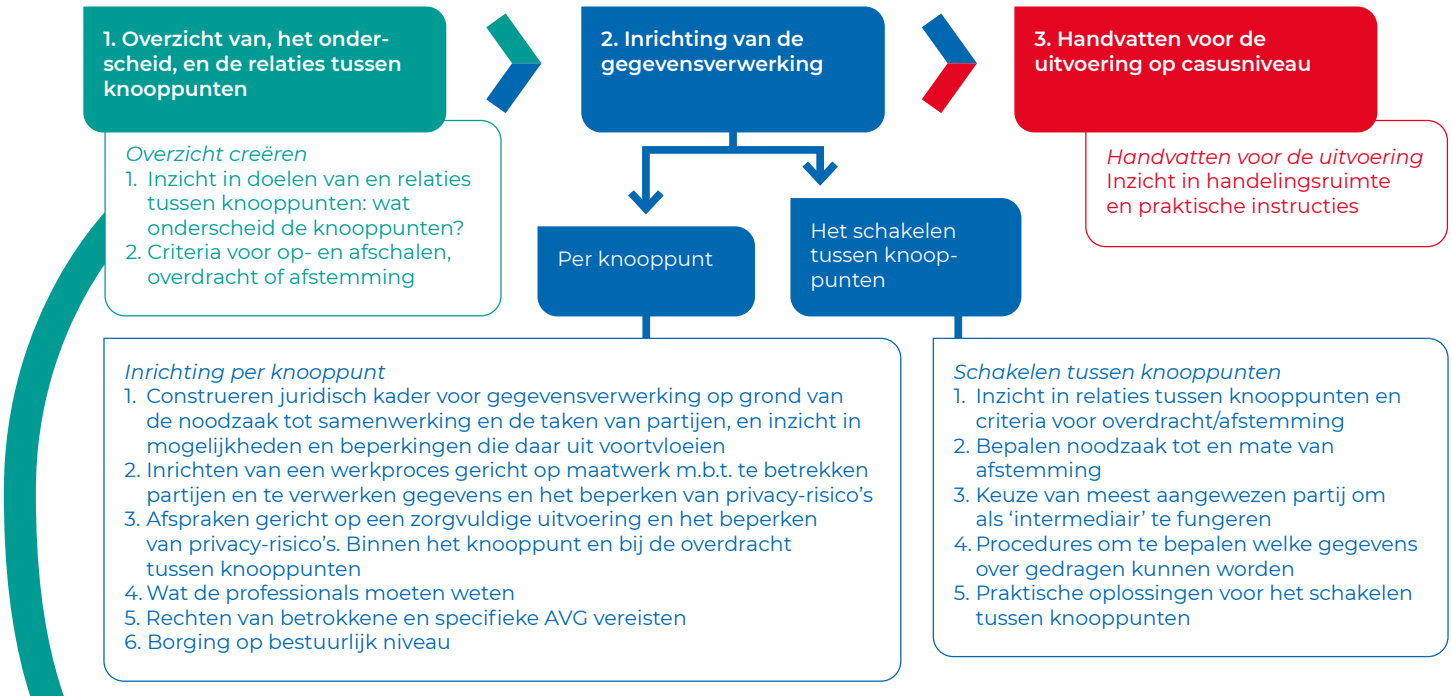
Figuur 1. Voorbeeld van een -niet limitatief- overzicht van knooppunten

De tendens om voor elk nieuw vraagstuk en elke nieuwe doelgroep een nieuw knooppunt op te richten, leidt in veel regio's tot een gefragmenteerd en complex veld van knooppunten (zie figuur 1). Dit leidt er ook toe dat de gegevensverwerking voor de meeste knooppunten verschillend wordt ingericht. Terwijl veel zaken, vanuit een gegevensverwerkingsperspectief, vergelijkbaar ingericht kunnen of zelfs moeten worden. Er zijn verschillende spelregels en wetmatigheden in het proces die voor elk knooppunt opgaan. Daardoor komen ook mogelijkheden in beeld om tot een meer generieke infrastructuur te komen voor samenwerking bij casuïstiek in het sociaal, zorg- en veiligheidsdomein. In het vervolg van deze handreiking beschrijven we de samenwerking in het sociaal, zorg- en veiligheidsdomein vanuit het oogpunt van één knooppunt, omdat dit de plaats is waar de gegevensuitwisseling rond specifieke casussen plaatsvindt.

Een generieke benadering voor de verschillende knooppunten creëert eenduidigheid voor professionals met betrekking tot het delen van persoonsgegevens. Zij hoeven zich dan niet het hoofd te breken over de juridische aspecten van gegevensverwerking, en de verschillende spelregels per knooppunt. In plaats daarvan kunnen ze zich concentreren op de inhoudelijke noodzaak en de generieke spelregels voor zorgvuldigheid.

2.4 Inrichten gegevensverwerking

Het landelijk beleid is erop gericht dat elke regio een goede infrastructuur van meldpunten, overlegtafels en voorzieningen heeft om casuïstiek op het snijvlak van het sociaal, zorg- en veiligheidsdomein op te pakken. Zodat niemand tussen wal en schip valt. Al die knooppunten dienen hun gegevensverwerking ingericht te hebben op een manier die rechtmatig en zorgvuldig is, en met respect voor de inwoner wordt uitgevoerd. Uiteraard moet het ook voor professionals uitvoerbaar en behapbaar zijn. Een gestructureerde benadering (zie figuur hieronder) helpt om overzicht te creëren en stap voor stap de inrichting van de gegevensverwerking op orde te krijgen.



Figuur 2. Schema Inrichting van de gegevensverwerking

Deze benadering bestaat uit de volgende elementen:

1. **Een overzicht van knooppunten en de onderlinge relaties.** Dit geeft beleidsmatig inzicht in de bestaande infrastructuur. Het overzicht is ook van belang om te kunnen beoordelen in welk knooppunt een casus thuishoort, inzicht te krijgen in de logische routes voor een casus – bijvoorbeeld via een meldpunt naar een overlegtafel – en om inzicht te krijgen waar overdracht tussen knooppunten plaatsvindt. Daar waar overdracht tussen knooppunten plaatsvindt, speelt altijd de vraag: welke informatie mogen knooppunten aan elkaar overdragen en hoe doen ze dat op een zorgvuldige manier?

2. **Inrichten van de gegevensverwerking.** In de eerste plaats gaat het hierbij om de inrichting van de gegevensverwerking binnen een knooppunt. Pas als deze goed is ingericht, kunnen uitspraken gedaan worden over de mogelijkheden om gegevens uit te wisselen met een ander knooppunt. Voorwaarde is wel dat de gegevensverwerking van het andere knooppunt ook goed is ingericht.

3. **Handvatten voor de uitvoering.** Op basis van de inrichting van een specifiek knooppunt en inzicht in de relaties met andere relevante knooppunten, kunnen praktische handvatten voor de professionals opgesteld worden. Deze handvatten hebben betrekking op hun handelingsruimte om gegevens te kunnen verwerken en uitwisselen binnen een knooppunt en bij het overdragen van een casus naar een ander knooppunt.

De inrichting van de gegevensverwerking leidt uiteindelijk tot afspraken op bestuurlijk niveau tussen de samenwerkende organisaties. In de regel hebben gemeenten de bestuurlijke verantwoordelijkheid om het speelveld van knooppunten in het sociaal domein en het zorg- en veiligheidsdomein in hun regio te organiseren. Vaak wordt de uitvoering van een specifiek knooppunt bij een organisatie belegd.

In deze aanpak wordt het hart van een goede inrichting van de gegevensverwerking gevormd door een goede inrichting van alle afzonderlijke knooppunten. Dat is natuurlijk een enorme opgave. Maar wie een paar knooppunten heeft ingericht aan de hand van de stappen in deze publicatie, zal zien dat veel elementen kunnen worden hergebruikt. Want bij veel tafels is er een overlap in de partijen en de (wettelijke) taken waarvoor ze participeren in een knooppunt. Ook zal blijken dat voor knooppunten steeds een vergelijkbaar proces nodig is om tot een zorgvuldige op maatwerk gerichte gegevensverwerking te komen. Dit geldt zowel voor de meldpunten als voor de overlegtafels.

2.5 Ordening knooppunten

Het is mogelijk om ordening aan te brengen in het veld van knooppunten aan de hand van een aantal typeringen.

Functie

De eerste typering is de functie van het knooppunt. Daaraan zijn ook het doel en de aard van de gegevensverwerking verbonden. Overlegtafels en meldpunten verschillen op dit punt van elkaar.

Bij een overlegtafel is het doel gezamenlijke duiding van de problematiek, om tot een plan van aanpak te komen waarin de activiteiten van verschillende partijen op elkaar zijn afgestemd. De aard van de gegevensverwerking is gezamenlijk en multilateraal. Bij een meldpunt is het in principe één partij (het meldpunt) die informatie verzamelt, met als doel om een andere partij in staat te stellen zijn taak uit te gaan voeren. De gegevensuitwisseling is vooral bilateraal. Partijen informeren het meldpunt en het meldpunt verstrekt vervolgens de noodzakelijke gegevens aan de partij waarheen wordt doorgeleid.

Bij een meldpunt kán wel sprake zijn van multilaterale gegevensuitwisseling. Zo kan Veilig Thuis een overleg beleggen in het kader van haar onderzoek. Maar bij meldpunten staat het overleg primair ten dienste van de taak om een situatie te beoordelen en een vervolgactie uit te zetten.

Wettelijke regeling of taak

De tweede typering is of het knooppunt een expliciete wettelijke regeling kent of dat er een wettelijke taak van één specifieke partij aan ten grondslag ligt. Voorbeelden van wettelijk geregelde knooppunten zijn: Veilig Thuis, het meldpunt Wvggz, het Trajectberaad Jeugd en het overleg tussen Penitentiaire Instelling, gemeente en Reclassering in het kader van de re-integratie van ex-gedetineerden.

Voorbeelden van knooppunten die toe te rekenen zijn aan de taak van een partij zijn: de Jeugdbeschermingstafel of het ZSM-overleg ten behoeve van een afdoeningsbeslissing door het OM bij een aangehouden verdachte. Knooppunten waarvoor dat minder evident is, zijn onder andere een jeugdgroepenoverleg, een lokale persoonsgerichte aanpak, of een meldpunt mensenhandel.

Als een knooppunt expliciet wettelijk geregeld is, volgt de grondslag voor de gegevensverwerking uit de wettelijke regeling. Vaak is dan ook geregeld dat partijen gegevens mogen verstrekken aan, of uitwisselen in het kader van het knooppunt. Dat maakt het AVG-vraagstuk een stuk eenvoudiger. Dit gaat overigens niet altijd op. Zo heeft het college van B&W volgens de Wvggz de wettelijke taak om een meldpunt te hebben en een verkennend onderzoek te doen. Tegelijkertijd ontbreekt het aan een goede regeling voor het verstrekken van gegevens door partijen ten behoeve van het verkennend onderzoek. Sterker nog, sommige geheimhoudingsbepalingen in de Wvggz staan dit zelfs in de weg. Helaas bemoeilijkt dit het verrichten van een goed verkennend onderzoek.

Als een knooppunt toe te rekenen is aan de taak van één specifieke partij, dan speelt vooral de vraag of andere partijen mogen verstrekken ten behoeve van die taak. Vaak zijn er ook dan voldoende wettelijke bepalingen te vinden die dat mogelijk maken. Zo mogen alle partijen die deelnemen aan het ZSM-overleg, verstrekken aan het OM ten behoeve van een afdoeningsbeslissing. Als een knooppunt minder expliciet geregeld is, of minder expliciet is toe te rekenen aan de taak van één specifieke partij, is het essentieel dat de betrokken partijen het belang en de noodzaak stevig kunnen onderbouwen.

Samenstelling deelnemende partijen
Een derde typering is de samenstelling van de deelnemende partijen. Is het knooppunt gericht op een specifiek thema met een (beperkt) aantal vaste deelnemers, of is er sprake van een knooppunt rondom een problematiek die zo divers is, dat de te betrekken partijen per casus sterk kunnen verschillen?

Een voorbeeld van het eerstgenoemde knooppunt is een jeugdgroepenoverleg waarin burgemeester, politie, OM en jongerenwerk overleggen over de aanpak van problematische jeugdgroepen. Ieders deelname is goed te onderbouwen vanuit ieders eigen taak. De stappen om tot een goede juridische basis te komen, zijn dan relatief eenvoudig.

Een voorbeeld van het tweede knooppunt is een lokale persoonsgerichte aanpak (PGA) of het zorg- en veiligheidshuis. Gezien de diversiteit van de casuïstiek, zijn dan veel partijen bij de samenwerking aangesloten. Maar in een concrete casus hoeft slechts een deel van die aangesloten partijen betrokken te worden. Voor de juridische analyse van de gegevensverwerking moet dan gekeken worden naar de taken van veel verschillende partijen en de mogelijkheden om met elkaar gegevens uit te wisselen. Dat maakt het complex. Daarnaast wordt de rechtmatigheid van de gegevensverwerking sterk bepaald door de vraag of in elke specifieke casus alleen de juiste partners betrokken worden. Dit om verspreiding van gevoelige persoonsgegevens onder partijen die niets met de casus te maken hebben, te voorkomen.

De ordening geeft inzicht in de complexiteit van het gegevensverwerkingsvraagstuk en kan behulpzaam zijn bij het vinden van richting voor de juridische analyse van hoofdstuk 3.

2.6 Regionaal overzicht van knooppunten

Een overzicht van knooppunten en de relaties tussen knooppunten op regionaal niveau is om meerdere redenen zinvol.
Voor bestuurders kan het overzicht antwoord geven op de volgende vragen:

- Is de bestaande infrastructuur dekkend voor de diversiteit aan vraagstukken op het gebied van sociaal, zorg- en veiligheid in onze regio?
- Hebben we voor elk nieuw vraagstuk een nieuw knooppunt nodig, of kunnen sommige nieuwe vraagstukken opgepakt worden door een reeds bestaand knooppunt (al dan niet met wat aanpassingen)?
- Is het mogelijk de infrastructuur te stroomlijnen en te vereenvoudigen door knooppunten samen te voegen?
- Kunnen wij onze bestuurlijke verantwoordelijkheid waarmaken als het gaat om het onderbouwen van de rechtmatigheid van de samenwerking en de gegevensverwerking, en het voorkomen van onbedoelde negatieve effecten voor de burger?

Voor uitvoerend professionals kan het overzicht antwoord geven op vragen als:

- Hoe verhoudt het knooppunt waaraan onze organisatie deelneemt, zich tot andere 'aanpalende' knooppunten? Voor een meldpunt Zorg en Overlast is het bijvoorbeeld van belang om te weten naar welke overlegtafel(s) een cliënt eventueel kan worden doorverwezen.
- Welke overlegtafel is het meest geschikt om een bepaalde casus op te pakken?
- Bij welke tafels kan deze casus nog meer terechtgekomen zijn en hoe voorkomen we dat we langs elkaar heen werken?
- Is op bestuurlijk niveau invulling gegeven aan de verantwoordelijkheid om de rechtmatigheid van de samenwerking en de gegevensverwerking te onderbouwen, en onbedoelde negatieve effecten voor de burger te voorkomen?

Stappenplan overzicht knooppunten

Stap 1: Bepaal het doel van de inventarisatie

De ervaring leert dat wie domweg begint met het inventariseren van knooppunten, al snel vastloopt in de veelheid aan knooppunten en hun abstractieniveau.

Een reden om een inventarisatie te maken, kan bijvoorbeeld zijn dat de gemeentelijke veiligheidsdirectie of de burgemeester wil weten of er in de regio een dekkend netwerk is van knooppunten voor samenwerking op zorg- en veiligheidsvraagstukken. Een dergelijke inventarisatie past bij de coördinerende taak die de (centrum)gemeente vaak heeft in een regio. Bijvoorbeeld om tot een sluitende aanpak rondom verward gedrag te komen, of om de openbare orde en veiligheidstaak van de burgemeester goed te kunnen uitvoeren.

Een ander voorbeeld is een GGZ-organisatie die een overzicht wil maken van overlegtafels waar zij mogelijk bij betrokken kan worden. Dit om, op basis van de criteria van die tafels, te beoordelen of de GGZ-organisatie daadwerkelijk bij de samenwerking betrokken wil zijn. Het zou bijvoorbeeld kunnen dat het vanuit haar specifieke (medische) rol in de hulpverlening niet passend is.

Een derde voorbeeld is een meldpunt zorg- en overlast dat inzichtelijk wil maken naar welke overlegtafels het meldpunt mogelijk kan doorverwijzen.

Bovenstaande voorbeelden zullen alle drie leiden tot andere inventarisaties. In het eerste voorbeeld (overzicht vanuit de gemeente) zullen de beschrijvingen vooral globaal zijn, maar zullen wel veel knooppunten in beeld komen. Het tweede voorbeeld (GGZ-organisatie) zal alleen betrekking hebben op knooppunten waar psychische problematiek onderdeel is van de casuïstiek. Het zou een analyse kunnen bevatten van het doel van deelname van de GGZ in de samenwerking, of de wijze waarop voldaan wordt aan de eisen van het medisch beroepsgeheim. Het derde voorbeeld (doorverwijzing vanuit het meldpunt zorg- en overlast) zal waarschijnlijk focussen op de criteria voor aanmelding bij de aanpalende overlegtafels.

Stap 2: Beschrijf de maatschappelijke opgave van de knooppunten

Mogelijke vragen per knooppunt:

- Welk type problematiek pakt dit knooppunt op?
- Welke criteria hanteert het knooppunt om een casus op te pakken?
- Waarom is samenwerking noodzakelijk om dit type problematiek op te pakken en welke partijen zijn daarvoor nodig?
- Is duidelijk op grond van welke taak elke partij nodig is in de samenwerking?
- Rechtvaardigen de aard van de problematiek en het doel van de samenwerking de inbreuk die daarmee per definitie gemaakt wordt op de persoonlijke levenssfeer van de burger?
- Is er een analyse gemaakt van de risico's voor onbedoelde en onterechte negatieve effecten voor de burger, en worden deze risico's door de werkwijze beperkt?
- Welke andere knooppunten zijn relevant voor dit knooppunt? Bijvoorbeeld omdat ze vergelijkbare casuïstiek behandelen en er een grote kans is op overlap in problematiek, of in verband met overdracht van casuïstiek.
- Voldoet de gegevensverwerking van dit knooppunt aan alle eisen?

Stap 3: Verifieer het gemaakte overzicht

Knooppunten kennen een diverse ontstaansgeschiedenis. De mate waarin de inrichting van de gegevensverwerking gestructureerd heeft plaats gevonden, verschilt. Vaak is er wel impliciet al nagedacht over een aantal van de vragen uit stap 2. Verifieer daarom altijd bij de uitvoerend professionals en de betrokken organisaties of de beschrijving klopt. Uiteraard kan de organisatie ook betrokken worden bij het opstellen van de beschrijving.

3. Het juridisch kader

Hoe zorg je voor een goede juridische basis onder de samenwerking en de gegevensdeling aan en tussen de verschillende tafels?

Regelgeving
Het juridisch kader draait om de relatie tussen de cliënt en de deelnemende partijen, en de wet- en regelgeving die van toepassing is bij de gegevensverwerking. Eerst dient dit inzichtelijk te worden gemaakt. Vervolgens kunnen de AVG-grondslag voor de verwerkingen en eventueel de grondslagen op grond van de Wet politiegegevens (WPG) of de Wet justitiële en strafvorderlijke gegevens (WJSG) worden bepaald. Daarnaast is er aandacht voor de mogelijkheden om bijzondere en strafrechtelijke gegevens te verwerken. Tot slot kan inzicht gekregen worden in specifieke mogelijkheden, belemmeringen of randvoorwaarden die van belang zijn voor de gegevensuitwisseling tussen partners. Denk daarbij bijvoorbeeld aan geheimhoudingsbepalingen of verstrekkingsbevoegdheden.

Zorgvuldigheidsbeginselen
Naast dit juridisch kader op basis van regelgeving, is het van belang dat de deelnemende partijen in het knooppunt invulling geven aan de zorgvuldigheids-beginselen van de AVG. In paragraaf 3.2 gaan we hier gaan we nader op in.

Alleen als aan beide elementen wordt voldaan, is gegevensverwerking ook daadwerkelijk rechtmatig. Als de grondslag in orde is, maar de werkwijze voldoet niet aan de zorgvuldigheidsbeginselen, is de gegevensverwerking alsnog onrechtmatig. Onzorgvuldig is altijd onrechtmatig.

3.1 Wetten en regelingen

Er is niet één wet die volledig beschrijft wat, met het oog op de bescherming van de privacy van betrokkenen, wel of niet is toegestaan. Het juridisch kader voor de privacybescherming (‘de privacyregels’) is een hiërarchie van verschillende wetten en regelingen:

1. Grondwet en EVRM
Op het hoogste wetsniveau regelen de Grondwet (artikel 10) en het Europees Verdrag tot bescherming van de rechten van de mens (EVRM, artikel 8) dat iedereen recht heeft op ‘privacy’. Dit behelst ‘het recht op eerbiediging van de persoonlijke levenssfeer’ (Grondwet) en het ‘recht op respect voor het privéleven’ (EVRM). Privacy is daarmee een grondrecht. Dat grondrecht is echter niet absoluut; het moet worden afgewogen ten opzichte van andere grondrechten. Daarnaast zijn ‘beperkingen van het grondrecht’ mogelijk. Zo is een inbreuk op de privacy mogelijk als dat bijvoorbeeld nodig is voor de nationale veiligheid, de openbare orde, maar bijvoorbeeld ook voor de bescherming van de gezondheid of het bevorderen van het ‘het economisch welzijn’ van het land.

Zowel de Grondwet als het EVRM stellen echter heel nadrukkelijk dat een inbreuk op de privacy, of een beperking van het grondrecht, alléén mag als dat bij wet is geregeld. Overigens stelt de Grondwet ook dat de wettelijke bescherming van de privacy gaat over het gebruik van persoonsgegevens (artikel 10, lid 2). Daarmee betekent het (abstracte) begrip 'privacybescherming' in de praktijk vooral de 'bescherming van persoonsgegevens'.

2. De AVG en UAVG

De Algemene Verordening Gegevensbescherming (AVG) geeft op Europees niveau de uitwerking van de eis in het EVRM om de privacybescherming bij wet nader te regelen. De AVG stelt een aantal algemene kaders en zorgvuldigheidseisen die voor alle verwerkingen van persoonsgegevens gelden. Een belangrijk onderdeel daarvan zijn de rechten van de betrokken persoon, zoals inzagerecht of het recht om niet in een verwerking opgenomen te worden. Daarnaast vereist de AVG de inzet van een aantal praktische tools om de privacybescherming goed te kunnen organiseren. De AVG regelt bijvoorbeeld wanneer een DPIA (Data Protection Impact Assessment) moet worden gedaan, wat de rol van de Functionaris Gegevensbescherming is, hoe een verwerkingsregister eruit moet zien, hoe je met datalekken om moet gaan en hoe je transparant moet zijn naar betrokken personen over het gebruik van hun persoonsgegevens.

Specifiek voor Nederland is de AVG uitgebreid met een aantal regels die voor Nederland gelden, onder andere om de AVG goed op de Nederlandse wetgeving te laten aansluiten. Dit is geregeld in Uitvoeringswet AVG (UAVG). De Autoriteit Persoonsgegevens (AP) houdt in Nederland toezicht op de uitvoering van de AVG en de UAVG.

3. Wetgeving voor politie en justitie (WPG en WJSG)

Het gebruik van persoonsgegevens voor de openbare veiligheid of bij de opsporing en rechtspraak is in de AVG expliciet uitgesloten (artikel 2, lid 2 Sub d). De AVG stelt wel dat de EU-lidstaten daar specifieke wetgeving voor moeten maken. In Nederland is dat geregeld in de Wet politiegegevens (WPG) voor de politie en de Wet justitiële en strafvorderlijke gegevens (WJSG) voor het Openbaar Ministerie en de Rechtspraak.

De WPG en de WJSG staan náást de AVG. Beide wettelijke kaders zijn volledig onderscheidend: een partij die onder de WPG valt, valt niet onder de AVG en andersom. Alle partijen vallen onder een van de drie kaders. Zo valt de openbare orde en veiligheidstaak (OOV-taak) van de burgemeester onder de AVG. Maar de inzet van de politie (die de burgemeester op grond van zijn OOV-taak mag vorderen) valt onder de WPG.

4. Materiewetten en uitvoeringsbesluiten

De AVG regelt dat de wetgever nadere eisen kan (c.q. moet) stellen aan de manier waarop bij de uitvoering van een wettelijke taak persoonsgegevens gebruikt worden. Dit is geregeld in de zogeheten 'materiewetten'. Het gaat dan bijvoorbeeld om de Wet maatschappelijke ondersteuning, de Jeugdwet, de Participatiewet, de Wet gemeentelijke schuldhulpverlening, de Zorgverzekeringswet, de Wet langdurige zorg, de Wet verplichte ggz, de Penitentiaire beginselenwet, de Politiewet etc.

In de materiewetten is geregeld welke maatschappelijke taak een partij heeft, welke persoonsgegevens daarvoor verwerkt mogen worden, welke gegevens eventueel van andere partijen verkregen mogen worden en welke gegevens de uitvoerder van de taak aan derden mag verstrekken (inclusief de voorwaarden waaronder de eventuele gegevensuitwisseling moet plaatsvinden).

Daarnaast geven de materiewetten vaak richting aan het onderliggende werkproces. De Wvggz beschrijft bijvoorbeeld in detail hoe de burgemeester, de geneesheerdirecteur in de GGZ en de officier van justitie met elkaar moeten samenwerken in geval van een crisismaatregel of een zorgmachtiging. De materiewetten zijn in het algemeen verder uitgewerkt in een algemene maatregel van bestuur (AMvB) of een besluit. De precieze details van welke gegevens uitgewisseld mogen worden onder welke voorwaarden, is in het algemeen in dergelijke besluiten opgenomen en niet in de wet zelf.

5. Specifieke persoonsgegevenswetten
Een aantal wetten gaat specifiek over de omgang met bepaalde persoonsgegevens. Een voorbeeld is de Wet algemene bepalingen burgerservicenummer (Wet BSN) en de Wet gebruik burgerservicenummer in de zorg (Wbsn-z). Een ander voorbeeld is de Wet basisregistratie personen, die regelt onder welke voorwaarden de officieel vastgelegde gegevens over naam, adres, woonplaats en familierelaties gebruikt mogen worden. De gegevenswetten stellen heel precieze eisen aan het gebruik van bepaalde gegevens (zoals BSN en adres).

6. Beroepsgeheim en medische wetgeving
Voor het zorgdomein gelden verschillende wetten die heel precies regelen hoe medische professionals met gegevens over hun patiënten moeten omgaan. De belangrijkste is de Wet geneeskundige behandelovereenkomst (Wgbo), die het medisch beroepsgeheim regelt. Het medisch beroepsgeheim staat náást de privacywetgeving. Het is dus mogelijk dat een gegevensuitwisseling op grond van de AVG en de materiewetgeving is toegestaan, maar dat op grond van de Wgbo de medische professional besluit de informatie toch niet te delen. Dat is een belangrijk recht dat de medische professional en de patiënt hebben, om de vertrouwelijke relatie tussen behandelaar en patiënt te beschermen.

Ook de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG) stelt nadere eisen aan de (medische) professional en de kwaliteit van de zorgverlening. Voor de jeugdzorg geldt ook een beroepsgeheim op grond van de Jeugdwet, en een verplichte registratie in het Kwaliteitsregister Jeugd (SKJ-registratie). Overigens zijn er meer beroepsgroepen waarvoor een beroepsgeheim geldt. Denk aan advocaten, notarissen, politiemensen, accountants en ambtenaren in fiscale- of inlichtingendiensten.

Samenhang
De kern van de 'privacyregels' worden in deze hiërarchie gevormd door de privacywetten (AVG, UAVG, WPG en WJSG). Deze bieden het algemeen kader met beginselen en voorwaarden die aan een rechtmatige en zorgvuldige verwerking van persoonsgegevens gesteld worden. Zij bevatten de rechten van betrokkene. Zoals het recht op inzage, correctie en bezwaar of verzet tegen de verwerking van gegevens. De AVG bepaalt dat de overheid persoonsgegevens van burgers mag verwerken – en dus ook delen - als deze noodzakelijk zijn voor de goede uitvoering van een wettelijke taak. Bij WPG en WJSG is dat net andersom. Politie en Justitie mogen in het algemeen slechts gegevens delen als dit specifiek in de wet of de onderliggende besluiten is geregeld.

Binnen deze kaders zijn de materiewetten van belang. Zij beschrijven de wettelijke taken van de overheid op specifieke onderwerpen zoals maatschappelijke ondersteuning (Wmo), werk en inkomen (o.a. de Participatiewet) en verplichte zorg (Wvggz). Voor overheidsorganisaties ligt daar de juridische basis voor de verwerking van persoonsgegevens op grond van de AVG. De AVG stelt namelijk dat de overheid alleen persoonsgegevens van burgers mag verwerken als dat berust op een wettelijke taak. Geen taak betekent voor de overheid ook geen bevoegdheid tot gegevensverwerking over burgers.

Daarnaast regelen de materiewetten vaak bevoegdheden voor instanties die actief zijn als aanbieder van voorzieningen, hulp of zorg. De materiewetten bevatten veelal gedetailleerde paragrafen gegevensverwerking. Daarin staan verplichtingen, bevoegdheden, geheimhoudingen en andere mogelijkheden en beperkingen voor gegevensverwerking.

De complexiteit van gegevensverwerking zit niet zo zeer in de AVG, maar in de diversiteit en gedetailleerdheid van deze regelgeving.

Analyse relevante regelgeving
Al deze wetten kunnen van belang zijn om, in het kader van samenwerking, gegevens uit te kunnen wisselen. Welke wetten het precies betreft, hangt af van de partijen en hun beoogde taken binnen de samenwerking. Professionals kunnen dit juridische veld onmogelijk overzien. Bij het inrichten van een nieuwe samenwerking moeten de juristen van de deelnemende organisaties daarom een gedegen analyse maken. Deze bevat niet alleen de relevante wetgeving, maar ook de mogelijkheden, beperkingen en randvoorwaarden voor de gegevensverwerking die daaruit voortvloeien. Zo komt het juridisch kader tot stand, op basis waarvan de professionals uiteindelijk heldere instructies krijgen voor hun handelingsruimte.

3.2 Zorgvuldigheid volgens de AVG

De AVG bevat vrijwel geen verboden[6], maar geeft de uitgangspunten en randvoorwaarden voor een zorgvuldige gegevensverwerking.

Maar wat is zorgvuldig? Daarvan geeft de AVG een concrete definitie. De verwerking van persoonsgegevens (en daarmee ook de gegevensuitwisseling) moet voldoen aan de zes beginselen uit artikel 5 van de AVG en de verwerkingsverantwoordelijke moet kunnen aantonen dat deze hieraan voldoet.

De beginselen van zorgvuldigheid

1. Rechtmatigheid, behoorlijkheid en transparantie

De verwerker moet kunnen aantonen dat hij de gegevens mag verwerken en dat dit noodzakelijk is voor het goed uitvoeren van zijn wettelijke taken. Daarnaast moet er sprake zijn van proportionaliteit. De risico's voor de betrokkene als gevolg van de gegevensverwerking, moeten worden afgewogen tegen het maatschappelijk belang van de (wettelijke) taak (zoals zorgverlening, maatschappelijke ondersteuning, veiligheid etc.). Transparantie naar diegene van wie de persoonsgegevens worden verwerkt, is vereist. Dat kan bijvoorbeeld door hem te informeren over het doel van de verwerking en om welke persoonsgegevens het gaat.

2. Doelbinding

Het doel van de gegevensverwerking moet goed omschreven zijn en de persoonsgegevens mogen niet voor andere doeleinden worden gebruikt. Het doel van de gegevensverwerking vloeit rechtstreeks voort uit de taken vanuit de materiewetten. Een gemeente die bepaalde informatie over een cliënt heeft vanuit de Wmo, mag deze informatie dus niet (zomaar) gebruiken voor het uitvoeren van haar taken in de Participatiewet.
De AVG bevat wel een mogelijkheid om persoonsgegevens voor een ander doel te gebruiken, mits de doelen 'verenigbaar' zijn. Dit mag niet leiden tot extra risico's voor de betrokkene (AVG artikel 6, lid 4).

3. Minimale gegevensverwerking

Minimalisatie van gegevensverwerking houdt in dat er alléén gegevens verwerkt mogen worden die echt noodzakelijk zijn om het doel te bereiken. De AVG spreekt van: *toereikend, ter zake dienend en noodzakelijk voor de doeleinden waarvoor wordt verwerkt*.

De verwerkingen moeten ook proportioneel zijn. Dat wil zeggen dat ze in verhouding moeten staan tot het doel. Informatie die niet of niet meer voor het doel nodig is, wordt vernietigd. Nice to have is geen optie. Minimalisatie kan in de praktijk ook betekenen dat gegevens überhaupt niet worden opgeslagen. In een casusoverleg moet één van de basisafspraken zijn dat er géén behandelinformatie wordt opgeslagen in het casusondersteunend systeem. Informatie die niet is opgeslagen, kan immers ook niet in verkeerde handen vallen.

[6] Artikel 2, lid 3 van de AVG stelt: "Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de bescherming van persoonsgegevens."

4. Juistheid

Organisaties moeten zich inspannen om ervoor te zorgen dat de persoonsgegevens die zij verwerken correct zijn en regelmatig worden geactualiseerd. Informatie die niet klopt, wordt zo snel mogelijk gecorrigeerd of verwijderd. Bij de samenwerking in het sociaal, zorg- en veiligheidsdomein is dit bijvoorbeeld van belang bij een meldpunt (zoals het Meldpunt Zorg en Overlast of bij bemoeizorg), waar een melding vaak ook vermoedens bevat. Op grond van dit 'juistheidsbeginsel' moet het meldpunt voorkomen dat vermoedens als feiten worden behandeld. De vermoedens moeten onderzocht of onderbouwd worden, voordat de inhoud in de verdere dienstverlening kan worden gebruikt.

5. Opslagbeperking

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is. In een aantal materiewetten zijn wettelijke termijnen gesteld aan hoelang je bepaalde gegevens moet bewaren. Het meldpunt Veilig Thuis is bijvoorbeeld wettelijk verplicht om persoonsgegevens in dossiers ten minste twintig jaar te bewaren. Op grond van de AVG is deze minimale bewaartermijn meteen ook de maximale bewaartermijn.

Als er geen wettelijke bewaartermijn is, stelt de AVG dat je vooraf nadenkt hoelang je gegevens bewaart, en onderbouwt waarom die bewaartermijn noodzakelijk en proportioneel is. Als de bewaartermijn is verstreken, vernietig je de persoonsgegevens, of draagt deze conform de Archiefwet over aan het archief. De gegevens zijn dan niet meer te raadplegen voor operationele processen.

6. Integriteit en vertrouwelijkheid

Persoonsgegevens moeten op een passende manier beschermd worden door organisatorische maatregelen en beveiliging. Dit om te voorkomen dat onbevoegde personen toegang hebben tot de persoonsgegevens en dat de persoonsgegevens niet verloren gaan of misbruikt worden. Dit gaat over ICT-beveiliging (passwords, encryptie, gebruik van veilige mail e.d.), maar ook over training van medewerkers in 'privacybewustzijn'.

7. Verantwoordingsplicht

De AVG verplicht partijen die gegevens verwerken om aan te tonen dat aan bovenstaande zes beginselen is voldaan. Zij moeten onderbouwen op grond waarvan zij vinden dat ze gegevens van iemand mogen verwerken. Overheidspartijen moeten hun verwerking kunnen baseren op een wettelijke taak.

Ook is een analyse van risico's voor de betrokkene en een privacyplan vereist. Zo moeten plannen regelmatig worden geëvalueerd en vinden er bijvoorbeeld regelmatig audits (technisch en inhoudelijk) plaats. Voor de samenwerking in het sociaal, zorg- en veiligheidsdomein betekent dit dat zij moeten onderbouwen waarom samenwerking noodzakelijk is en waarom het belang van samenwerking zo groot is dat het privacybelang van de betrokkene hiervoor deels moet wijken (zie hoofdstuk 2). Een praktisch gevolg is dat samenwerkende partijen hun afspraken moeten vastleggen, bijvoorbeeld in een samenwerkingsconvenant en een privacyprotocol. Daarbij moet periodiek geëvalueerd worden of de afspraken in het convenant en protocol daadwerkelijk worden opgevolgd.

Deze principes geven geen concrete acties of maatregelen. Ze beschrijven alleen *wat* je moet doen, niet *hoe* je het moet doen. Het is aan organisaties die persoonsgegevens verwerken (en aan de samenwerkende partijen) om een afweging te maken hoe ze deze principes naleven bij de verwerking van persoonsgegevens. De verwerker heeft vanuit de AVG de plicht om de naleving van deze principes aan te kunnen tonen.

3.3 Grondslag

De noodzaak van een grondslag

Naast de beginselen van zorgvuldigheid vereist de AVG dat er een grondslag is voor de gegevensverwerking. Voor het uitwisselen van gegevens tussen samenwerkende partijen, zal in het algemeen de partij die de gegevens levert een grondslag moeten hebben om de informatie te verstrekken. De ontvangende partij zal een éigen grondslag moeten hebben om de ontvangen informatie voor de eigen taak verder te gebruiken.
De AVG kent zes mogelijke grondslagen. Deze staan in AVG artikel 6, lid 1.

AVG artikel 6, lid 1

1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:
   a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
   b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
   c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
   d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
   e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
   f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

Om een verwerking mogelijk te maken, moet de partij die de persoonsgegevens verwerkt één van deze grondslagen kunnen aanwijzen. Voor overheidsorganisaties en de meeste organisaties in het sociaal, zorg- en veiligheidsdomein is de grondslag in het algemeen niet het meest ingewikkelde vraagstuk.

De uitdaging zit in de zorgvuldigheid waarmee de afweging om wel niet gegevens te verwerken gebeurt. De grondslag vloeit voort uit de goede uitoefening van hun eigen (wettelijke) taken van partijen. Voor de overheid is in de praktijk artikel 6, lid 1 onder e vrijwel altijd de enige geldige grondslag. De grondslag artikel 6, lid 1 onder e is ook van toepassing op private organisaties die taken uitvoeren die bij wet zijn geregeld, zoals de Reclassering of een Gecertificeerde Instelling voor jeugdbescherming.

De grondslag overeenkomst (AVG artikel 6, lid 1 onder b) is met name van toepassing voor zorgpartijen, zoals de GGZ. Als zij zorg verlenen in het vrijwillig kader is daarop de Wet Geneeskundige Behandelovereenkomst van toepassing.

Partijen zonder expliciete taak
Voor een aantal partijen kan het ingewikkeld zijn om een goede grondslag te vinden om persoonsgegevens te mogen verstrekken of om ze te ontvangen en verder te verwerken. Dit geldt bijvoorbeeld voor woningbouwcorporaties. Die hebben geen expliciete taak, waaruit het delen van informatie met andere partijen in het sociaal, zorg- en veiligheidsdomein voortvloeit.

Om gegevensdeling met een woningbouwcorporatie toch mogelijk te maken, moet worden verwezen naar een taak in het sociaal, zorg- en veiligheidsdomein, waarin zij een rol spelen. Dat zal in het algemeen gelinkt zijn aan een specifiek doel (zoals het tegengaan van woonoverlast). Meldingen dóór woningbouwcorporaties zijn mogelijk als de wet een brede kring van mogelijke melders toestaat (zoals bijvoorbeeld bij Veilig Thuis of voor een verkennend onderzoek Wvggz). De melding moet dan wel specifiek betrekking hebben op het doel dat in die wet is vastgelegd. Het is niet mogelijk dat partijen zich in dit geval beroepen op 'restgrondslagen' zoals vitaal belang of gerechtvaardigd belang. Zolang er geen passende wetgeving wordt toegevoegd, is de uitwisseling van gegevens eenvoudigweg[7] niet mogelijk.

Toestemming is geen geldige grondslag
Toestemming is in de praktijk in de samenwerking in het sociaal, zorg- en veiligheids-domein nooit een passende grondslag. In de AVG is toestemming als grondslag voor de verwerking van persoonsgegevens door de overheid uitgesloten, omdat er per definitie sprake is van een afhankelijkheidsrelatie tussen betrokkene en de overheid. De overheid beslist immers over toekenning van rechten of voorzieningen, of kan sancties opleggen. Door die afhankelijkheidsrelatie is er geen sprake meer van 'toestemming in vrijheid gegeven'.

De Autoriteit Persoonsgegevens stelt: "Een 'onvrije' toestemming vormt geen grondslag. Gemeenten mogen dan alléén persoonsgegevens verwerken als zij zich kunnen baseren op een van de andere grondslagen."[8]

Om goede zorg te kunnen ontvangen van bijvoorbeeld een GGZ-instelling, zal deze instelling gegevens moeten kunnen verwerken van de burger. De burger is formeel vrij om zelf te kiezen wie hem zorg of hulp verleent, en bepaalt zelf welke informatie

[7] De komst van de WAMS (wet aanpak meervoudige problematiek sociaal domein) zal de woningbouwcorporaties iets meer mogelijkheden geven om zorgen over een cliënt te kunnen delen of om onderdeel te zijn van een gezamenlijke hulpverlening. Maar zolang de WAMS nog in behandeling is biedt dit geen grondslag en is het delen van informatie door bijvoorbeeld de woningbouwcorporaties nog niet toegestaan.

[8] Zie het Oonderzoeksrapport 'Verwerking van persoonsgegevens in het sociaal domein: Dde rol van toestemming', Autoriteit Persoonsgegevens, april 2016. NB.B. Dde beoordeling in het rapport is gemaakt op basis van de Wet Bescherming Persoonsgegevens (WBP), omdat in 2016 de AVG nog niet van kracht was. De argumentatie en conclusies van de AP zijn echter onverminderd geldig binnen de AVG. Zie: https://autoriteitpersoonsgegevens.nl/uploads/imported/toestemmingsrapport_definitief_incl_bijlagen.pdf

hij verstrekt. De grondslag voor de zorgverlener ligt in het feit dat de burger een behandelrelatie met hem of haar is aangegaan. Op die relatie is de Wgbo van toepassing. De AVG-grondslag om gegevens te verwerken is in dat geval artikel 6, lid 1 onder b, noodzakelijk voor de uitvoering van een overeenkomst.

Onderdeel van de Wgbo is het medisch beroepsgeheim. Daarin is in de regel toestemming vereist om het beroepsgeheim te doorbreken. Toestemming is in die context iets anders dan toestemming in de zin van de AVG. Soms is er sprake van verplichte zorg. In dergelijke situaties vormt niet een overeenkomst de basis voor de behandelrelatie, maar een door de rechter opgelegde maatregel. De grondslag voor de gegevensverwerking in het kader van de AVG is dan de uitvoering van een wettelijke taak (artikel 6, lid 1 onder e AVG).

In het sociaal zorg- en veiligheidsdomein ligt de basis voor het verwerken van gegevens, in vrijwel alle situaties, bij het uitvoeren van een bij de wet geregelde taak van de betreffende organisatie (artikel 6, lid 1 onder e AVG) of bij vrijwillige zorg in de behandelovereenkomst die een professional heeft met de betreffende patiënt/cliënt (artikel 6, lid 1 onder b AVG).

3.4. Risicobeoordeling (DPIA)

De verplichting om een Data Protection Impact Assessment (DPIA) uit te voeren, vloeit voort uit artikel 35 van de Algemene Verordening Gegevensbescherming (AVG) wanneer een nieuwe gegevensverwerking aanzienlijke privacyrisico's met zich meebrengt voor de betrokken personen.[9]

De Autoriteit Persoonsgegevens heeft specifieke criteria opgesteld om te bepalen voor welke soorten verwerkingen een DPIA noodzakelijk is.[10] Dit betreft bijvoorbeeld de verwerking van persoonsgegevens die als zeer persoonlijk worden beschouwd, of de verwerking van gegevens van kwetsbare groepen. In de praktijk zal bij de inrichting van een gegevensknooppunt binnen het sociaal domein of het zorg- en veiligheidsdomein vrijwel altijd sprake zijn van een situatie waarin een DPIA vereist is. Zoals beschreven in deze handreiking, is het uitvoeren van een DPIA daarom een verplichte stap bij de inrichting van een dergelijk knooppunt.

Het doel van de DPIA is om de mogelijke risico's voor de personen die bij het gegevensknooppunt betrokken zijn, in kaart te brengen en om maatregelen te identificeren die deze risico's zo veel mogelijk kunnen beperken. De AVG schrijft voor welke elementen een DPIA moet bevatten (art.35, lid 7 AVG):

a. Een beschrijving van de voorgenomen aanpak, het doel van de aanpak en de persoonsgegevens

Voor het type knooppunten dat in deze handreiking centraal staat, dient de DPIA een beschrijving te geven van het doel van het knooppunt, de partijen die deelnemen aan de samenwerking, en de noodzaak van hun betrokkenheid. Daarnaast moet de DPIA verduidelijken welke doelgroep door de samenwerking wordt bediend en op basis van welke criteria personen bij een meldpunt kunnen worden aangemeld of op een overlegtafel besproken kunnen worden.

9. De formele Nederlandse term voor DPIA die in de AVG wordt gebruikt, is 'gegevensbeschermingseffectbeoordeling'. In deze handreiking gebruiken we de term 'DPIA'.
10. Zie https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia

b. Een beoordeling van de noodzaak en evenredigheid van de aanpak
In de DPIA moet worden aangetoond dat het gegevensknooppunt zorgvuldig is ontworpen en dat alleen partijen deelnemen die essentieel zijn voor het bereiken van het beoogde doel. Dit houdt in dat voor elke deelnemende partij moet worden aangegeven wat hun rol in de samenwerking is, waarom die rol noodzakelijk is, en welke wettelijke basis (lees: wettelijke taak) hun deelname rechtvaardigt. Verder moet de DPIA aantonen hoe het knooppunt voldoet aan de zes basisbeginselen van de AVG (zie paragraaf 3.2) en hoe deze beginselen zijn geïmplementeerd in het ontwerp van het knooppunt.

c. Een inventarisatie van de mogelijke risico's voor de in de aanpak betrokken personen
Mogelijke risico's omvatten bijvoorbeeld het gevoel van stigmatisering wanneer iemand bij een meldpunt wordt gemeld of op een overlegtafel wordt besproken. Dergelijke situaties kunnen aanzienlijke gevolgen hebben voor de betrokkene, zoals problemen op werk of in hun opleiding. In extreme gevallen kan het zelfs de persoonlijke veiligheid van een individu in gevaar brengen als bekend wordt dat hij of zij in het knooppunt bekend is. Door deze risico's vooraf te identificeren, kunnen maatregelen worden getroffen om ze zoveel mogelijk te voorkomen.

d. Een beschrijving van maatregelen om de geïnventariseerde risico's te voorkomen
De maatregelen die in de DPIA worden beschreven, zijn bedoeld om te voorkomen dat personen onnodige schade ondervinden als gevolg van hun melding bij het knooppunt of hun opname in een gezamenlijke aanpak. Dit begint met een zorgvuldige organisatie van de aanpak, waarbij de DPIA beschrijft hoe dit is geregeld (zie hoofdstuk 4 voor een uitgebreide toelichting). Het is daarnaast cruciaal om ervoor te zorgen dat mensen niet onterecht worden gemeld of opgenomen in een aanpak. De DPIA moet aangeven welke controlemiddelen ('double checks') of maatregelen worden getroffen om dit te voorkomen. Ten slotte moeten er maatregelen worden genomen om te voorkomen dat gegevens in verkeerde handen vallen of door deelnemende partijen worden 'misbruikt'. De DPIA dient ook deze preventieve maatregelen te beschrijven om het lekken van gegevens of misbruik te voorkomen.

Tips:

- Bij het uitvoeren van een DPIA is het van belang de focus te leggen op de inhoud en de noodzaak van de beoogde aanpak. Hoewel de juridische analyse, waaronder het vaststellen van de grondslag, een belangrijk onderdeel vormt van de DPIA, is het niet de kern. De kern van de DPIA ligt in het aantonen van de inhoudelijke noodzaak van de aanpak, het identificeren van de risico's voor de betrokken personen, en het vaststellen van maatregelen om deze risico's te voorkomen. Het is daarom cruciaal om bij het opstellen van een DPIA niet alleen juridische adviseurs te betrekken, maar ook inhoudelijke experts van de samenwerkingspartners. Dit zorgt ervoor dat de inventarisatie van de risico's nauw aansluit bij de specifieke doelgroep. Overweeg daarbij ook om een vertegenwoordiger van deze doelgroep te betrekken bij de uitvoering van de DPIA, zodat de assessment uitgroeit tot een praktisch en concreet instrument dat effectief bijdraagt om het gegevensknooppunt meer aan te sluiten op de praktijk.
- De betrokkenheid van de functionaris gegevensbescherming (FG) is een vereiste bij de uitvoering van een DPIA (artikel 35, lid 2 AVG). De FG kan waardevol advies geven over de opzet en de inhoud van de DPIA. Voordat de FG wordt betrokken, is het essentieel om vast te stellen welke partij(en) verwerkingsverantwoordelijk is/zijn voor het beoogde gegevensknooppunt.

3.5 Overige vereisten vanuit de AVG

Het waarborgen van de inhoudelijke noodzaak alleen is niet voldoende om de rechtmatigheid van een gegevensknooppunt te garanderen. Hoewel de inrichting van een knooppunt begint met een inhoudelijke beoordeling van een maatschappelijk vraagstuk (zie hoofdstuk 2), moet ook aan de specifieke 'privacy-huiswerk' verplichtingen van de AVG worden voldaan. De AVG stelt een aantal concrete en specifieke vereisten waaraan altijd moet worden voldaan. De belangrijkste zijn:[11]

- **Privacyverklaring:** Zorg ervoor dat het algemene publiek geïnformeerd is over het doel, de werking en de wijze waarop binnen het gegevensknooppunt zorgvuldig met persoonsgegevens wordt omgegaan. Dit kan bijvoorbeeld via een 'privacyverklaring' op de website van de gemeente of het samenwerkingsverband waarin het knooppunt is ondergebracht.
- **Rechten van betrokkenen:** Op grond van de privacywetgeving (art. 12-23 AVG) heeft de persoon waarvan de gegevens worden verwerkt, verschillende rechten, zoals het recht om bezwaar te maken, het recht op inzage, en (onder bepaalde voorwaarden) het recht om onjuiste gegevens te laten corrigeren of verwijderen.
- **Informeren van de betrokkene:** Het is verplicht om de personen waarvan gegevens in een knooppunt worden verwerkt, hiervan op de hoogte te stellen. Dit betekent bijvoorbeeld dat een persoon na triage voor een overlegtafel geïnformeerd moet worden dat hij of zij daar besproken zal worden. De betrokkene moet geïnformeerd worden over welke persoonsgegevens worden verwerkt, door welke partijen, met welk doel, en waarom die verwerking noodzakelijk is. Daarnaast moet de betrokkene worden ingelicht over de rechten die hij of zij heeft.

11. Het doel van deze handreiking is niet om volledig te zijn over de vereisten vanuit de AVG. Op andere plaatsen is volop informatie beschikbaar over welke vereisten er zijn en op welke manier daaraan voldaan kan worden. Zie bijvoorbeeld https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/#privacy voor een overzicht van veel handreikingen voor specifieke AVG-producten.

- **Verwerkingsverantwoordelijke:** Zorg ervoor dat duidelijk is welke partij de verwerkingsverantwoordelijke is voor het gegevensknooppunt, of welke partijen gezamenlijk verwerkingsverantwoordelijk zijn. Duidelijkheid over de verwerkingsverantwoordelijkheid is essentieel, onder meer omdat dit de partij is die aansprakelijk is voor eventuele boetes indien de gegevensverwerking onrechtmatig blijkt te zijn. Daarnaast is het van belang om te weten welke functionaris(sen) gegevensbescherming toezicht houdt (houden) op de gegevensdeling in het knooppunt
- **Informatiebeveiliging:** alle persoonsgegevens die worden verwerkt moeten goed beveiligd zijn en alleen toegankelijk zijn voor de medewerkers die ook echt bij een casus betrokken zijn. Een goede informatiebeveiliging omvat niet alleen technische ICT-maatregelen (zoals passwords en autorisatietabellen), maar ook organisatie-maatregelen (zoals het screenen van medewerkers of het organiseren van toezicht). De inrichting van de informatiebeveiliging van buiten bestek van deze handreiking. Het is raadzaam om deskundigen binnen de samenwerkende partijen om advies te vragen om dit goed in te richten.[12]

3.6 Gegevensverwerking bij samenwerking

De AVG en de meeste materiewetten kennen geen specifieke bepalingen over gegevensverwerking ten behoeve van samenwerking. Een organisatie die gegevens verwerkt en deelt in het kader van de samenwerking, doet dat in beginsel op basis van zijn eigen taak in relatie tot de gemeenschappelijke maatschappelijke opgave. En de AVG-grondslag voor de gegevensverwerking vindt zijn basis in de eigen materiewet of behandelrelatie met de betrokkene.

Dat is gebaseerd op de veronderstelling dat de samenwerking en afstemming met andere organisaties mede noodzakelijk is voor de goede uitvoering van de eigen taken en werkzaamheden. Oftewel, om het eigen werk goed te kunnen doen, is het noodzakelijk om samen te werken met anderen. Dat speelt met name als er sprake is van samenhang in de problemen die de burger ervaart en veroorzaakt, en de activiteiten van de verschillende betrokken partijen elkaar beïnvloeden. Samenwerking en afstemming is dan nodig om de eigen werkzaamheden zo effectief mogelijk te laten zijn, en om te voorkomen dat werkzaamheden van partijen elkaar tegenwerken. Alleen door samenwerking kan bereikt worden dat het beter gaat met de persoon en de problemen die deze veroorzaakt verminderen.

[12] Over informatiebeveiliging zijn veel handreikingen beschikbaar. Een schat aan informatie over informatiebeveiliging bij gemeenten en hun samenwerkingspartners: https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/#IB

Voorbeeld

Iemand die schulden heeft als gevolg van een verslaving, maakt zich schuldig aan diefstal. Het bestraffen van de diefstal alléén, lost het probleem niet op. Het kan de schulden zelfs verergeren. De schulden worden niet opgelost als de verslaving voortduurt. En als er niets gebeurt, komt de betrokkene in een negatieve spiraal terecht, die tot gezondheidsschade kan leiden.

Door samenwerking en afstemming van interventies kunnen alle betrokken partijen effectiever worden in hun eigen taken. Denk aan het voorkomen van recidive, het verminderen van schulden en andere negatieve effecten van de verslaving, zoals overlast of gezondheidsschade voor de betrokkene of mensen in de omgeving. Het overkoepelende doel van de samenwerking kan zijn: het verminderen van de overlast, door te zorgen dat het beter gaat met de persoon in kwestie.

De grondslag voor het verwerken, waaronder het delen van gegevens, bij samenwerking is dus voor elke partij primair dezelfde grondslag als de grondslag voor de eigen (wettelijk) taak. Als het in het bovenstaande voorbeeld gaat om een volwassene met kinderen, zal waarschijnlijk ook het college van B&W betrokken zijn. Omdat de gemeente, naar alle waarschijnlijkheid, jeugdhulp of jeugdbescherming in zal zetten, in aanvulling op de trajecten van andere organisaties. De grondslag voor de gegevens-verwerking door het college van B&W is dan gelegen in artikel 6, lid 1 onder e AVG: de gegevensverwerking is noodzakelijk voor de goede uitvoering van haar jeugdwettaak.

Het vertrekpunt van de samenwerking wordt bepaald door:

- Het belang van de maatschappelijke opgave;
- De noodzaak voor samenwerking;
- De wettelijke taken uit de materiewetten (bijv. Wmo, schuldhulpverlening, Jeugdwet, Politiewet) die noodzakelijk zijn voor de aanpak bij de maatschappelijke opgave;
- De relevante problematiek waarvoor betrokkene in behandeling is bij een zorgverlener en de samenhang daarvan met de andere problemen.

De (wettelijke taak) van de inbrengende partij is doorgaans leidend voor de grondslag om gegevens te delen. Het helder hebben van het doel, de taken van de te betrekken partijen en hun relatie met de betrokkene zijn daarmee essentiële voorwaarden om de mogelijkheden voor het delen van persoonsgegevens in beeld te krijgen.

Er kan discussie ontstaan in hoeverre de samenwerking nog voldoende past bij de eigen taak en relatie met de betrokkene. Uiteindelijk is het aan de verwerkingsverantwoordelijke (in de regel de bestuurders) om daar, op basis van een inhoudelijke onderbouwing, een knoop over door te hakken.

3.7 Een stappenplan

Om de rechtmatigheid van de gegevensverwerking bij samenwerking aan te tonen, moeten bovenstaande elementen in samenhang bekeken worden. Voor zo'n analyse is het volgende stappenplan[13] behulpzaam.

Op basis van de juridische analyse, kunnen de (wettelijke) taken en grondslagen benoemd worden op grond waarvan de partijen in de samenwerking gegevens mogen delen. Mits hun betrokkenheid nodig is in een specifieke casus. Dat is een eerste onderdeel van de onderbouwing van de rechtmatigheid van de gegevensverwerking.

De beginselen van zorgvuldigheid van artikel 5 van de AVG bieden vervolgens houvast om te kunnen bepalen of de gegevensuitwisseling en samenwerking zorgvuldig zijn ingericht. En voor de specifieke mogelijkheden en belemmeringen van partijen in de samenwerking om gegevens te delen, zijn de materiewetten van belang. Het is dus nodig om het totaal aan wetten en wettelijke vereisten te overzien om een juridische grondslag te kunnen construeren voor een samenwerking en gegevensuitwisseling in een knooppunt.

Stappenplan rechtmatigheid gegevensverwerking bij samenwerking

Stap 1: Doel en noodzaak van de samenwerking

Beschrijf het doel en de noodzaak van de samenwerking zo concreet mogelijk. Wat is de maatschappelijke opgave, welke bijdrage moet samenwerking daaraan leveren, waarom is die samenwerking noodzakelijk?

Stap 2: Deelnemers en inventarisatie van materiewetten

Benoem de partijen die potentieel noodzakelijk zijn voor de samenwerking en breng elke partij afzonderlijk in kaart op grond van welke (wettelijke) taak zij deelnemer kunnen zijn in het knooppunt. Doe dit op artikelniveau.

Stap 3: Noodzakelijke gegevens

Inventariseer welke type gegevens, gezien de het doel van de samenwerking, aan de orde kan zijn in de samenwerking. Dit betekent niet dat al deze gegevens altijd worden verwerkt. Welke gegevens in een specifieke casus noodzakelijk zijn, wordt uiteraard bepaald door de inhoud van de casus.

Stap 4: Juridische analyse

a. Vereisten vanuit privacywetgeving

Benoem specifieke vereisten vanuit de privacywetgeving, zowel de WPG (voor de politie), de WJSG (voor het Openbaar Ministerie) als de AVG. Het gaat dan bijvoorbeeld om de van toepassing zijnde grondslagen conform artikel 6 AVG die voortvloeien uit de (wettelijke) taken van partijen, de beginselen van zorgvuldigheid zoals benoemd in artikel 5 van de AVG, de verwerkingsverantwoordelijkheid, de rechten van betrokkenen, de noodzaak om eventueel een DPIA doen, en dergelijke.

[13] Dit stappenplan is tot stand gekomen in samenwerking met Eric Schreuders van Net2Legal.

b. Bijzondere persoonsgegevens

De AVG stelt dat het gebruik van bijzondere persoonsgegevens[14] verboden is, tenzij aan specifieke uitzonderingen uit artikel 9, lid 2 van de AVG is voldaan. Die uitzonderingen zijn o.a. te vinden in de voor een partij geldende materiewetgeving en de UAVG. De WPG en de WJSG kennen hun eigen uitzonderingen.

Inventariseer óf er sprake is van de verwerking van bijzondere persoonsgegevens, onderbouw waarom dat noodzakelijk is, en onderbouw op grond waarvan de verwerking van die gegevens mogelijk is voor elke deelnemende partij afzonderlijk.

c. Strafrechtelijke gegevens

De AVG stelt dat strafrechtelijke gegevens alleen onder toezicht van de overheid mogen worden verwerkt (artikel 10 AVG), of als dat specifiek in nationale wetgeving is geregeld. Die bepalingen zijn te vinden in de materiewetten en in de UAVG. WPG en WJSG regelen de verwerking van strafrechtelijke gegevens door politie en justitiepartners.

Inventariseer óf er sprake is van de verwerking van strafrechtelijke gegevens, onderbouw waarom dat noodzakelijk is, en onderbouw op grond waarvan de verwerking van die gegevens mogelijk is voor elke deelnemende partij afzonderlijk.

d. Wettelijke nummers en BRP

Het gebruik van identificerende persoonsgebonden nummers en gegevens uit de BRP is in aparte wetgeving geregeld, zoals Wet algemene bepalingen burgerservicenummer, Wet BRP en de wet BSN in de zorg. Vaak wordt het gebruik van BSN verplicht in materiewetgeving.

Inventariseer óf er sprake is van de verwerking van persoonsgebonden nummers, onderbouw waarom dat noodzakelijk is, en onderbouw op grond waarvan de verwerking van die gegevens mogelijk is voor elke deelnemende partij afzonderlijk.

e. Specifieke bepalingen over geheimhouding of verstrekking

Inventariseer of er specifieke bepalingen zijn die verstrekking verhinderen, of die partijen juist verplichten tot het verstrekken van gegevens. Hierbij kan onder andere gedacht worden aan het (medisch) beroepsgeheim (Wgbo) de wet BIG of de Jeugdwet, een crisismaatregel (Wvggz), de verstrekkingsverplichtingen aan de Raad voor de Kinderbescherming en de verstrekkingsrechten aan Veilig Thuis.

[14] Bijzondere persoonsgegevens zijn gegevens over ras of etnische afkomst, politieke opvattingen, religie, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gegevens over gezondheid en gegevens over seksueel gedrag of seksuele gerichtheid (artikel 9, lid 1 AVG). Voor gegevens over strafbare feiten of veroordelingen gelden extra eisen (artikel 10 AVG).

3.8 Samenwerkingsconvenant en privacyprotocol

De uitkomst van dit stappenplan wordt vastgelegd in een samenwerkingsconvenant en/of een privacyprotocol van het knooppunt. Een samenwerkingsconvenant is niet altijd verplicht[15], maar het is wel verstandig om de volgende punten beschreven te hebben:

- Doel van de samenwerking, zo concreet en specifiek mogelijk beschreven;
- Welke partijen potentieel kunnen deelnemen aan de samenwerking en op grond van welke (wettelijke) taak;
- Welke grondslagen voor de gegevensverwerking van toepassing zijn;
- Welke typen gegevens aan de orde kunnen zijn, inclusief of het bijzondere, strafrechtelijke en/of persoonsgebonden nummers betreft;
- Hoe de verwerkingsverantwoordelijkheid is geregeld inclusief – indien van toepassing - het gebruik van een gezamenlijk systeem en datalekkenprocedure;
- Hoe de rechten van betrokkene worden geborgd, inclusief de mogelijkheid voor bezwaar en beroep;
- Hoe invulling gegeven wordt aan de zorgvuldigheidbeginselen uit artikel 5 van de AVG.

Let op: een samenwerkingsconvenant biedt op zichzelf niet een grondslag voor de gegevensuitwisseling. De grondslag vloeit altijd voort uit de wettelijke taken en bevoegdheden (zoals vastgelegd in de materiewetten) en de algemene kaders van AVG, WPG en WJSG. Een convenant is wel een manier om zaken die in wetgeving in algemene zin zijn benoemd specifiek te maken. Een belangrijk element daarin is het doel van de samenwerking. Wetgeving vereist dat gegevens verwerkt worden voor een specifiek doel. Het convenant beschrijft wat in een concrete samenwerking het doel is. Een convenant is tevens de manier om met elkaar ondubbelzinnig vast te leggen hoe wordt omgegaan met de wettelijke (on)mogelijkheden voor gegevensuitwisseling en om spelregels af te spreken over een omgang met respect voor elkaars kaders. Dat maakt de samenwerking en de gegevensuitwisseling transparant. Daarnaast worden zorgvuldigheidsafspraken ontdaan van vrijblijvendheid en wordt de zorgvuldige omgang met gegevens en elkaar afdwingbaar.

Model samenwerkingsconvenant en privacyprotocol

De Nederlandse zorg- en veiligheidshuizen hebben een model voor een samenwerkings-convenant en voor een privacyprotocol[16] opgesteld die hiervoor als basis hiervoor kunnen dienen. Het opstellen van een convenant is niet alleen nuttig om duidelijke afspraken te maken met de samenwerkende partijen in het knooppunt, maar ook kun je daarmee cliënten en andere partijen informeren over de het doel en de werkwijze van het knooppunt.

15. In een aantal gevallen is een convenant wél verplicht, met name als de politie in de samenwerking deelneemt. De verplichting is dan op grond van artikel 20 WPG.
16. Modelconvenant en protocol voor zorg- en veiligheidshuizen: https://www.zorgenveiligheidshuizen.nl/publicaties-nieuw/140720_modelconvenant-en-protocol-voor-de-zorg-en-veiligheidshuizen-beschikbaar

4. Zorgvuldigheid borgen in het werkproces

Hoe organiseer je de samenwerking aan de verschillende tafels zorgvuldig en zoveel mogelijk eenduidig voor de professionals?

Om professionals in staat te stellen zorgvuldig te handelen, moet de gegevensverwerking in het knooppunt goed georganiseerd zijn. Deze publicatie richt zich op knooppunten waarin meerdere partijen samenwerken om casuïstiek op te lossen, en waarin veelal sprake zal zijn van casusoverleg.

4.1 De AVG in de praktijk

In het vorige hoofdstuk hebben we de beginselen voor zorgvuldige gegevensverwerking uit artikel 5 van de AVG besproken. Wat betekent dit voor gegevensverwerking bij samenwerking in de praktijk?

De beginselen van zorgvuldigheid in de praktijk

1. Rechtmatigheid, behoorlijkheid en transparantie

Het juridische huiswerk moet op orde zijn. Dat betekent dat duidelijk is op basis waarvan de partners aan tafel kunnen zitten en waaraan deze hun bevoegdheid ontlenen om gegevens te verwerken. Geen taak is geen deelname. Die toets vindt plaats bij het inrichten van de samenwerking, maar dient bij elke casus steeds opnieuw plaats te vinden. Welke partijen zijn nodig *in dit specifieke geval*, gezien de aard van de problematiek?

2. Doelbinding

Het doel van de samenwerking moet gerechtvaardigd zijn. Op bestuurlijk niveau moet worden vastgesteld of het maatschappelijk belang van de samenwerking zo groot is, dat het de inbreuk op de persoonlijke levenssfeer van de burger rechtvaardigt en waarom dat zo is. In het sociaal, zorg- en veiligheidsdomein gaat het dan meestal om het belang van het verminderen of voorkomen van recidive bij ernstige overlast, criminaliteit of veiligheidsproblematiek. Niets doen is geen optie, omdat dit zou leiden tot onaanvaardbare situaties of escalatie van ernstige problemen.

Samenwerking is noodzakelijk, omdat de ernstige problemen anders niet verminderen of niet duurzaam worden opgelost. Bijvoorbeeld doordat interventies ineffectief zijn, omdat partijen langs elkaar heen werken. Ook hier vindt de afweging plaats op het inrichtingsniveau van de samenwerking. ‘Welke problematiek is zo ernstig dat het de samenwerking rechtvaardigt?’ En ook bij elke casus afzonderlijk: ‘Voldoet deze casus aan de criteria, is deze *specifieke casus* ernstig genoeg, dat die samenwerking rechtvaardigt?’

3. Minimale gegevensverwerking

Dit beginsel heeft betrekking op de bekende drie-eenheid: noodzaak, proportionaliteit en subsidiariteit. Je verwerkt alleen de gegevens die noodzakelijk zijn. Niet meer, maar ook niet minder. Daarbij moet altijd nagedacht worden over de consequenties van het delen van gegevens. Leidt het verstrekken niet tot onnodige en onevenredig zware consequenties voor de betrokkene, en hoe kan dit voorkomen worden? Voor een juiste maatvoering is een werkproces noodzakelijk waarin per fase wordt bekeken welke gegevens nodig zijn voor het doel van die fase, en welke gegevens door moeten naar de volgende fase. We laten in de volgende paragraaf zien hoe zo'n proces er uit ziet.

4. Juistheid

De partijen maken onderling afspraken om te zorgen dat de gegevens kloppen. Uitgangspunt is dat de partij die gegevens inbrengt verantwoordelijk is en blijft voor de juistheid van die gegevens, en ook voor de correctie van gegevens bij de bron (als blijkt dat gegevens niet (meer) juist zijn). Als een van de andere partijen constateert of vermoedt dat een gegeven niet klopt, geeft ze dit door aan de bronpartij.

5. Opslagbeperking

De samenwerkende partijen spreken af hoelang een gezamenlijk dossier bewaard wordt. Omdat een samenwerkingsdossier meestal niet onder een specifieke materiewet valt, is daarop de AVG van toepassing. Die stelt geen specifieke termijn, maar stelt dat gegevens niet langer bewaard mogen worden dan noodzakelijk. Partijen zullen dus, op basis van de inhoud van de problematiek, moeten onderbouwen hoelang het noodzakelijk is om de gegevens te bewaren. Zij moeten borgen dat de gegevens na het verstrijken van die termijn worden vernietigd of geanonimiseerd.

Let op: overheidspartijen zijn gehouden aan aanvullende vereisten uit de Archiefwet. Die vallen buiten het bestek van deze publicatie.

6. Integriteit en vertrouwelijkheid

De samenwerkende partijen zorgen ervoor dat hun ICT-systemen op orde en dus ook veilig zijn. Bijvoorbeeld dat uitsluitend mensen die te maken hebben met de casus, toegang hebben tot de voor hen relevante onderdelen van een dossier. Dat er controlemechanismen zijn om onrechtmatige toegang te detecteren en op te sporen en dat de procedures voor inbreuken en datalekken op orde zijn.

7. Verantwoordingsplicht

De organisaties die samenwerken, moeten op grond van de AVG kunnen aantonen dat ze aan bovenstaande beginselen voldoen. Dit kan door de afspraken vast te leggen in een samenwerkingsconvenant of privacyprotocol. Daarnaast zal het in het algemeen nodig zijn een DPIA uit te voeren op de samenwerking. De beschrijving van hoe je met de beginselen omgaat is vast onderdeel van een DPIA. Tot slot is het nodig om periodiek te toetsen of de afspraken ook worden nageleefd in de praktijk. Dit kan bijvoorbeeld in de vorm van een privacy-audit.

4.2 Uitgangspunten voor het werkproces

Als we de beginselen van zorgvuldigheid van de AVG vertalen naar een werkproces, levert dat voor **overlegtafels** de volgende uitgangpunten op:

- Aan het begin van het werkproces wordt getoetst of de casus op de betreffende overlegtafel thuishoort of niet. Alleen casussen die voldoen aan de criteria worden in behandeling genomen. Andere casussen worden doorverwezen naar het meest aangewezen knooppunt of de meest aangewezen partij.
- Het werkproces zelf 'filtert naar maatwerk' met betrekking tot de te betrekken partijen én de te verwerken gegevens.
- In elke fase van het werkproces (deze worden in de volgende paragraaf beschreven) is duidelijk wat het doel is van die concrete stap, om zo tot een goede maatvoering te komen van de noodzakelijke gegevens en de te betrekken partijen.
- Er zijn expliciete afwegingsmomenten bij de overgang tussen fasen over de gegevens die noodzakelijk zijn om mee te nemen naar de volgende fase.
- Van elke partij is steeds duidelijk op grond van welke taak die betrokken wordt in de verschillende fasen.
- Er zijn afspraken om het gebruik van de gegevens uit de samenwerking door individuele partners te reguleren.

Als het knooppunt een **meldpunt** is zijn de uitgangspunten vergelijkbaar. Als er sprake is van een integraal meldpunt voor bijvoorbeeld Wvggz, en Zorg en Overlast, is de eerste stap een triage om te bepalen in welk juridisch kader de melding wordt opgepakt. Beide meldpunten kennen immers een eigen wettelijk kader. Vaak is het proces in een meldpunt compacter omdat het niet is gericht op casusbehandeling, maar op doorgeleiding naar een specifieke instantie of ander knooppunt.

Door het werkproces voor een overlegtafel of een meldpunt in fasen op te splitsen, kunnen de betrokken partijen de privacyrisico's voor de betrokkene beperken. Voor het toetsen aan de criteria zijn bijvoorbeeld niet heel veel gegevens nodig. En door eerst te bepalen welke partijen noodzakelijk zijn voor de specifieke casus, voorkom je dat je gevoelige gegevens bespreekt met partijen die niets met de casus te maken hebben. Daarbij moet er wel ruimte zijn voor voortschrijdend inzicht. Het gaat immers om complexe casuïstiek. Hoe een stapsgewijze benadering en spelregels daar ruimte voor bieden, wordt in de volgende paragrafen duidelijk.

Reflecteren en leren

Een belangrijk onderdeel van zorgvuldigheid is reflecteren en leren. Reserveer regelmatig tijd om de samenwerking en effectiviteit van het knooppunt te evalueren en verbeteren. En maak de gegevensverwerking hier expliciet onderdeel van.

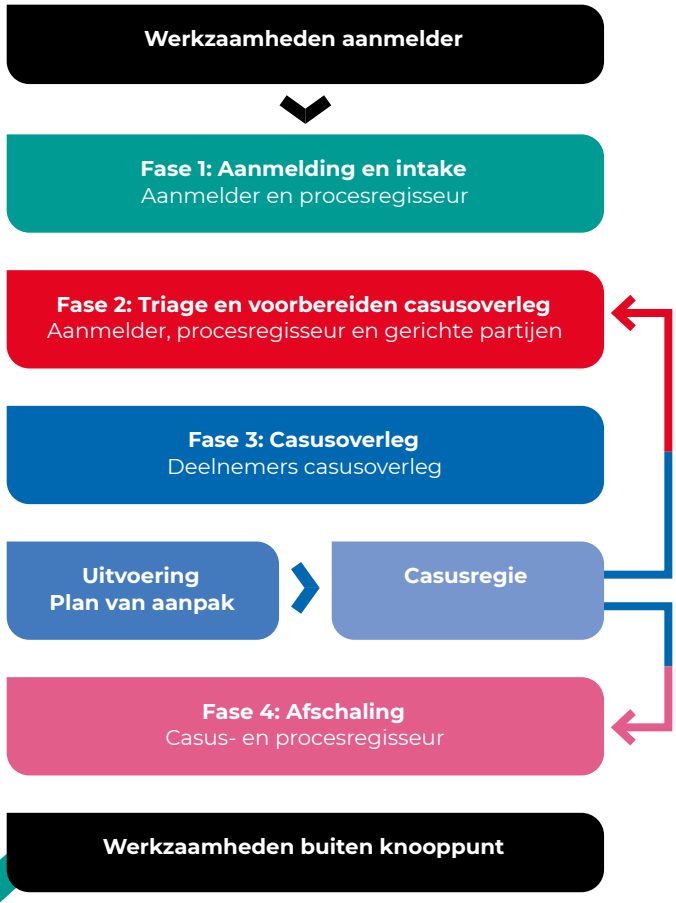
Vragen die hierbij aan bod komen zijn:

- Werken we goed samen en durven wij elkaar aan te spreken?
- Delen we te gemakkelijk gegevens of zijn we juist te voorzichtig?
- Bereiken we de gestelde doelen?
- Hoe effectief is het werkproces: werken de fasering en de werkafspraken nog, zijn we niet te bureaucratisch geworden?
- Hebben we de juiste balans tussen waarborgen voor de cliënt en het effectief oplossen van problemen?
- Werken we nog steeds vanuit respect voor de cliënt en respect voor elkaars kaders?

4.3 Een generiek werkproces

In deze paragraaf behandelen we een generiek werkproces voor knooppunten waarin meerdere partijen casusoverleg voeren. In de bijlage zijn varianten op het generieke werkproces opgenomen met aandachtspunten voor specifieke doelen zoals groepsaanpak, vroegsignalering en meldpunten.

De uitgangspunten van paragraaf 4.2 zijn te vertalen naar een werkproces in vier fasen: aanmelding en intake, triage, casusoverleg en monitoring, afsluiten of overdragen. Voor een zorgvuldig werkproces is het noodzakelijk om alle stappen te doorlopen. We behandelen de verschillende fasen met hun doelen en de te verwerken gegevens per fase.



Figuur 3. Visuele weergave van het werkproces van een knooppunt. De activiteiten die voor en na de werkzaamheden in het knooppunt plaatsvinden, zijn in zwart weergegeven.

Fase 1: Aanmelding en intake

Het doel van de aanmelding en intake is om te bepalen of een casus in het knooppunt thuishoort of niet. Samen met de aanmelder wordt beoordeeld of de casus past binnen de criteria voor de samenwerking. In deze fase worden dus alleen gegevens verwerkt om te toetsen aan die criteria. In principe gebeurt dat op basis van de informatie van de aanmelder. Eventueel kunnen ook gegevens waarover het knooppunt zelf al beschikt, benut worden. Bijvoorbeeld om te checken of de persoon al in behandeling is bij het knooppunt. Er worden nog geen uitgebreide analyses gemaakt en er wordt geen brede uitvraag gedaan bij andere organisaties.

Het resultaat van deze fase is:

- De casus hoort hier thuis en wordt doorgezet naar fase 2: de triage.
- De casus hoort hier niet thuis. De casus wordt niet in behandeling genomen en teruggegeven aan de aanmelder (eventueel met een advies). De gegevens worden vernietigd of volledig geanonimiseerd.
- Het beeld is nog niet eenduidig. Er is voldoende reden om aan te nemen dat de casus waarschijnlijk in het knooppunt thuishoort, maar de triagefase moet uitwijzen of dat daadwerkelijk zo is. De casus wordt doorgezet naar fase 2. Met als eerste doel: bepalen of de casus thuishoort in het knooppunt of niet.

Fase 2: Triage

Het doel van de triage is om in het knooppunt op hoofdlijnen een beeld te vormen van de aard en omvang van de problematiek in de casus, en van de partijen die nodig zijn om te betrekken bij het casusoverleg (fase 3). Informatie die in deze fase gedeeld wordt, gaat voornamelijk over de betrokkenheid van partijen en het type probleem waarvoor ze betrokken zijn. Het gaat niet over de specifieke inhoud van de casus.
Hierbij zijn drie vragen relevant:

- Welke problemen spelen er?
- Welke partijen zijn al betrokken bij de casus?
- Welke partijen moeten, gezien de aard van de problematiek, waarschijnlijk nog betrokken worden?

Het resultaat van deze fase is:

- Inzicht in de problematieken die spelen en die van belang zijn om te bespreken in het casusoverleg.
- Inzicht in de partijen die noodzakelijk zijn voor het casusoverleg en op grond van welke taak dat mogelijk is.
- Voortschrijdend inzicht: de casus hoort bij nader inzien niet thuis in dit knooppunt. Bijvoorbeeld omdat blijkt dat twee partijen de casus bilateraal op kunnen pakken. De casus wordt teruggegeven aan de aanmelder met een advies. De gegevens worden vernietigd of volledig geanonimiseerd.

Fase 3: Casusoverleg en monitoring

Het doel van de fase casusoverleg en monitoring is om inzicht te krijgen in de problematiek en het zoeken naar oplossingen In deze fase komt meer inhoudelijke informatie over de casus op tafel. Het casusoverleg valt doorgaans uiteen in de volgende stappen:
Stap 1: Het doorgronden van de casus en de samenhang van de problemen, en het in beeld brengen van de handelingsopties.

Stap 2: Het komen tot een plan van aanpak en afspraken wie wat gaat doen op basis van zijn eigen taken en bevoegdheden. Het plan van aanpak bevat tevens afspraken over monitoring en de casusregie.

Stap 3: Afspraken over wie welke gegevens nodig heeft en mag gebruiken om zijn aandeel in het plan uit te kunnen voeren. Het resultaat van deze fase is:

- Voortschrijdend inzicht: de casus hoort bij nader inzien niet thuis in dit knooppunt. De casus wordt teruggegeven aan de aanmelder met een advies. De gegevens worden vernietigd of volledig geanonimiseerd.
- Een samenvatting van de probleemanalyse.
- Een plan van aanpak en afspraken over het gebruik van gegevens uit het overleg.
- Bijstellen van het plan van aanpak op basis van de monitoring en evaluatie.
- Besluit tot afsluiten of overdragen van de casus, omdat betrokkenheid van het knooppunt niet meer nodig is.

Fase 4: Afsluiten of overdragen

In deze laatste fase worden de behandeling van de casus en de bijbehorende gegevensverwerking afgerond. Het gezamenlijk dossier (inclusief de gegevens-verwerking) wordt gesloten. Er zijn afspraken gemaakt voor het geval een partner signaleert dat er binnen een bepaalde periode terugval optreedt. Na het aflopen van de afgesproken bewaartermijn, wordt het dossier vernietigd, geanonimiseerd of gearchiveerd conform de Archiefwet. Als in het casusoverleg is afgesproken dat de reguliere bewaartermijn wordt verlengd, wordt vastgelegd waarom daartoe is besloten en voor hoelang de verlenging geldt. Na afloop van de verlenging vindt er alsnog vernietiging, anonimisering of archivering conform de Archiefwet plaats.

Bij overdracht van de casus aan een ander knooppunt, bijvoorbeeld van een lokaal team naar een zorg- en veiligheidshuis, spreken de betrokken partijen af wie de casus daar aanmeldt en welke informatie meegegeven kan worden. Aanmelding moet in principe altijd via een van de partners lopen. Een knooppunt heeft zelf meestal geen eigen wettelijke taak, en dus ook geen zelfstandige bevoegdheid om een casus aan te melden. Hier zijn uitzonderingen op. Bijvoorbeeld het meldpunt Veilig Thuis en het meldpunt Wvggz zijn beide wel op een eigen wettelijke taak gebaseerd en kunnen dus zelf meldingen doorzetten naar andere partijen.

Het belang van fasering

Het is belangrijk dat elke fase afzonderlijk wordt doorlopen. Pas nadat een fase volledig is afgerond, wordt overgegaan naar de volgende fase. Dat kan soms heel snel gaan. Bijvoorbeeld omdat vrijwel meteen duidelijk is welke partijen betrokken moeten worden. Het vermengen van de fasen brengt risico's met zich mee en is daarom uit den boze. Er zouden bijvoorbeeld gegevens verzameld kunnen worden rond casussen die helemaal niet in het knooppunt thuishoren. Of er schuiven partijen aan bij het casusoverleg die niets met de casus te maken hebben. De fasering is dus nodig om het werkproces zorgvuldig te maken. Een proces dat niet zorgvuldig is, is altijd onrechtmatig.

4.4 Rechten en plichten

Het beschreven werkproces (paragraaf 4.3) is cruciaal om te kunnen voldoen aan de eisen van rechtmatigheid, noodzaak en proportionaliteit in een concrete casus. Onderdeel van het werkproces is óók dat de betrokkene geïnformeerd wordt over het feit dat er gegevens over hem worden verwerkt in de samenwerking. Tevens wordt duidelijk gemaakt waarom dat zo is en hoe hij zijn rechten kan uitoefenen.

Gezamenlijke verwerkingsverantwoordelijkheid

De AVG geeft de samenwerkende partijen een aantal rechten en plichten. De partijen dienen afspraken te maken, zodat zij hier daadwerkelijk invulling aan geven (artikel 26 AVG). Dat betekent onder andere dat zij vast moeten stellen welke verwerkingen onder de gezamenlijke verwerkingsverantwoordelijkheid vallen. In de regel zijn dat de gegevens die een procesregisseur opslaat in het samenwerkings- of regiedossier. Daarnaast zijn de partijen gezamenlijk verantwoordelijk voor de zorgvuldigheid van de gegevensuitwisseling tijdens het casusoverleg.

Rechten betrokkene

De samenwerkende partijen moeten een contactpunt afspreken voor de betrokkene, zodat deze laagdrempelig gebruik kan maken van zijn AVG-rechten:

- Recht op inzage;
- Recht op correctie;
- Recht op wisseling van gegevens;
- Recht op beperking van de gegevensverwerking;
- Recht van bezwaar tegen de verwerking van gegevens.

Daarbij moeten de samenwerkende partijen afspraken maken hoe zij invulling geven aan hun gezamenlijke plichten op grond van de AVG:

- De informatieplicht;
- De kennisgevingsplicht van correctie of wisseling van gegevens;
- Een procedure voor datalekken.

De AVG kent strikte bepalingen ten aanzien van uitzonderingen op de plichten van de verwerkingsverantwoordelijken en de rechten van betrokkene. Als in een casus zo'n uitzondering wordt toegepast, zullen partijen de noodzaak hiervan moeten onderbouwen. Zo'n uitzondering is in de regel altijd tijdelijk. Zo kan de informatieplicht soms tijdelijk achterwege blijven, bijvoorbeeld vanwege een opsporingsbelang.
In dat geval moet wel duidelijk zijn wanneer er een heroverweging van die uitzondering plaatsvindt.
Samenwerking tussen partijen betekent per definitie een inbreuk op de persoonlijke levenssfeer van de betrokkene. De situatie is voor de betrokkene, vaak gaat het om kwetsbare mensen, al snel moeilijk te overzien. De uitgangspunten van zorgvuldigheid en respect voor de burger vereisen dan ook extra aandacht voor een goede invulling van deze rechten en plichten.

4.5 Partijen met een beroepsgeheim

In de samenwerking kunnen partijen deelnemen die een beroepsgeheim hebben. Voor een medische professional, zoals een huisarts of een GGZ-professional, geldt het medisch beroepsgeheim. Dat is wettelijk geregeld in de WGBO (Wet Geneeskundige Behandelovereenkomst). Voor jeugdhulpprofessionals geldt een beroepsgeheim op grond van de Jeugdwet.

Bij onzorgvuldig handelen lopen medische professionals of jeugdhulpverleners het risico op een tuchtrechtelijke zaak. Ook kunnen zij hun registratie als hulpverlener verliezen. Voor de medische professionals is dat de BIG-registratie en voor de jeugdhulpverleners de SKJ-registratie.

Medische professionals en jeugdhulpverleners zullen daarom in de samenwerking over het algemeen zeer terughoudend zijn in het delen van gegevens over hun cliënt of patiënt. Ze zullen in elk geval geen informatie over de diagnose of de behandeling geven.

De achtergrond van het beroepsgeheim voor medici en jeugdhulpverleners is het beschermen van de vertrouwelijke relatie met de patiënt. In de spreekkamer of tijdens een behandeling moet een patiënt open en vrij kunnen vertellen over zijn of haar situatie. Bij het minste of geringste vermoeden dat die informatie op andere plekken terecht kan komen, is er het risico dat de patiënt niet open wil spreken. Dan faalt de hulpverlening en kan de medische professional of de jeugdhulpverlener zijn werk niet doen. Het beroepsgeheim voor medici en jeugdhulpverleners is daarom wettelijk stevig verankerd en het wordt door de professionals strikt gevolgd.

Op grond van de wet zijn er een paar situaties waarin een professional het beroepsgeheim kan doorbreken:

- **Toestemming**. Dit betekent dat de patiënt ermee instemt dat de medische professional of jeugdhulpverlener bepaalde gegevens deelt in een samenwerkingsverband.
  Let op: toestemming als doorbrekingsgrond voor het (medisch) beroepsgeheim is iets anders dan toestemming in de zin van de AVG. Het is mogelijk dat op grond van de AVG toestemming niet nodig is, bijvoorbeeld omdat de gegevensdeling noodzakelijk is voor de uitvoering van een wettelijke taak. Die wettelijke taak is niet voldoende om het (medisch) beroepsgeheim te doorbreken. Om het beroepsgeheim te doorbreken is dan apart toestemming van de patiënt aan de medische professional of de jeugdhulpverlener noodzakelijk.
- **Conflict van plichten.** Dit betekent dat de professional oordeelt dat het delen van de informatie noodzakelijk omdat er een ander belang is, dat groter is dan het beschermen van de vertrouwelijkheid van de spreekkamer. Bijvoorbeeld als de veiligheid van anderen in gevaar is.
  Let op: de beoordeling of er sprake is van een ‘conflict van plichten’ en of het andere belang zwaarder weegt dan het beroepsgeheim is aan de professional zelf. De samenwerkende partijen kunnen zich niet beroepen op een wettelijk taak of op afspraken in een convenant of iets dergelijks. Als een professional beoordeelt dat het conflict van plichten niet zwaar genoeg weegt om het beroepsgeheim te doorbreken, dan hebben de andere partijen in de samenwerking dat te respecteren.

- **Wettelijke spreekplicht of meldrecht.** In enkele uitzonderingssituaties is in de wet expliciet geregeld dat een medisch professional in een samenwerking informatie kan geven of soms zelfs moet geven. Een arts mag bijvoorbeeld aan Veilig Thuis informatie geven als dat voor een melding nodig is. En in de uitvoering van de Wvggz is de psychiater verplicht bepaalde informatie aan de burgemeester of het OM te verstrekken.

- **Noodsituatie of vitaal belang.** Als er een acuut risico is op levensgevaar of ernstig letsel mag een professional ook gegevens over de patiënt verstekken aan anderen. Ook in deze situatie is het aan de medische professional om te beoordelen of doorbreking van het beroepsgeheim noodzakelijk is.

De handreiking 'Gegevensuitwisseling in de bemoeizorg'[16] bevat een stappenplan voor hoe professionals met een beroepsgeheim toch kunnen deelnemen in een knooppunt:

Stappenplan deelname aan knooppunt door professional met beroepsgeheim

(1) Maak vooraf afspraken op welke manier en onder welke voorwaarden professionals met een beroepsgeheim kunnen deelnemen in de samenwerking of in het knooppunt.
(2) De deelname van de professional met een beroepsgeheim is noodzakelijk voor de samenwerking. De conclusie dat deelname noodzakelijk is, is altijd getrokken op basis van duidelijke signalen of informatie. Bovendien zijn die signalen onderzocht, bijvoorbeeld in een triagefase. Bij het onderzoek of de professional noodzakelijk deelneemt aan de samenwerking, wordt zo mogelijk de patiënt betrokken.
(3) De medische professional of de jeugdhulpverlener informeert de patiënt/cliënt over de deelname aan de samenwerking en vraagt daarvoor toestemming. Als toestemming vragen niet mogelijk is of niet passend is voor de samenwerking, dan neemt de professional deel op grond van 'conflict van plichten'. De medische professional of de jeugdhulpverlener maakt zelf de afweging of het conflict van plichten aan de orde is.
(4) In de samenwerking zoeken de partijen steeds naar de minst ingrijpende vorm van gegevensdeling. Bijvoorbeeld door een casus anoniem te bespreken. De uit te wisselen informatie gaat in het algemeen over hoe te handelen ("hoe kan ik deze cliënt benaderen?", "kan cliënt deze interventie aan?") en niet over de medische behandeling of de diagnose.
(5) Voor het delen van medische gegevens in een casusoverleg of aan een meldpunt geldt hetzelfde als voor de deelname van de professional aan het overleg: de patiënt is geïnformeerd en heeft toestemming gegeven voor de gegevensdeling. Als dat niet kan, vindt de gegevensdeling op grond van 'conflict van plichten' plaats, te beoordelen door de medische professional.
(6) In de samenwerking deelt de professional met een beroepsgeheim zo min mogelijk gegevens en alleen gegevens die strikt noodzakelijk zijn voor de samenwerking. De professional legt in zijn of haar eigen dossier vast welke gegevens zijn gedeeld, met welke partij(en) en met welke reden.

[16] Handreiking Gegevensuitwisseling in de bemoeizorg, GGD GHOR Nederland, GGZ Nederland en KNMG, 2014, www.knmg.nl/download/handreiking-gegevensuitwisseling-bemoeizorg.

5. Zorgvuldigheid borgen in de uitvoering

Hoe zorg je dat de samenwerking met respect voor de betrokken cliënt en met respect voor de andere ketenpartners wordt ingevuld?

Nadat zorgvuldigheid is geborgd in het werkproces, moet het ook in de uitvoering worden geborgd. Daarvoor zijn werkafspraken nodig. Enkele vuistregels of spelregels kunnen daarbij helpen om de professionals houvast te geven voor het zorgvuldig omgaan met persoonsgegevens.

Als de juridische bedding goed is geconstrueerd (hoofdstuk 3), en het werkproces goed is ingericht (hoofdstuk 4), kunnen de professionals, op basis van de inhoud van de problematiek, bepalen welke gegevens noodzakelijk zijn om te delen. De spelregels helpen om dat op een zorgvuldige manier te doen. Ze worden opgesteld aan de hand van een risico-maatregel-analyse.

Een belangrijk onderdeel van het borgen van zorgvuldigheid in de uitvoering is het samen evalueren en leren. Reflectie op de samenwerking en gegevensdeling is daarom essentieel om samen een zo goed mogelijke praktijk te ontwikkelen.

5.1 Risico's en maatregelen

De AVG eist dat er is nagedacht over de privacyrisico's voor de betrokkene. Er moeten maatregelen worden genomen om de kans dat die risico's zich voordoen, te beperken en onnodig negatieve effecten voor de burger te verminderen. Daarom worden eerst op bestuurlijk niveau criteria voor de samenwerking geformuleerd. Daarna is het werkproces ingericht om zoveel mogelijk maatwerk te kunnen bieden met betrekking tot de te betrekken partijen en de te verwerken gegevens. Door middel van een risicoanalyse op de verschillende fasen van het werkproces, kunnen spelregels en werkafspraken voor de uitvoering geformuleerd worden.

Tabel 1 geeft weer hoe zo'n risicoanalyse en de daaraan gekoppelde maatregelen er voor een knooppunt uit zou kunnen zien.

Fase aanmelding	
Risico's	**Maatregelen**
Er worden casussen behandeld die niet in het knooppunt thuishoren en de zwaarte van de gegevensverwerking niet rechtvaardigen.	Heldere criteria voor aanmelding. Aanmelder dient aanmelding te onderbouwen. Knooppunt toetst aanmelding op criteria en verwijst zo nodig terug of door (al dan niet met warme overdracht).
Partijen nemen kennis van gegevens, terwijl zij niet noodzakelijk zijn voor de casus.	In de aanmeldfase worden geen andere partijen betrokken dan de melder, de regisseur van het knooppunt en de persoon waar de melding over gaat.
Er worden gegevens verwerkt zonder dat duidelijk is of deze noodzakelijk zijn.	Aan het eind van elke fase wordt beoordeeld welke gegevens noodzakelijk zijn om te vast te leggen, en welke noodzakelijk zijn om door te zetten naar de volgende fase.
Iemand wordt aangemerkt als 'probleemgeval' terwijl hij niet in het knooppunt thuishoorde en dat dus niet is.	Indien de casus niet thuishoort in het knooppunt, worden geen persoonsgegevens vastgelegd (of worden deze vernietigd/geanonimiseerd).

Fase triage en voorbereiden casusoverleg	
Risico's	**Maatregelen**
Partijen nemen kennis van gegevens, terwijl zij niet noodzakelijk zijn voor de casus.	Zorg voor een getrapte bevraging van de partijen. Bevraag eerst een beperkt aantal partijen (op basis van de informatie van de aanmelder). Pas daarna kunnen andere partijen gericht worden bevraagd.
Partijen verwerken 'vraaginformatie' voor eigen doeleinden, terwijl dat niet de bedoeling is.	Spreek duidelijk af dat de betrokken partijen de 'vraaginformatie' niet vastleggen.
Er worden meer gegevens doorgezet naar de volgende fase dan noodzakelijk.	Aan het eind van elke fase wordt beoordeeld welke gegevens nog noodzakelijk zijn voor de volgende fase.
Iemand wordt aangemerkt als 'probleemgeval' terwijl hij niet in knooppunt thuishoorde en dat dus niet is.	Indien de casus toch niet thuishoort in het knooppunt, worden de gegevens vernietigd/ geanonimiseerd.

Fase casusoverleg en monitoring	
Risico's	**Maatregelen**
Partijen nemen kennis van gegevens, terwijl zij geen betrokkenheid hebben en niet nodig zijn voor de casus.	In triage wordt beoordeeld welke partijen noodzakelijk zijn en vanuit welke rol. Niet nodig, betekent geen deelname.
Er vindt onnodige verspreiding plaats van gegevens uit het casusoverleg onder partijen.	Partijen leggen geen gegevens vast tijdens het overleg. Aan het eind wordt afgesproken wie welke gegevens nodig heeft en mag gebruiken voor hun aandeel in het plan. Geen uitvoerende/regisserende rol, betekent geen gegevens.
Partijen delen informatie niet uit angst de controle kwijt te raken. Dit vergroot het risico op keuze voor een verkeerde interventie.	De partij die gegevens inbrengt, houdt de zeggenschap over die gegevens en beslist of hij gegevens wil/kan verstrekken aan een partij t.b.v. een specifieke taak.
Partijen gebruiken gegevens uit het casusoverleg voor andere doelen dan afgesproken.	Dit is een ernstige schending van het vertrouwen die op bestuurlijk niveau aan de orde moet worden gesteld.
Er ontstaat ongerichte gegevensuitwisseling (bijvoorbeeld via e-mail) tussen alle betrokken partijen.	Gegevensuitwisseling verloopt uitsluitend bilateraal, of via de proces/casusregisseur. Deze beoordeelt in hoeverre anderen de gegevens ook moeten ontvangen.

Fase overdragen en afsluiten	
Risico's	**Maatregelen**
Er wordt meer informatie overgedragen dan noodzakelijk is.	In het casusoverleg wordt besproken welke gegevens noodzakelijk zijn om over te dragen. Er worden alleen gegevens overgedragen als dat voor de gezamenlijke aanpak noodzakelijk is.
Partijen hebben geen controle meer over hoe hun gegevens na overdracht door de ontvangende partij worden gebruikt.	Partijen beslissen zelf over de overdracht van 'hun' gegevens. Er is geen sprake van een 'plicht' tot gegevenslevering. Een partij kan zelf besluiten om de gegevens wel of niet te delen. De ontvangende partij maakt duidelijk waarvoor de gegevens gebruikt zullen worden. De ontvangende partij gebruikt de gegevens alleen als de leverende partij daarvan op de hoogte is en akkoord is met het gebruiksdoel van de gegevens.
Casussen blijven onnodig lang beschikbaar. Of juist te kort, terwijl de aard van de problematiek langer bewaren rechtvaardigde.	Maandelijkse check of dossiers volgens de bewaartermijnen zijn dichtgezet/geanonimiseerd. Langer bewaren vraagt om een specifieke en beargumenteerde afweging. Periodiek wordt geëvalueerd of hier goed mee omgegaan wordt.

Tabel 1: Risico's en maatrelen per fase

Risico's bij andere typen knooppunten

De hierboven opgesomde risico's en maatregelen (tabel 1) zijn vrij generiek gegeven voor toepassing in een knooppunt. In de praktijk zijn bovenstaande risico's en maatregelen vooral van toepassing voor casusoverlegtafels.

Bij een meldpunt kunnen er aanvullende aandachtspunten zijn. Als er door de wet specifieke eisen gesteld zijn aan het meldpunt, zoals bij Veilig Thuis of het meldpunt Wvggz, is er bijvoorbeeld een risico dat er niet goed omgegaan wordt met geheimhoudingsbepalingen die de wet stelt. Dergelijke bijzonderheden kunnen meegenomen worden in de werkafspraken voor dat meldpunt.

Bij een knooppunt dat vooral een signaleringsfunctie heeft (zoals bijvoorbeeld een signaleringsoverleg mensenhandel) is er een belangrijk aanvullend risico. Namelijk dat er breed informatie gedeeld wordt met partijen, zonder dat duidelijk is of er echt iets aan de hand is. Ook bij het verkennen van signalen van huiselijk geweld en kindermishandeling door lokale teams, doet dat risico zich voor. Het gevolg kan dan zijn dat mensen onterecht te boek komen te staan als dader van ernstige feiten. Bij dergelijke knooppunten is extra aandacht voor deze risico's (en de maatregelen om die te voorkomen) van belang.

5.2 Vuistregels voor de behandeling van een casus

Op basis van de in tabel 1 benoemde maatregelen kunnen werkafspraken worden gemaakt. Onderdeel van deze werkafspraken is een setje met vuistregels voor de professionals over wat een zorgvuldige omgang met persoonsgegevens is. Deze spelregels gaan voor elk knooppunt op. Als ze niet worden toegepast, wordt er per definitie onzorgvuldig gewerkt en is de gegevensuitwisseling onrechtmatig.

Vuistregels behandeling casus

Algemeen werkproces

1. Er is sprake van een strikte doelbinding bij de verschillende fasen van het behandelen van casussen.
2. Er worden alleen gegevens verwerkt die voor dat doel noodzakelijk zijn.
3. Als het doel wijzigt, wordt allereerst opnieuw beoordeeld of de eerder verwerkte gegevens ook daarvoor noodzakelijk zijn en gebruikt mogen worden. Zo niet, dan worden deze verwijderd uit de dossiers.

Welke partijen worden wanneer betrokken?

4. Er worden alleen partijen betrokken die noodzakelijk zijn voor het doel van de betreffende fase. Bij de aanmelding van een casus zijn dat bijvoorbeeld alleen de aanmelder en de procesregisseur van een knooppunt. In de triagefase bevraagt de procesregisseur andere partijen een-op-een om telkens bilateraal te beoordelen of zij een bijdrage kunnen leveren aan de casus en uitgenodigd moeten worden voor het casusoverleg. Tijdens het casusoverleg sluiten alleen die partijen aan waarvan tijdens de triage is gebleken dat zij (hoogstwaarschijnlijk) een bijdrage kunnen leveren aan het oplossen van de problematiek.
5. De rollen van de verschillende organisaties worden duidelijk van elkaar onderscheiden en benoemd. Het kan zijn dat een partij alleen wordt uitgenodigd als adviseur of als informant. Het is belangrijk dat dat duidelijk is voor iedereen.

Hoe om te gaan met gegevens in een casusoverleg?

6. Elke deelnemer houdt de zeggenschap over de gegevens die hij/zij inbrengt tijdens het overleg.
7. Het overleg is vertrouwelijk: niemand neemt informatie mee uit het overleg, tenzij dat voor de vervolgacties strikt noodzakelijk is. Deelnemers aan het overleg ondertekenen een geheimhoudingsverklaring. Adviseurs of informanten hebben geen rol in de vervolgacties en nemen dus nooit informatie uit het overleg mee.
8. Aan het eind van het overleg wordt afgesproken wie welke informatie nodig heeft voor zijn of haar aandeel in het vervolg van het plan van aanpak. De informatie mag door de ontvangende partij alleen gebruikt worden voor hetgeen in het plan van aanpak daarover is afgesproken.
9. Deze informatie mag alleen gebruikt worden als degene die de informatie heeft ingebracht daarmee akkoord is.

Deze vuistregels zijn een belangrijk onderdeel van goede werkafspraken. Ze vormen een waarborg om te voorkomen dat informatie uit een casusoverleg in allerlei dossiers terechtkomt en een eigen leven gaat leiden. Uitgangspunt is dat partijen alleen gegevens meenemen die nodig zijn voor hun eigen aandeel in het plan van aanpak. Daar hoort uiteraard ook enige contextinformatie bij, maar niet elke partij heeft bijvoorbeeld ook strafrechtelijke of gezondheidsgegevens nodig.

Een partij kan bijvoorbeeld informatie delen om te komen tot een beter gezamenlijk inzicht in de problematiek, maar of hij die informatie ook mag en wil delen voor specifieke interventies, vergt een aparte afweging. Doordat de partij die de gegevens heeft ingebracht, beslist of een andere partij deze gegevens mag gebruiken voor de afgesproken acties, is geborgd dat elke partij zijn eigen verantwoordelijkheid neemt ten aanzien van de gegevensverwerking en de betrokkene.

5.3 Vuistregels voor het verstrekken van persoonsgegevens

Bij het delen van persoonsgegevens is het van belang om te onderscheiden of het verstrekken van de gegevens onderdeel is van de eigen (wettelijke) taak of dat het onderdeel is van de taak van de ontvanger. Daarnaast is van belang of er sprake is een wettelijk beroepsgeheim. Voor het verstrekken van persoonsgegevens aan een andere partij gelden de volgende vuistregels.

Vuistregels verstrekken persoonsgegevens

- **Eigen taak:** Op grond van de AVG is het doorgaans toegestaan persoonsgegevens te delen als het noodzakelijk is voor de goede uitvoering van de eigen taak. Dat geldt ook als er bijvoorbeeld activiteiten moeten worden afgestemd, of samenwerking nodig is om een probleem op te lossen. In zo'n geval zijn de gegevens noodzakelijk voor zowel de eigen taak als die van de ontvanger. Let wel: dit gaat veelal om coördinatie- of afstemmingsinformatie en dus niet om gedetailleerde dossierinformatie.
- **Taak van de ontvanger:** Als de persoonsgegevens alleen noodzakelijk zijn voor de uitvoering van de taak van de ontvanger, en daarmee losstaan van de taak van de verstrekker en het gemeenschappelijk doel dat deze heeft geformuleerd, dan is delen meestal niet toegestaan. Een uitzondering daarop kan zijn dat er een wettelijke verplichting of bevoegdheid is om gegevens te verstrekken aan de ontvangende partij. Zo is bijvoorbeeld iedereen bevoegd om gegevens te verstrekken aan Veilig Thuis als dat noodzakelijk is om een vermoeden van huiselijk geweld of kindermishandeling te onderzoeken. Zo nodig, zelfs met doorbreking van een wettelijk beroepsgeheim.
- **Wettelijk beroepsgeheim:** Partijen met een wettelijk beroepsgeheim zullen in de regel altijd een extra afweging moeten maken. Ook als het delen van gegevens past bij de goede uitvoering van de eigen taak. In de regel zullen zij toestemming nodig hebben om informatie te delen in alle fasen van het werkproces. Het kan dus voorkomen dat een psychiater in het overleg zegt 'ik kan hier nu niets over zeggen. Ik moet dat overleggen met mijn cliënt'. Dat is dan geen onwil, maar vloeit voort uit de beroepsverantwoordelijkheid. Het is belangrijk elkaar die ruimte te geven.
- Elke partij bepaalt zelf welke gegevens zij inbrengt in het casusoverleg.

Schakelen tussen knooppunten
Het uitwisselen van informatie tussen knooppunten vergt steeds een specifieke afweging. In de eerste plaats is het van belang wat voor type knooppunten betrokken zijn bij de uitwisseling. Betreft het de uitwisseling tussen twee knooppunten die beide op een eigen wettelijke taak gebaseerd zijn, dan is het relatief eenvoudig. Op basis van de eigen juridische kaders is eenvoudig te bepalen met welke andere knooppunten welke informatie uitgewisseld kan worden. Op basis daarvan kunnen instructies opgesteld worden voor de medewerkers.

Is een van de knooppunten een overlegtafel, zoals een casusoverleg in het zorg- en veiligheidshuis of een lokale PGA, dan heeft dat knooppunt geen eigen wettelijke taak op grond waarvan het gegevens kan verstrekken aan derden. Als zo'n knooppunt een casus wil overdragen, bijvoorbeeld van een lokale PGA naar het zorg- en veiligheidshuis, dan zullen daarvoor de zorgvuldigheidsbeginselen uit de AVG moeten worden toegepast. Als eerste moet beoordeeld worden welke partij de meest aangewezen partij is om de casus aan te melden bij het andere knooppunt.

Vuistregels schakelen tussen knooppunten
- Spreek af welke partij de casus aanmeldt bij een ander knooppunt. Baseer de keuze voor een partij op basis van de meest relevante maatschappelijke taak.
- Spreek af welke gegevens noodzakelijk zijn om te verstrekken aan het andere knooppunt.
- De partij die de gegevens heeft ingebracht, bepaalt vervolgens of deze gegevens verstrekt kunnen worden. Zo kan een partij aangeven nu geen gegevens te willen verstrekken, maar bijvoorbeeld rechtstreeks betrokken te willen worden bij de behandeling in het andere knooppunt. Zodat deze partij beter kan beoordelen welke gegevens noodzakelijk zijn.
- Spreek af wie de cliënt informeert over welke persoonsgegevens zijn gedeeld, tussen welke partijen, met welk doel en waarvoor de gegevens wel en niet gebruikt worden.

5.4 Welke informatie krijgen de procesregisseur en professionals?
Professionals hoeven niet alle ins en outs van de juridische onderbouwing van het knooppunt te weten. Voor hen is belangrijk dát ze weten dat er een goede juridische basis is om gegevens te delen in het kader van de samenwerking. Én dat hen dat desgevraagd kan worden uitgelegd. Ook dienen zij goede handvatten mee te krijgen om binnen die kaders zorgvuldig te handelen.

Begrip van de doelen van de samenwerking en de eigen rol en taak daarin, het werkproces en de spelregels uit de vorige paragrafen zijn essentieel. Elke deelnemende partij zal zelf aanvullende handvatten moeten ontwikkelen om de eigen professionals daarin te ondersteunen.

De procesregisseur heeft een belangrijke rol om de zorgvuldigheid in het proces en het naleven van de vuistregels en de werkafspraken te borgen. Kennis van de rollen en verantwoordelijkheden van de verschillende partners is essentieel om het casusoverleg constructief te laten verlopen. Denk onder andere aan de bijzondere positie van partijen die gebonden zijn aan een (wettelijk) beroepsgeheim. In tabel 2 geven we een lijst van onderwerpen die handig zijn om een professional of procesregisseur mee te geven:

Onderdeel	Toelichting
Doel van het knooppunt	• Wat is het doel van het knooppunt? • Welke andere knooppunten hebben vergelijkbare doelen?
Criteria	• Heldere criteria om te toetsen of een casus thuishoort in het knooppunt. • Criteria voor het op- en afschalen naar een ander knooppunt
Gegevensverwerking algemeen	• Uitleg over juridische grondslag. • Mogelijkheden en beperkingen vanuit wettelijke kaders. • Zorgvuldigheid als bouwsteen van rechtmatigheid.
Regisseur van het knooppunt	• Rol en taken van de regisseur als bewaker van zorgvuldigheid.
Betrokken partijen	• Partijen in het knooppunt met hun taken en eventuele bijzonderheden, zoals het beroepsgeheim. • Respect voor verantwoordelijkheden van elke partij.
Werkproces en gegevensverwerking	• Uiteenzetting van de verschillende stappen in het werkproces. • Doelen per fase. • Soort persoonsgegevens dat gedeeld mag worden per fase.
Zorgvuldigheidsafspraken	• De afspraken, het belang ervan, en handelwijze als spelregels niet worden nageleefd door een of meerdere partijen
Vuistregels voor uitwisseling	• Welke informatie kan in verschillende fasen gedeeld worden onder welke voorwaarden?
Bijzondere situaties	• Verschillen van inzicht tussen partijen over wat nodig is/mogelijk is om uit te wisselen. • Bijzondere positie beroepsgeheim.

Tabel 2: Belangrijke onderwerpen om mee te geven

5.5 Houdingsaspecten

Onduidelijkheid over gegevensverwerking is vaak een bron voor onbegrip en handelingsverlegenheid tussen professionals. Met de informatie uit deze handreiking kan al veel meer duidelijkheid geboden worden. Maar, samenwerken blijft mensenwerk. Het draait niet zozeer om de vraag: ‘wat mag en wat mag niet?’ maar om de vraag: ‘hoe komen we samen verder bij het oplossen van de problematiek?’. Dat is ook een kwestie van houding en bejegening van de cliënt.

Nieuwsgierig zijn, met respect voor elkaars positie

Partijen kunnen variëren van inzicht over wat nodig en mogelijk is in een casus. Indien een partij geen gegevens wil delen, wees dan nieuwsgierig naar de reden daarvoor. Het kan zijn dat de partij (nog) geen vertrouwen heeft in de manier waarop wordt omgegaan met de gevraagde gegevens. Misschien is het nog niet helder waarvoor een partij de gegevens wil gebruiken of zijn de afspraken daarover onduidelijk. Een partij kan ook gebonden zijn aan het beroepsgeheim, waardoor er geen gegevens gedeeld mogen worden, zonder daar met de cliënt over gesproken te hebben. Zet elkaar niet onder druk en respecteer de verschillende antwoorden. Laat de beslissing aan de professional met het beroepsgeheim over.

Het is daarbij ook de kunst om de goede vragen te stellen. Vraag bijvoorbeeld om een algemeen bejegeningsadvies, in plaats van naar de medische conditie van een betrokkene. Of vraag geen gegevens, maar vraag wat een partij op basis van zijn eigen taken en bevoegdheden kan bijdragen aan de oplossing van het probleem. Een partij met een beroepsgeheim kan ook vragen terugstellen. Bijvoorbeeld wat de achtergrond is van een bepaalde vraag. Zo kan beter worden beoordeeld op welke manier deze kan bijdragen aan de aanpak.

Openstaan voor (zelf)kritiek
In het sociaal, zorg- en veiligheidsdomein is samenwerking vaak noodzakelijk om zwaarwegende maatschappelijke problematiek op te lossen. Bij samenwerking is het uitwisselen van gegevens onvermijdelijk. Maar wees kritisch op de gegevens die ook echt noodzakelijk zijn om verder te komen. Niet iedereen heeft altijd alle informatie nodig. Uiteindelijk gaat het erom dat partijen een handelingsperspectief hebben dat past bij hun taak en relatie met de betrokkene. Maak die vraag steeds weer expliciet: Als dít het plan is, wie heeft dan welke informatie nodig?

Wanneer partijen uit eigen beweging misschien te veel informatie delen, wijs ze daar dan op. Soms kan het ook voldoende zijn dat partijen een-op-een informatie uitwisselen, buiten een casusoverleg om. Zo voorkom je dat informatie gedeeld wordt met partijen die bepaalde informatie helemaal niet nodig hebben. Wanneer je twijfelt of het verstandig is om bepaalde informatie te delen, neem dan de ruimte om bijvoorbeeld eerst een collega te consulteren. Organisaties die in samenwerkingsverbanden participeren, doen er verstandig aan om hiervoor ook een vraagbaakfunctie in te richten. Deze functie kan worden ingevuld door een persoon die op de hoogte is van het doel van de samenwerking, de rol van de eigen organisatie daarin, en de wijze waarop de organisatie kan bijdragen en gegevens kan delen.

Feedback en reflectie
Gegevensverwerking is een organisatievraagstuk dat van casus tot casus varieert. De kans bestaat dat er soms te veel en soms te weinig persoonsgegevens worden gedeeld. Het is geen schande als er fouten worden gemaakt, zolang er maar van geleerd wordt. Het is daarom van belang om de samenwerking tussen collega's en andere partijen regelmatig te evalueren. Zorg dat er in het werkproces ruimte en tijd is voor feedback en reflectie. Dat draagt bij aan een prettige samenwerking en stelt het knooppunt in staat om effectief te opereren.

5.6 Tot slot

In deze publicatie zijn we uitgebreid ingegaan op de maatschappelijke opgave, het juridische vraagstuk, de zorgvuldige inrichting van de organisatie en de uitvoering met betrekking tot de gegevensverwerking bij samenwerking, en de vragen die daarbij spelen. Het antwoord op deze vragen vormt samen de juridische onderbouwing van het knooppunt.

Je kunt nu onderbouwen welke partijen in een knooppunt vertegenwoordigd zijn en waarom hun deelname noodzakelijk is. Je kunt aangeven wat de verschillende belangen, doelen, verantwoordelijkheden zijn, maar ook welke zorgen organisaties hebben over de samenwerking in het knooppunt. Je kunt onderscheidende criteria opstellen om te bepalen welke casussen in het knooppunt behandeld worden en welke casussen niet bij het knooppunt thuishoren.

Op basis van de intake en triage van een casus, kun je vaststellen welke partijen aan- en afwezig zijn bij de behandeling van een casus en welke rol en taken zij op zich nemen. Je weet wat de mogelijkheden zijn van partijen maar ook welke beperkingen er zijn. Je kunt een zorgvuldig werkproces inrichten waarbij je per casus een afweging maakt tussen noodzaak en proportionaliteit om privacyrisico's zo beperkt mogelijk te houden. Je maakt afspraken op organisatie- en casusniveau over de omgang met persoonsgegevens. Op deze wijze heb je het organisatievraagstuk van het knooppunt van de juiste context voorzien en heb je de basis gelegd voor een rechtmatige uitwisseling van persoonsgegevens.

Meer weten?

Meer informatie is beschikbaar via www.samenvoorzorgenveiligheid.nl. Deze website bundelt gevalideerde producten over privacy en gegevensverwerking.

Zo bevat de site onder andere het *Handvat voor gegevensuitwisseling in het zorg- en veiligheidsdomein*, dat dieper ingaat op de juridische aspecten van verschillende partijen.

Bijlage. Varianten op het generieke werkproces

Om ervoor te zorgen dat professionals zorgvuldig kunnen handelen, moet de gegevensverwerking in het knooppunt goed georganiseerd zijn. Hoofdstuk 4 beschrijft het generieke werkproces voor casusoverleggen, dat is afgeleid van het werkproces voor de zorg- en veiligheidshuizen. Het proces is toepasbaar op overleggen waarin sprake is van meervoudige problematiek, en waar partners gezamenlijk een aanpak moeten formuleren. Denk bijvoorbeeld aan persoonsgerichte aanpakken in een lokale Persoonsgerichte Aanpak (PGA) of in het zorg- en veiligheidshuis.

Deze bijlage schetst drie varianten op het generieke basisproces, gericht op specifieke knooppunten:

1. **Generiek werkproces meldpunten;**
2. **Generiek werkproces (vroeg)signaleringstafels;**
3. **Generiek werkproces groepsaanpak**.

Let op: Deze generieke werkprocessen dienen als hulpmiddel bij het inrichten van een zorgvuldig werkproces, maar vormen slechts één onderdeel van wat nodig is voor een rechtmatige gegevensverwerking. Het blijft essentieel om alle elementen, zoals beschreven in deze publicatie, toe te passen. In het bijzonder moeten de noodzaak tot samenwerking worden onderbouwd en moet de analyse van juridische kaders, evenals de mogelijkheden en beperkingen van de betrokken instanties om gegevens uit de wisselen, grondig worden geanalyseerd.

Bijlage 1.1 Generiek werkproces meldpunten

Voorbeelden
Meldpunt zorgwekkend gedrag, meldpunt Wvggz, meldpunt Veilig Thuis, meldpunt woonoverlast.

Generiek doel: advies en triage
Het doel van een meldpunt is om de melder of gemelde te adviseren en triage uit te voeren. Dit houdt in dat de situatie wordt beoordeeld en wordt doorverwezen naar de instantie of overlegtafel die het best in staat is de probleemsituatie op te lossen. Meldpunten bieden doorgaans zelf geen hulp of interventies aan. Daarom is de gegevensverwerking vaak beperkt. Meldingen kunnen bovendien worden gedaan door zowel professionals als burgers, wat een onderscheidend kenmerk is van meldpunten.

Sommige meldpunten, zoals meldpunt Veilig Thuis en het meldpunt Wvggz, hebben ook een onderzoekstaak, wat een uitgebreidere gegevensverwerking met zich meebrengt. Desondanks blijft het hoofddoel hetzelfde: bepalen welke instantie(s) verantwoordelijk zijn voor het duurzaam oplossen van de probleemsituatie.

Generiek werkproces

Doelen per fase

1. Aanmelding en intake

In deze fase is het doel om een helder beeld te krijgen van de aard van de problematiek. Er wordt beoordeeld of het vraagstuk thuishoort bij het meldpunt of dat er moet worden doorverwezen. De mogelijke uitkomsten zijn als volgt:

- Indien ja: Relevante informatie wordt geregistreerd voor triage.
- Indien nee: Doorverwijzing naar een passend meldpunt of loket vindt plaats.

In sommige gevallen kan de melder direct advies ontvangen, zonder dat het nodig is om persoonsgegevens te verwerken of vast te leggen.

2. Contact met gemelde

Het doel in deze fase is om inzicht te krijgen in het perspectief van de gemelde persoon. Contact opnemen met de betrokkene is altijd van groot belang, maar bij meldpunten is dit cruciaal. Vaak gaat het om vermoedens en niet om vastgestelde feiten, en het is belangrijk om de relatie tussen melder en gemelde goed te begrijpen voordat verdere stappen worden genomen.

3. Triage

De triage bestaat uit drie belangrijke stappen:

a. Bepalen van de vervolgstap op basis van de informatie die in fase 1 en 2 is verzameld. Mogelijke uitkomsten kunnen zijn: advies aan de melder, advies aan de gemelde, of verder onderzoek als dat nodig is. In het geval van verder onderzoek gaat de casus door naar de volgende stap.

b. Nader onderzoek wordt uitgevoerd om vast te stellen naar welke instantie of overlegtafel de casus het best kan worden doorverwezen. Dit kan bijvoorbeeld door gerichte vragen te stellen aan ketenpartners.

c. Doorverwijzing naar de juiste instantie of overlegtafel die de casus verder oppakt. Hierbij is het belangrijk om de gemelde, waar mogelijk, vooraf te informeren en de melder op hoofdlijnen terug te koppelen, gezien de gevoeligheid van de gedeelde informatie.

4. Monitoring

Het monitoren heeft als doel te verzekeren dat de casus is opgepakt en dat er contact is geweest met zowel de gemelde als de melder. Dit zorgt ervoor dat de casus effectief wordt opgevolgd.

5. Afsluiten

Bij afsluiting wordt de casus als voltooid geregistreerd, en wordt gezorgd voor een correcte archivering en naleving van de bewaartermijn, in lijn met het wettelijke kader.

Bijlage 1.2 (Vroeg)signaleringstafels

Voorbeelden

Vroegsignaleringstafel risicojongeren of jonge aanwas van criminele groepen, signaleringstafels mensenhandel.

Generiek doel: advies en triage

Vroegsignaleringstafels hebben als doel om probleem- of risicosituaties vroegtijdig te onderkennen en, indien nodig, de juiste instantie of overlegtafel in te schakelen voor ondersteuning of interventie. Door (zachte) signalen van diverse partijen samen te brengen, kan gezamenlijk worden geïnterpreteerd of er daadwerkelijk sprake is van een probleem. Deze tafels zijn vooral belangrijk bij problematiek waar de informatie en perspectieven van meerdere partijen nodig zijn om een volledig beeld te krijgen, bijvoorbeeld wanneer een school gedragingen van een leerling signaleert die kunnen wijzen op crimineel gedrag, maar daar niet goed zicht op krijgt.

Specifieke aandachtspunten vanuit privacy en gegevensdelingsperspectief

Bij (vroeg)signaleringstafels gaat het om vermoedens van problematisch of risicogedrag, niet om vaststaande feiten. Daarom is signalering een zeer gevoelig proces dat zorgvuldigheid vereist. Het is belangrijk te voorkomen dat mensen ten onrechte worden aangemerkt als probleemgeval, slachtoffer of crimineel. De zorgvuldigheid van het interne signaleringsproces binnen de organisatie die de casus wil bespreken is minstens zo belangrijk als het proces van de signaleringstafel zelf. Voorkomen moet worden dat signalen 'zwerven' en ongecontroleerd terechtkomen in de dossiers van andere partners.

Generiek signaleringsproces en aandachtspunten voor zorgvuldigheid
Het generieke signaleringsproces, zoals hieronder schematisch weergegeven, bevat de stappen die essentieel zijn om zorgvuldigheid te waarborgen in het vroegsignaleringstraject. Dit proces is gebaseerd op benaderingen voor vroegsignalering van risicojongeren in verschillende gemeenten.

Interne signalering partners

Doel: toetsen signalen en noodzaak aanmelding signaleringstafel.
- Welke signalen?
- Toetsen we die zorgvuldig?
- Bespreken met betrokkene (bijv. jongere, ouders).
- Wat kunnen we zelf?
- Hanteren we criteria voor aanmelden signaleringstafel?
- Informeren betrokkene over aanmelding signaleringstafel.
- Op basis van welke taak melden we aan?
- Hoe beschermen we de betrokkene tegen vooroordelen en stigmatisering?

Aanmelding en intake: weging

Doel: bepalen of signalen serieus genoeg zijn om aan signalentafel te bespreken.
- Overleg tussen melder-regisseur, bij voorkeur in eerste instantie anoniem.
- Toetsen aan criteria.

Triage

Doel: bepalen of casus geagendeerd moet worden en met welke partners.
- Bevragen partners.
- Hebben jullie ook signalen?
- Agenderen ja/nee?
- Bepalen welke partners voor overleg.
- Hoe betrekken we de betrokkene?
- Informeren betrokkene over overleg.

Signaleringstafel

Doel: wegen signalen, doorgeleiden naar juiste instantie/overlegtafel.
- Vooral 'dat-gegevens'+ signalen.
- Hoe beschermen we de betrokkene tegen vooroordelen en stigmatisering?
- Niemand neemt gegevens van mee uit het overleg.
- Uitsluitend de regisseur legt noodzakelijke gegevens vast t.b.v. doorgeleiding.
- Informeren betrokkene over uitkomst.
- AVG-verantwoordelijkheid en rechten betrokkene(n).

Vervolg-trajecten

Afsluiten signalerings-proces

- Casus registreren als afgesloten.
- Bewaartermijn en archivering conform wettelijk kader.

Bijlage 1.3 Groepsaanpak

Voorbeelden
Het meest bekende voorbeeld is de Aanpak problematische jeugdgroepen. Hiervoor is zowel een modelconvenant als een 7-stappenmodel voor jeugdgroepen ontwikkeld. Ook andere vormen van groepsaanpakken, zoals de aanpak van problematische voetbalsupportersgroepen en criminele familienetwerken, vallen hieronder.

Generiek doel
Het doel van groepsaanpakken is om het problematisch groepsgedrag terug te dringen en uiteindelijk te beëindigen, en nieuwe aanwas te voorkomen. Bij jeugdgroepen omvat de aanpak bijvoorbeeld de volgende interventies:

- Gebiedsgerichte interventies, zoals cameratoezicht en extra toezicht door politie en BOA's op specifieke locaties.
- Groepsgerichte interventies, zoals het aanbieden van activiteiten, het bevorderen van ander gedrag bij groepsleden, en het losweken van meelopers door groepsdynamische interventies.
- Individu-gerichte aanpakken, variërend van het inschakelen van jeugdhulp via aanmelding bij het college van B&W, het doorverwijzen naar een lokale persoonsgerichte aanpak of het zorg- en veiligheidshuis, tot strafrechtelijke vervolging van individuele groepsleden als dat nodig is.

Specifieke aandachtspunten vanuit privacy- en gegevensdelingsperspectief
Een typisch risico bij groepsaanpakken is dat groepsgerichte en individuele aanpakken door elkaar gaan lopen. Hierdoor kan een overleg over een groep ontaarden in een breed 'multi-casusoverleg' over individuele groepsleden, waarbij partijen betrokken raken die slechts met één of enkele groepsleden te maken hebben. Dit leidt ertoe dat gevoelige informatie over individuele groepsleden onnodig, en daarmee onrechtmatig, bij veel partijen terechtkomt.

Om dit risico te beperken, is in het modelconvenant en het 7-stappenmodel voor de aanpak van jeugdgroepen gekozen voor een groepsoverleg met een beperkt aantal vaste deelnemers. Deze deelnemers hebben vanuit hun taken een rol in interventies op het niveau van de groep en de groepsdynamiek, zoals de afdeling Openbare Orde en Veiligheid van de burgemeester, de politie, (jeugd)BOA's, het Openbaar Ministerie, en buurt- of jongerenwerkers. In dit groepsoverleg worden alleen analyses op groepsniveau besproken, gebaseerd op signalen, eigen informatie, en gesprekken met individuele leden en eventueel hun ouders.

Als de situatie van een individueel groepslid aanleiding geeft tot verdere actie, wordt deze persoon aangemeld voor individuele zorg, ondersteuning of een persoonsgerichte aanpak binnen Zorg en Veiligheid. Pas in het kader van een PGA-aanpak (Persoonsgerichte Aanpak) worden gegevens op maat gedeeld tussen de verschillende betrokken domeinen, met als doel een passende aanpak voor het individu te realiseren. De toelichting bij het modelconvenant biedt richtlijnen om zorgvuldig af te stemmen tussen de groepsaanpak en de persoonsgerichte aanpak waar dat nodig is.

Onderstaand proces biedt een vereenvoudigde weergave van het modelconvenant en het 7-stappenmodel voor jeugdgroepen. Deze benadering biedt ook waardevolle handvatten voor andere groepsaanpakken.

Generiek proces groepsaanpakken

Signalering problematisch groepsgedrag bijvoorbeeld door organisaties in wijk of buurt

Aanmelding en intake

Doel: bepalen of signalen serieus genoeg zijn om de groep te bespreken in groepsoverleg.

- Overleg tussen melder-regisseur, bij voorkeur in eerste instantie anoniem.
- Toetsen aan criteria.
- Uitsluitend gegevens op groepsniveau.

Groepsoverleg beperkt aantal vaste partners

STAP 1
Doel: Beoordelen signalen aangevuld met eigen waarnemingen.

STAP 2
Doelen indien noodzakelijk:

- Duiden groep
- Vaststellen leden van de groep
- Informeren leden van de groep

STAP 3
Komen tot een plan van aanpak:

- Analyse groepsdynamiek
- Interventies op groepsniveau
- Interventies op individueel niveau door vaste deelnemers
- Triageren geselecteerde groepsleden naar individuele ondersteuning of PGA zorg en veiligheid
- Informeren betreffende leden

STAP 4
Monitoren aanpak en afstemming met individuele PGA's.

Afsluiten groepsaanpak

- Aanpak groep registreren als afgesloten.
- Individuele leden informeren over afsluiting groepsaanpak, of als ze niet meer als groepslid gezien worden.
- Bewaartermijn en archivering conform wettelijk kader.

KEN!
Wij richten ons op het oplossen van privacy- en gegevensdelingsvraagstukken in het sociaal, zorg- en veiligheidsdomein. Door netwerken van professionals en organisaties te vormen en te faciliteren, ontwikkelen zij samen kennis en oplossingen voor de inrichting van gegevenswerking bij samenwerking rond deze complexe maatschappelijke vraagstukken.
KEN! is onderdeel van Platform Sociaal Domein.

Heeft u vragen over deze publicatie?
Neem contact met ons op via
contact@samenvoorzorgenveiligheid.nl.

www.platformsociaaldomein.online
Nassaulaan 12, 2514 JS Den Haag
Postbus 30435, 2500 GK Den Haag