



Persoonsgerichte aanpak voorkoming radicalisering en extremisme

Handleiding voor gemeenten, politie,
Openbaar Ministerie en ketenpartners

Persoonsgerichte aanpak voorkoming radicalisering en extremisme

Handleiding voor gemeenten, politie, Openbaar Ministerie en ketenpartners

Inhoudsopgave

1	Inleiding	3
1.1	Achtergrond	3
1.2	Doel en doelgroep	3
1.3	Leeswijzer	3
2	Werkproces	4
2.1	Weergave werkproces	4
3	Weegploeg: beoordeling signalen en bepalen vervolgstappen	5
3.1	Stroomschema	5
3.2	Rol weegploeg	5
3.3	Rol uitvoerder	6
3.4	Beslissingen Weegploeg	6
	Beslissing 1: Casuswaardig	6
	Beslissing 2: Benodigde casuspartners	6
	Beslissing 3: Informeren betrokkene	7
4	Casusoverleg: plan van aanpak	8
4.1	Stroomschema	8
4.2	Casusoverleg	9
4.3	Uitvoerder	9
4.4	Taken	10
5	Informatieplicht en rechten betrokkene	11
5.1	Toelichting	11
5.2	Informeren betrokkene	11
5.3	Rechten van betrokkenen	13
5.4	Uitvoeren verzoeken rechten van betrokkenen: toepasselijk recht	13
6.	Informatiebeveiliging	16
6.1	Informatiebeveiliging	16
6.2	Datalekken	16
6.3	Bewaartermijnen	17
7	Referentiekader	18
	Bijlage I Gehanteerde begrippen	19

1 Inleiding

1.1 Achtergrond

In de Nationale contraterrorismestrategie 2016-2020 is de inzet van het kabinet en de lokale partners voor de komende jaren weergegeven. Onderdeel van de nationale aanpak van terrorisme en extremisme is een multidisciplinair casusoverleg in alle betrokken gemeenten, dat is gericht op het voorkomen van radicalisering en op de- radicalisering van diegenen die er reeds extremistische denkbeelden op nahouden. Waar dit voor de casuïstiek noodzakelijk is, werken de betrokken landelijke en lokale partijen intensief samen in een casusoverleg. De deelnemende casuspartners wisselen daar waar nodig en mogelijk informatie uit en stellen aan de hand daarvan een integraal plan van aanpak op. Voor de totstandkoming en uitvoering van het integraal plan van aanpak is het noodzakelijk en onvermijdelijk dat partners relevante gegevens, waaronder ook persoonsgegevens, verwerken.

De Algemene Verordening Gegevensbescherming (AVG) stelt strikte voorwaarden aan het delen/verwerken van (bijzondere) persoonsgegevens.

Ten behoeve van deze samenwerking is het (model)convenant persoonsgerichte aanpak voorkoming radicalisering en extremisme (Modelconvenant) opgesteld. Deze procesbeschrijving maakt daar integraal onderdeel van uit.

Met de invoering van de AVG per mei 2018 wordt van de verwerkingsverantwoordelijke meer transparantie en verantwoording gevraagd dan onder de Wet Bescherming Persoonsgegevens (Wbp) gekregen. Zo is in algemene bewoordingen vastgelegd dat de verwerkingsverantwoordelijke passende maatregelen moet treffen om aan te tonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG en de Uitvoeringswet AVG (UAVG) wordt uitgevoerd (artikel 24 AVG). Deze maatregelen moeten in verhouding staan tot de verwerkingen. Hoe risicovoller of privacygevoeliger de gegevensverwerking, hoe strenger de beschermingsmaatregelen moeten zijn. Enkele verplichtingen voor de verwerkingsverantwoordelijke zijn nieuw. Zo wordt de meldplicht voor verwerkingen wordt onder de AVG vervangen door de verplichtingen om verwerkingen vast te leggen in een verwerkingsregister. Dit geldt ook voor de verwerkingen die op grond van dit samenwerkingsverband worden gedaan..

Voor het overige wordt verwezen naar de handleiding Algemene Verordening Gegevensbescherming, te vinden op www.rijksoverheid.nl.

Met de invoering van de AVG zijn ook de rechten van de betrokkene versterkt. In Hoofdstuk 5 van deze handleiding wordt hier nader op ingegaan.

1.2 Doel en doelgroep

Het doel van het Modelconvenant is het waarborgen van een rechtmatige en zorgvuldige verzameling en verwerking van gegevens binnen de persoonsgerichte casusaanpak voorkoming radicalisering en extremisme

Het doel van de procesbeschrijving is:

1. Het beschrijven en toelichten van de werkwijze die ten grondslag ligt aan het modelconvenant in een praktische handreiking voor de convenantpartners en partijen met een rol in de persoonsgerichte casusaanpak voorkoming radicalisering en extremisme.
2. Het bevorderen van een landelijk uniforme werkwijze met betrekking tot de persoonsgerichte aanpak voorkoming radicalisering en extremisme.

Deze procesbeschrijving is ontwikkeld in samenspraak tussen de NCTV, de Nationale Politie, het Openbaar Ministerie, de G4 (namens de priogemeenten), de Raad voor de Kinderbescherming en Reclassering Nederland. Zij zijn hierbij ondersteund door het COT Instituut voor Veiligheids- en Crisismanagement.

1.3 Leeswijzer

Hoofdstuk 2 bevat een schematische weergave van het werkproces van de persoonsgerichte aanpak. De hoofdstukken 3 en 4 bevatten de uitwerking van de processtappen. Per stap een uitwerking van de volgende onderwerpen:

1. **Stroomschema:** de beslismomenten die doorlopen dienen te worden.
2. **Rollen:** de rollen van de weegploeg, het casusoverleg en de uitvoerder.
3. **Beslissingen:** per beslismoment een toelichting op de keuzesopties.
4. **Randvoorwaarden:** een beschrijving van de randvoorwaarden waaraan dient te worden voldaan, zodat de aanpak in lijn is met het Modelconvenant.

2 Werkproces

2.1 Weergave werkproces

Hieronder een weergave van het werkproces. De afzonderlijke stappen worden in de volgende hoofdstukken toegelicht.

Convenantspartijen en externe casuspartners

Bij de opstelling van het convenant is zoveel als mogelijk gekozen voor landelijk opererende partijen.

Het convenant kent 'Kernpartijen' bestaande uit de gemeente, het Openbaar Ministerie en de Politie en 'casuspartijen' bestaande uit de Raad voor de Kinderbescherming en de Reclassering Nederland.

Daarnaast zijn er nog andere partners, de zogenaamde 'externe casuspartners', die een belangrijke rol kunnen spelen in het opstellen, uitvoeren en monitoren van het plan van aanpak binnen de casusaanpak maar waar niet op voorhand van kan worden gesteld welke van deze partijen nodig zijn om tot een persoonsgerichte aanpak te komen. Deze partners zijn geen partij bij het convenant maar kunnen wel deelnemen aan casusoverleg met inachtneming van de hierna verder uitgewerkte randvoorwaarden. De convenantspartijen en de externe casuspartners zijn tezamen de "casuspartners". Op deze manier wordt voorkomen dat er onnodig, zeer gevoelige informatie, met teveel partijen wordt gedeeld.

Type casuspartners	Wie?
1. Kernpartijen (convenantpartijen)	Gemeente, Openbaar Ministerie en de Politie
2. Casuspartijen (convenantpartijen)	Raad voor de Kinderbescherming, Reclassering Nederland
3. Externe casuspartners (geen convenantspartij)	Diverse (zorg)organisaties

De externe casuspartners dienen een geheimhoudingsverklaring te ondertekenen. Door de kernpartijen wordt op lokaal niveau in een bijlage bij het convenant, van te voren vastgesteld welke externe casuspartners kunnen deelnemen aan een casusoverleg. Per casusoverleg wordt dan besloten of betrokkenheid van deze partners noodzakelijk is.

Startpunt: signalen

Startpunt van het proces is het door of via de politie, Openbaar Ministerie en gemeente gezamenlijk analyseren en beoordelen van signalen ten aanzien van een persoon die kunnen duiden op radicalisering of extremisme. Deze gezamenlijke analyse heeft betrekking op signalen waarover de genoemde partijen reeds vanuit de eigen informatiesystemen beschikken alsmede signalen die door tussenkomst van deze partijen zijn ontvangen, waarbij gedacht kan

worden aan een melding via een meldpunt radicalisering of een zorgmelding van:

- Ouders/vrienden/familie
- Maatschappelijke organisaties
- Instanties zoals jeugdwerk en jeugdhulpverlening.

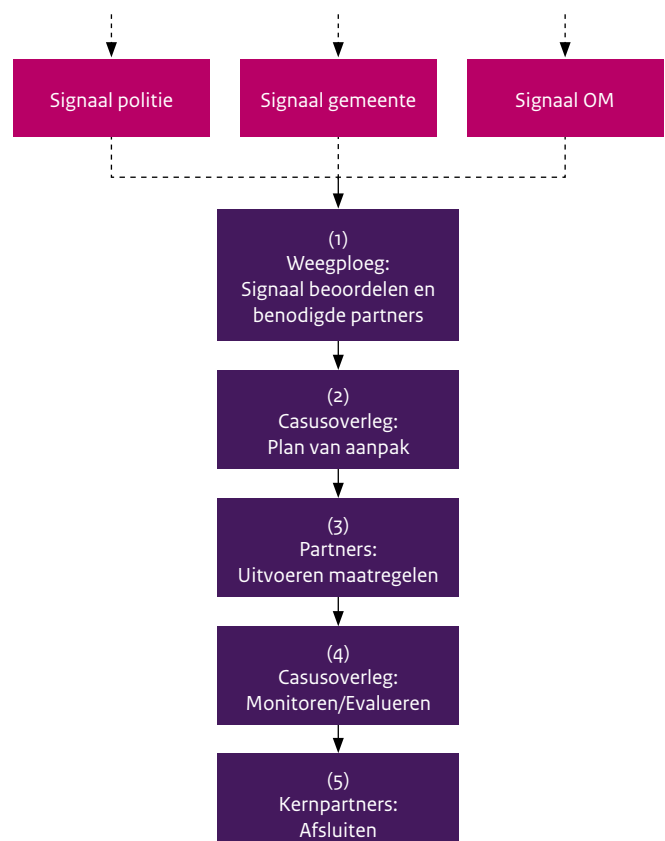
Hierbij is het mogelijk dat er met betrekking tot de desbetreffende persoon reeds een regulier hulpverleningstraject bestond of nog gaande is.

Beoordeling signalen, casusoverleg en uitvoeren maatregelen

Na de beoordeling van het signaal worden benodigde vervolgvactiteiten bepaald, waaronder de noodzaak voor een casusoverleg en opstellen van een plan van aanpak en uitvoeren van maatregelen. Zie verder hoofdstuk 3 en 4.

Eindpunt: afsluiten casusaanpak

Eindpunt van het proces is de beslissing van de kernpartijen, na advies van de casusoverleg, tot afsluiten van de casus. Afsluiten betekent dat de *gezamenlijke* casusaanpak voorkomen radicalisering en extremisme wordt beëindigd. Een eventueel reeds bestaand hulpverleningstraject kan daarbij overigens gewoon doorlopen.



3 Weegploeg: beoordeling signalen en bepalen vervolgstappen

3.1 Stroomschema

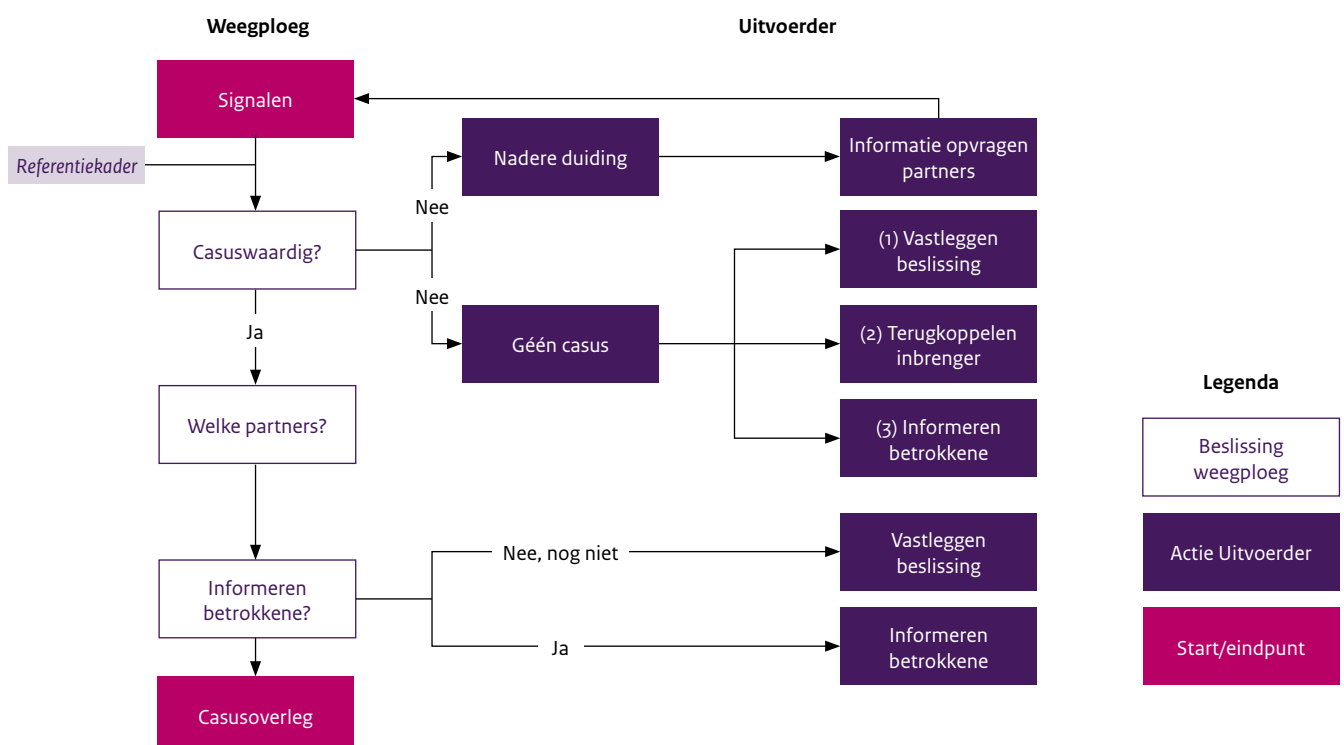
Hieronder staan de verschillende keuzemomenten (en uitkomsten) in het proces weergegeven. In de volgende paragrafen worden de betrokken actoren (weegploeg, uitvoerder) en keuzes nader toegelicht.

3.2 Rol weegploeg

De weegploeg beoordeelt op basis van het referentiekader de feitelijke gedragingen die mogelijkwijds duiden op radicalisering, extremisme en/of uitreizen. Op basis van de beoordeling van deze signalen beslist de weegploeg of een casusoverleg nodig is, en welke casuspartners hierbij betrokken dienen te worden.

De weegploeg bestaat uit de gemachtigde vertegenwoordiger(s) van de kernpartijen:

- de betreffende gemeente
- Politie
- OM



3.3 Rol uitvoerder

Voor de feitelijke uitvoering van de verplichtingen van de kernpartijen wordt een uitvoerder aangewezen. De uitvoerder heeft tot taak namens de kernpartijen op een zorgvuldige wijze uitvoering te geven aan de taken die voortvloeien uit de **AVG** en verricht alle voorbereidende werkzaamheden ten behoeve van de weegploeg en het casusoverleg.

In de praktijk kan de uitvoerder werkzaam zijn bij bijvoorbeeld een gemeente of een Veiligheidshuis. Ook kan er voor worden gekozen om twee uitvoerders aan te stellen: één voor de weegploeg en één voor het casusoverleg. De werkzaamheden voert de uitvoerder echter uit namens de kernpartijen.

Ten aanzien van de weegploeg vervult de uitvoerder de volgende taken:

- Ambtelijk secretaris van de weegploeg (beslissingen vastleggen).
- Aanmaken van een (digitaal) bestand in een beveiligd systeem voor de weegploeg. In het bestand worden beslissingen van de weegploeg vastgelegd (inclusief gehanteerde argumenten) en de informatie die heeft geleid tot beslissing. Tevens bevat het bestand de gegevens zoals omschreven in artikel 8 van het convenant.
- Het namens de kernpartijen opvragen van nadere (duidelings) informatie. Dit indien en voor zover bestaande signalen onvoldoende zijn om te kunnen afwegen of de signalen casuswaardig zijn. *Let op: De afweging casuswaardig of niet berust bij de weegploeg, niet bij de uitvoerder.*
- Informeren van de betrokkene die wordt besproken in de weegploeg:
 - indien wordt besloten betrokkenen niet te agenderen in het casusoverleg;
 - tenzij één van de uitzonderingen genoemd in artikel 41 UAVG van toepassing is. Zie verder: § 5.1 Informeren van betrokkene.
- Vastleggen van de beslissing over het informeren van de betrokkene (en de wijze van informeren).

Als wordt gekozen om een externe partij (niet zijnde een natuurlijk persoon) aan te wijzen als verwerker als bedoeld in artikel 4 aanhef onder 8 AVG, zoals GCOS, dan is het noodzakelijk om een verwerkersovereenkomst op te stellen.

Artikel 28 van de AVG bevat nadere regels hieromtrent.

3.4 Beslissingen Weegploeg

Beslissing 1: Casuswaardig

De signalen die (via een van de partners) bij de weegploeg binnenkomen worden in de weegploeg besproken. De weegploeg beoordeelt het signaal aan de hand van het referentiekader.

De weegploeg maakt de keuze welke opvolging nodig is. Er zijn drie opties, namelijk:

1. Casusoverleg: zie verder beslissing 2
2. Geen casusoverleg: zie verder ad 2
3. Nadere duiding: zie verder ad 3

ad 2. Geen casusoverleg

Indien geen casusoverleg nodig is, worden de volgende acties genomen:

1. De beslissing (om niet te agenderen) wordt vastgelegd door de uitvoerder in de casusnotulen van de weegploeg.
2. De oorspronkelijke aanbrengrer van informatie wordt (door de partner die het signaal inbrengt in de weegploeg) geïnformeerd over de beslissing.
3. De betrokkene wordt geïnformeerd door de uitvoerder, tenzij 1 van de uitzonderingen genoemd in artikel 41 UAVG van toepassing is.

ad 3: Nadere duiding

Indien een nadere duiding nodig is, worden de volgende acties genomen:

1. De uitvoerder verzamelt (slechts) die informatie bij relevante partners die noodzakelijk is voor de weegploeg om een afweging te kunnen maken of de betreffende casus casuswaardig is.
2. De uitvoerder agendaert de casus vervolgens voor een nieuwe beoordeling door de weegploeg.

Beslissing 2: Benodigde casuspartners

Indien een casusoverleg nodig is, bepaalt de weegploeg op basis van de beschikbare informatie welke partners nodig zijn voor het casusoverleg. Alleen die casuspartners die een rol kunnen spelen in het plan van aanpak worden uitgenodigd voor het casusoverleg.

Naast de kernpartijen kunnen de volgende casuspartners uitgenodigd worden:

Raad voor de Kinderbescherming

De Raad voor de Kinderbescherming kan worden betrokken bij een casus indien:

1. radicalisering een bedreiging voor de ontwikkeling van de minderjarige vormt.(art. 255 BW)

De kinderrechter kan een minderjarige onder toezicht stellen van een gecertificeerde instelling indien:

- een minderjarige zodanig opgroeit dat hij in zijn ontwikkeling ernstig wordt bedreigd, en
- de zorg die in verband met het wegnemen van de bedreiging noodzakelijk is voor de minderjarige of voor zijn ouders of de ouder die het gezag uitoefenen, door dezen niet of onvoldoende wordt geaccepteerd.

2. Een proces verbaal is opgemaakt wegens strafbaar gedrag dat aan radicalisering gerelateerd is.

De RvdK geeft het OM en rechter een pedagogisch passend strafadvies.

Het is overigens mogelijk dat de Raad al betrokkenheid bij een minderjarige heeft voordat er sprake is van een geïntegreerde casusaanpak.

De Raad kan in het casusoverleg op 2 manieren deelnemen:

- als algemeen casusadviseur op geanonimiseerde basis. Hierdoor is het informeren van de betrokkene door de Raad van de Kinderbescherming niet direct noodzakelijk; en
- als inhoudelijk betrokken partij, bijvoorbeeld indien onderzoek door de Raad nodig is. In dit geval is de Raad verplicht om de betrokkenen te informeren (indien de Raad al betrokkenheid had bij een minderjarige is deze dus vanzelfsprekend al op de hoogte van de inmenging van de Raad).

Reclassering

De Reclasseringsinstellingen hebben tot taak bij te dragen aan de veiligheid van de samenleving door het beheersen van risico's en om een veroordeelde of verdachte te stimuleren zijn of haar gedrag te veranderen. Op die manier werken zij aan het voorkomen van criminaliteit en het terugdringen van recidive. De reclasseringsinstellingen voeren taakstraffen uit en houden toezicht op maatregelen en ander beslissingen van justitiële instanties. Haar taken bij geradicaliseerde personen worden verricht door een specialistisch landelijk georganiseerd team. Dit team is toegerust om de specifieke signalen van radicalisering te herkennen en daarop te acteren.

Externe casuspartners

Naast de vijf partijen uit het convenant is het natuurlijk goed mogelijk dat ook andere partners over relevante informatie beschikken ten aanzien van een casus of een rol kunnen spelen bij de aanpak van radicalisering. Hierbij kan worden gedacht aan bijvoorbeeld zorgpartijen of deskundigen zoals de NCTV en de IND. Welke casuspartners nodig zijn dient bij iedere casus afzonderlijk te worden afgewogen. Deze partners kunnen dan deelnemen aan het casusoverleg. Zij zijn betrokken bij het opstellen, uitvoeren en monitoren van het plan van aanpak en kunnen – alles voor zover toegestaan binnen de wettelijke kaders van de betrokken partijen-informatie verstrekken en ontvangen voor zover noodzakelijk.

Voor zowel convenantpartijen als overige partners geldt dat zij slechts deelnemen aan een casusoverleg wanneer zij een rol kunnen spelen in de aanpak van het probleem of beschikken over relevante informatie. Zo heeft de Raad voor de Kinderbescherming bijvoorbeeld geen rol bij meerderjarige casuïstiek en heeft dan ook geen toegang tot het bestand.

Beslissing 3: Informeren betrokkene

Uitgangspunt: informeren, tenzij

Uitgangspunt bij het informeren van betrokkene is “informeren, tenzij...” . De weegploeg overlegt of één van de uitzonderingen genoemd in [artikel 41 UAVG](#) van toepassing is, waardoor het informeren van betrokkene dat hem/haar aangaande informatie wordt verwerkt kan worden uitgesteld.

Zodra de uitzonderingen genoemd in de wet niet langer van toepassing zijn dient betrokkene alsnog te worden geïnformeerd. Dit geldt ook indien besloten is af te zien van het treffen van verdere maatregelen.

Uitzonderingen

Hoewel direct informeren het uitgangspunt is, zijn er situaties denkbaar waarin het *direct* informeren van de betrokkene om bepaalde redenen niet mogelijk is. Dan dient **per geval** te worden afgewogen of deze situaties onder de uitzonderingen van genoemd in [artikel 41 Uitvoeringswet](#) vallen. Zie verder: § 5.1 Informeren van betrokkene.

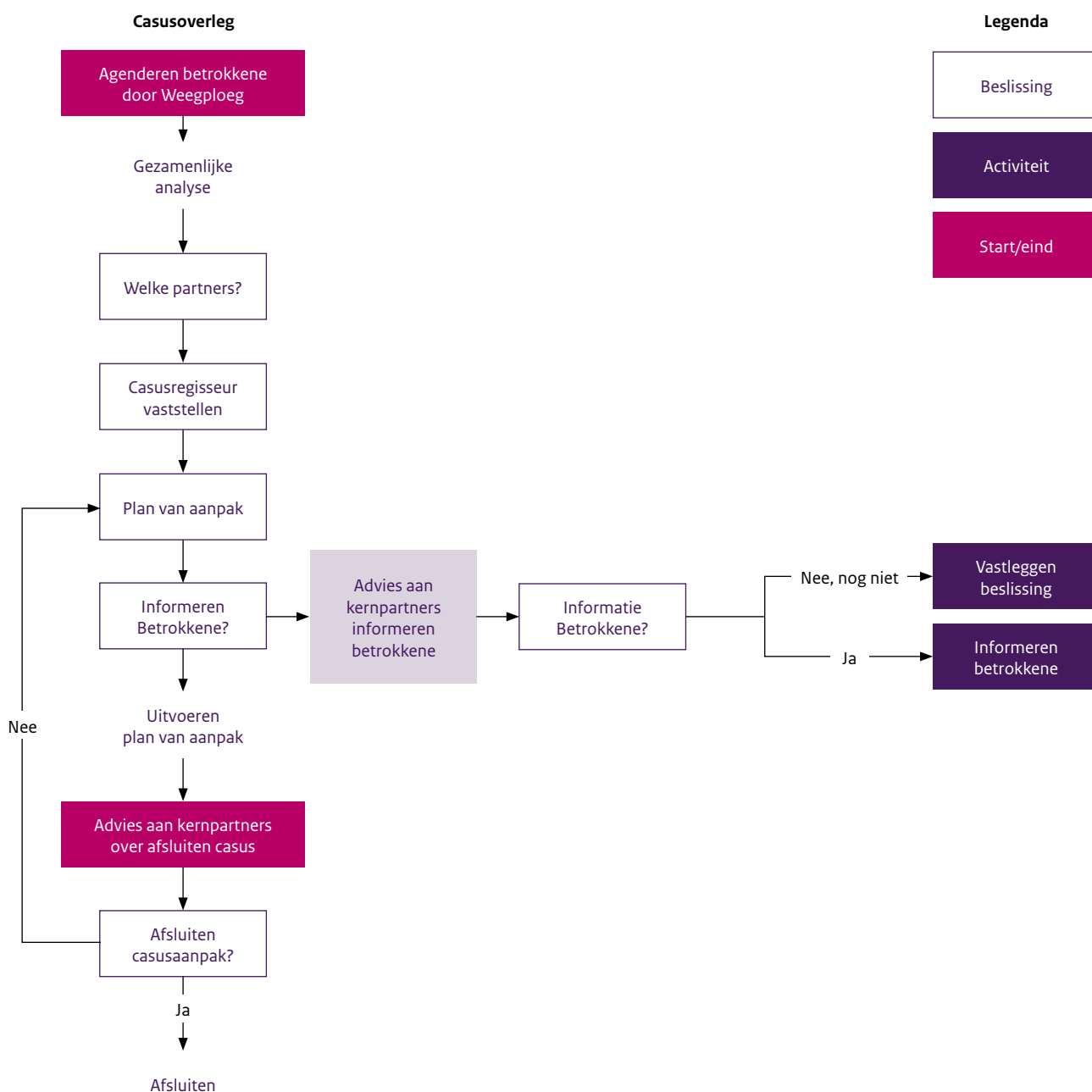
Overige aandachtspunten informeren

- Betrokken casuspartners beoordelen wie geïnformeerd wordt: de betrokkene zelf (in geval van meerderjarigheid) en/of zijn ouders (in geval van minderjarigheid).
- De wijze waarop/ door wie betrokkene wordt geïnformeerd kan onderdeel uitmaken van het plan van aanpak.
- Betrokken casuspartners zorgen dat zij heldere afspraken maken over door wie, op welke wijze en op welk moment de betrokkene en/of zijn ouders wordt geïnformeerd. Daarin wordt meegenomen of de betrokkene of zijn/haar ouders al in een eerder stadium is geïnformeerd, bijvoorbeeld in een eerder hulptraject bij een jeugdinstituut.

4 Casusoverleg: plan van aanpak

4.1 Stroomschema

Hieronder staan de verschillende keuzemomenten (en uitkomsten) in het proces weergegeven. In de volgende paragrafen worden de betrokken actoren (casusoverleg, uitvoerder) en keuzes nader toegelicht.



4.2 Casusoverleg

In de vorige stap heeft de weegploeg in eerste instantie beslist welke casuspartners bij het casusoverleg betrokken dienen te worden. Indien echter bij de behandeling van de casus blijkt dat andere of aanvullende casuspartners noodzakelijk zijn kunnen die alsnog worden betrokken door het casusoverleg zelf.

Voor de samenstelling van het casusoverleg gelden de volgende richtlijnen:

Samenstelling casusoverleg

Er zijn 3 kernpartijen en 2 casuspartijen benoemd in het convenant, namelijk:

1. kernpartijen, zijnde de:
 - a. de gemeente
 - b. de politie
 - c. het OM
2. 2 casuspartijen zijnde de:
 - a. Raad voor de Kinderbescherming
 - b. Reclassering Nederland

Externe casuspartners

- Alle andere casuspartners zoals zorgpartijen, maatschappelijke hulpinstellingen maar ook bijvoorbeeld onderdelen van het ministerie van V&J, zoals de NCTV en de IND zijn géén partij van het convenant.
- Dat wil niet zeggen dat zij niet over relevante informatie kunnen beschikken of een (belangrijke) rol kunnen spelen in het plan van aanpak. Deze partners kunnen relevante informatie delen met de genoemde casuspartners.
- Deze externe casuspartners mogen slechts informatie ontvangen c.q. verstrekken die noodzakelijk is voor het opstellen en de uitvoering van het plan van aanpak en voor de uitvoering van de eigen taak.
- Bij het opstellen van een plan van aanpak kunnen andere casuspartners dan de convenantpartijen worden betrokken indien:
 - a) zij over een deskundigheid beschikken die noodzakelijk is bij de aanpak van een specifieke casus
 - b) zij een rol spelen bij de uitvoering van het plan van aanpak.

Er dient altijd een afweging te worden gemaakt of het hebben van informatie ook aanleiding moet zijn om deel te nemen aan een casusoverleg. Uitgangspunt is dat informatie van bijvoorbeeld een uitvoeringsorganisatie via de vertegenwoordiger van de gemeente wordt ingebracht in het casusoverleg. Dit omdat het niet noodzakelijk is dat deze uitvoeringspartij kennis neemt van informatie van andere partijen. Telkens dient het nut en de noodzaak van deelname te worden afgewogen.

- Alle bij het plan van aanpak betrokken casuspartners hebben inzage in het plan van aanpak en de voortgang daarop.
- Ten behoeve van het casusoverleg wordt alleen die informatie verwerkt die noodzakelijk is voor het opstellen en uitvoeren van het plan van aanpak.

Aandachtspunten

- Met het uitbreiden van het casusoverleg dient terughoudend om te worden gegaan. Dit om te voorkomen dat informatie onnodig wordt gedeeld. Alleen die casuspartners die een rol kunnen spelen in het opstellen en uitvoeren plan van aanpak mogen deelnemen.
- Met 'noodzakelijke informatie' wordt bedoeld dat er een bewuste afweging dient te worden gemaakt welke informatie nodig is voor het opstellen en uitvoeren van het plan van aanpak. Er dient door partijen actief te worden bepaald welke informatie wél en welke informatie niet kan worden gedeeld.
- Het casusoverleg vervangt geen reguliere platforms en bilaterale overleggen.
- Elke deelnemer aan het casusoverleg behoudt zijn eigen verantwoordelijkheden. Er gaan dus geen taken en/of verantwoordelijkheden van individuele casuspartners over naar het casusoverleg.
- Door het casusoverleg zelf wordt besloten welke partij de lead in de casus heeft: de zogenaamde casusregisseur.
- Het casusoverleg kan ten behoeve van het opstellen en/of uitvoeren van het plan van aanpak advies vragen aan het "multidisciplinair adviesplatform." Dit platform bestaat onder andere uit vertegenwoordigers van de convenantpartijen werkzaam binnen de aanpak radicalisering en extremisme op landelijk niveau. Het platform brengt vanuit haar landelijke expertise op verzoek een vrijblijvend advies uit aan het casusoverleg. Indien noodzakelijk kan dit platform worden uitgebreid met andere deskundigen met expertise op het gebied van voorkomen en tegengaan van radicalisering en extremisme, zoals beschreven in art 9 lid 5 van het convenant.

4.3 Uitvoerder

Ten aanzien van het casusoverleg vervult de uitvoerder de volgende taken:

- Optreden als technisch voorzitter van het casusoverleg.
- Optreden als ambtelijk secretaris van het casusoverleg (vastleggen beslissingen, voorbereiden casusoverleg, planning)
- Aanmaken van een (digitaal) bestand in een beveiligd systeem voor het casusoverleg. In het bestand worden beslissingen van het casusoverleg vastgelegd (inclusief gehanteerde argumenten) en de informatie die heeft geleid tot beslissing.
- Zorgdragen voor autorisatie en het maken van afspraken met casuspartners over de wijze waarop om wordt gegaan met informatie (beveiliging) en autorisatieverlening.
- Informeren van betrokkene tenzij: a) één van de uitzonderingen genoemd in [artikel 41 UAVG](#) van toepassing is en b) tenzij in het plan van aanpak is afgesproken dat iemand anders dan de uitvoerder de betrokkene informeert.
- Zorgen voor de afhandeling van inzage/correctie/verzetverzoeken

4.4 Taken

Het casusoverleg richt zich op de volgende taken:

1. Gezamenlijke analyse van informatie. Na de weging van de casus door de weegploeg, volgt in het casusoverleg de gezamenlijke analyse van de casus ('casusdiagnose'). Op grond van de analyse kan een plan van aanpak worden opgesteld.
2. Bepalen welke partners deelnemen: op grond van de gezamenlijke analyse bepaalt het casusoverleg of deelname van nader te bepalen partners aan het casusoverleg noodzakelijk is.
3. Aanwijzen casusregisseur: het casusoverleg kan een casusregisseur aanwijzen. De casusregisseur vertegenwoordigt de meest gerede partner in een specifieke casus en coördineert de praktische afstemming van de acties voortvloeiende uit het plan van aanpak.
4. Plan van aanpak: het casusoverleg stelt een plan van aanpak op. De benodigde maatregelen onder regie van de casusregisseur uitgevoerd de casuspartners.
5. Evalueren en advies over afsluiten: op basis van de evaluatie van de aanpak formuleert het casusoverleg een advies aan de kernpartijen over het afsluiten van de casus.
6. Informeren betrokkene: indien de betrokkene nog niet is geïnformeerd, geeft het casusoverleg een advies over het informeren van de betrokkene aan de kernpartijen. Het casusoverleg overweegt zonodig periodiek of en wanneer alsnog moet worden overgegaan tot informeren van betrokkene. Bij het opstellen van het plan van aanpak wordt besloten door wie en wanneer betrokkene wordt geïnformeerd.

5 Informatieplicht en rechten betrokkene

5.1 Toelichting

Uitgangspunt bij het informeren van betrokkene is “informeren, tenzij...”. De weegploeg/het casusoverleg overlegt of een van de uitzonderingen genoemd in **artikel 41 UAVG** van toepassing is, waardoor het informeren van betrokkene dat hem/haar aangaande informatie wordt verwerkt nog niet mogelijk is. Zie verder artikel 11 van het modelconvenant.

Zodra de uitzonderingen in de wet niet langer van toepassing zijn dient betrokkene alsnog te worden geïnformeerd. Dit geldt ook als besloten is af te zien van het treffen van verdere maatregelen.

In dit hoofdstuk zullen aan de hand van de van toepassing zijnde wetgeving praktijksituaties worden toegelicht die vallen onder de reikwijdte van de wet.

5.2 Informeren betrokkene

Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen (Art. 14 AVG)

1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie:
 - a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
 - b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
 - c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking;
 - d) de betrokken categorieën van persoonsgegevens;
 - e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
 - f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een ontvanger in een derde land of aan een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van de in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

2. Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie om ten overstaan van de betrokkene een behoorlijke en transparante verwerking te waarborgen:
 - a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
 - b) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;
 - c) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid;
 - d) wanneer verwerking op artikel 6, lid 1, punt a) of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
 - e) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
 - f) de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen;
 - g) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.
3. De verwerkingsverantwoordelijke verstrekt de in de leden 1 en 2 bedoelde informatie:
 - a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
 - b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
 - c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

4. Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.
5. De leden 1 tot en met 4 zijn niet van toepassing wanneer en voor zover:
- a) de betrokkene reeds over de informatie beschikt;
 - b) het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
 - c) het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of
 - d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijke recht, waaronder een statutaire geheimhoudingsplicht.

Uitzonderingen op rechten betrokkene en plichten verwerkingsverantwoordelijke (Art. 41 UAVG)

1. De verwerkingsverantwoordelijke kan de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34 van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van:
- a. de nationale veiligheid;
 - b. landsverdediging;
 - c. de openbare veiligheid;
 - d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
 - e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
 - f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;

- g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepsregels voor geregelde beroepen;
 - h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
 - i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of
 - j. de inning van civielrechtelijke vorderingen.
2. Bij de toepassing van het eerste lid houdt de verwerkingsverantwoordelijke rekening met in ieder geval, voor zover van toepassing:
- a. de doeleinden van de verwerking of van de categorieën van verwerking;
 - b. de categorieën van persoonsgegevens;
 - c. het toepassingsgebied van de ingevoerde beperkingen;
 - d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;
 - e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijke;
 - f. de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;
 - g. de risico's voor de rechten en vrijheden van de betrokkenen; en
 - h. het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.

De volgende voorbeelden zijn (niet limitatieve) praktijksituaties die onder de reikwijdte van **artikel 41 UAVG** vallen en dus reden kunnen geven om betrokkene niet direct te informeren:

1. **Bescherming van anderen:** Wanneer iemand, bijvoorbeeld een melder gevaar zou lopen wanneer betrokkene te weten zou komen wie over hem/haar informatie heeft gedeeld, kan kennisgeving van informatie over de derde onder omstandigheden worden geweigerd met een beroep op **artikel 41, eerste lid, onder i, UAVG**.
2. **Alarmering andere personen.** Wanneer het informeren van betrokkene ervoor zou kunnen zorgen dat andere personen zouden worden gealarmeerd (en dit bijvoorbeeld een versturende werking zou hebben op het plan van aanpak of een lopend strafproces) kan worden afgezien van het direct informeren van betrokkene. (**artikel 41, eerste lid, onder d, UAVG**)
3. **Extra tijd nodig voor uitvoering van het plan:** Indien dit de effectiviteit en de uitvoering van het plan van aanpak/ ten goede komt kan dit, mits goed onderbouwd een reden zijn om betrokkene op een later moment te informeren. Betrokkenen zal worden geïnformeerd zodra het casusoverleg een plan van aanpak en een wijze van benaderen/informeren heeft vastgesteld. (**artikel 41, eerste lid, onder d, UAVG**)
4. **Bescherming van betrokkene:** bijvoorbeeld wanneer een radicaliserende minderjarige radicaliserende ouders heeft en het dus niet in het belang van de betrokkene is wanneer zijn/haar ouders worden geïnformeerd dat hij/zij wordt besproken in een casusoverleg (**artikel 41, eerste lid, onder i, UAVG**)

5.3 Rechten van betrokkenen

De betrokkene (of zijn wettelijk vertegenwoordiger), kan op grond van de AVG, de Wjsg of de Wpg aan de verwerkingsverantwoordelijke een verzoek indienen waarbij hij een beroep doet op een van zijn rechten als betrokkenen. Wanneer een dergelijk verzoek wordt ontvangen dient de uitvoerder allereerst te beoordelen aan wie het verzoek gericht is, onder welke wettelijke regime het verzoek valt en welke spelregels daarvoor gelden. Hierbij is het van belang dat er onderscheid wordt gemaakt in verzoeken die gericht zijn aan het samenwerkingsverband en verzoeken die rechtstreeks gericht zijn aan een van de deelnemende partijen van het samenwerkingsverband. Dit maakt namelijk wat uit voor de toepasselijkheid van de wettelijke kaders. Zie hieronder. De betrokkene heeft ook het recht om bij de Autoriteit Persoonsgegevens een klacht in te dienen over de verwerking van zijn persoonsgegevens.

5.4 Uitvoeren verzoeken rechten van betrokkenen: toepasselijk recht

Bij het ontvangen van een inzage- en/of correctieverzoek zal de uitvoerder moeten bekijken of het verzoek betrekking heeft op inzage en/of correctie in de gegevensverwerking (bestand) van het samenwerkingsverband zelf of dat het verzoek (via het samenwerkingsverband) gericht is aan een van de deelnemende partijen, bijvoorbeeld de politie of het OM.

Let op: diegene waar het verzoek binnenkomt (de uitvoerder) zorgt ervoor dat het verzoek zo snel mogelijk wordt doorgestuurd naar de partij waarop het verzoek betrekking heeft. Dit gelet op wettelijke beantwoordingstermijnen.

Op een inzage- en/of correctieverzoek in de gegevensverwerking door het samenwerkingsverband zijn de AVG en de UAVG van toepassing. Is het inzage- en/of correctieverzoek rechtstreeks aan het OM of de politie gericht, dan dient de uitvoerder het verzoek bij de betreffende partij neer te leggen. Aan het verzoek dient vervolgens uitvoering te worden gegeven aan de hand van de voor hen geldende wet- en regelgeving, respectievelijk de Wjsg en de Wpg. Voor de gemeenten, de Raad voor de Kinderbescherming en de Reclassering gelden de AVG en de UAVG.

AVG

Inzagerecht

Artikel 15 van de AVG regelt het inzagerecht. Dit recht stelt de betrokkene in staat om bij de verwerkingsverantwoordelijke na te gaan of zijn gegevens worden verwerkt (transparantiebeginsel). Vervolgens kan de betrokkene verzoeken om zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of te beperken etc. (zie verder artikel 16, 17 en 18 AVG).

Het uitoefenen van het inzagerecht doorloopt een aantal fases: ontvangst van het inzageverzoek (is het op de juiste plek, voor bestuursorganen geldt op grond van de Awb een doorzendplicht!),

de verificatie van de identiteit van de betrokkene door de verwerkingsverantwoordelijke, het controleren van gegevens over derden en de uiteindelijke berichtgeving aan de betrokkene.

Fase 1: Indienen van een inzageverzoek (artikel 15 AVG)

De betrokkene dient een inzageverzoek in, waar het volgende voor geldt:

- Een reden voor een inzageverzoek hoeft door de betrokkene niet te worden gegeven.
- Het betreft een schriftelijk /elektronisch verzoek.
- Het verzoek is met redelijke tussenpozen ingediend. Zo is de betrokkene niet toegestaan de verwerkingsverantwoordelijke meer dan gemiddeld te benaderen met het verzoek om informatie (zie ook hierna bij fase 3).

Fase 2: Verificatie van de betrokkene door verwerkingsverantwoordelijke

Een inzageverzoek mag alleen over de eigen gegevens gaan. Dit betekent dat de verwerkingsverantwoordelijke moet verifiëren of het inzageverzoek door de betrokkene zelf of namens hem wordt gedaan en wat de leeftijd van de betrokkene is.

1. Verzoek door betrokkene; controle identiteit (artikel 12, tweede en zesde lid, AVG)

Indien het verzoek tot inzage door betrokkene zelf is ingediend dient de verwerkingsverantwoordelijke zijn identiteit te controleren. Dit kan door het opvragen van een kopie van een geldig identiteitsbewijs, waarbij de foto en het BSN door de betrokkene wordt afgeschermd. Identificatie hoeft niet per se door middel van een geldig identiteitsbewijs plaats te vinden. Een betrokkene moet in de gelegenheid gesteld zich eventueel op andere wijze te identificeren (artikel 11, tweede lid, AVG).

2. Verzoek namens betrokkene; ondertekende machtiging

De betrokkene of de wettelijke vertegenwoordiger kunnen er voor kiezen een persoon te machtigen die namens hem het inzagerecht uitoefent. Mocht de betreffende persoon geen advocaat zijn, dan moet toestemming van de betrokkene blijken uit een door hem ondertekende machtiging. Houd er rekening mee dat toestemming en de machtigingsverklaring te allen tijde door de betrokkene kan worden ingetrokken.

3. Controleren leeftijd betrokkene (artikel 5, vierde lid, UAVG)

A) Jonger dan 16 jaar; wettelijk vertegenwoordiger /ouderlijk gezag

Artikel 5, vierde lid, UAVG bepaalt onder meer dat voor de betrokkene jonger dan 16 jaar de toestemming van de wettelijk vertegenwoordiger is vereist. Bij een inzageverzoek door een betrokkene jonger dan 16 jaar moet gecontroleerd worden of het verzoek door de wettelijk vertegenwoordiger is gedaan. Meestal is dat degene met die met het ouderlijk gezag is belast.

B) Ouder dan 16 jaar; zelfstandig recht of ondertekende machtiging

Bij een inzageverzoek door een ouder over een betrokkene ouder dan 16 jaar worden de gegevens niet ter inzage verleend, tenzij de

betrokkene die betreffende ouder schriftelijke gemachtigd heeft (zie onder punt 2). Kinderen van 16 jaar en ouder hebben zelfstandige rechten, tenzij er sprake is van curatele of mentorschap.

Fase 3: Rechten van derden

Voordat de verwerkingsverantwoordelijke over gaat tot de beantwoording van het inzageverzoek dient hij te controleren of gegevens van derden zijn opgenomen. Dat kan reden zijn om inzage van deze gegevens (deels) te beperken. Als er naar verwachting bezwaar staat tegen inzage in diens gegevens dan dient de verwerkingsverantwoordelijke de derde naar zijn mening te vragen alvorens te voldoen aan het inzageverzoek.

Fase 4: Berichtgeving aan betrokkene (artikel 12, lid 3, AVG)

De verwerkingsverantwoordelijke moet de betrokkene binnen een maand na ontvangst van het verzoek informeren over de uitvoering van het verzoek, ook als het een weigering van het verzoek betreft. Afhankelijk van de complexiteit van het verzoek kan de termijn met nog eens twee maanden worden verlengd.

De verwerkingsverantwoordelijke licht de betrokkene over het volgende in:

- de verwerkingsdoelstellingen;
- de betrokken categorieën van persoonsgegevens;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
- dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
- wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Indien de gegevens vernietigd zijn en er geen persoonsgegevens meer worden verwerkt, dan dient ook deze informatie aan de betrokkene gemeld te worden.

Het verlenen van inzage gebeurt in beginsel door een kopie/ afschrift van de documenten te verstrekken. Voor de kopie mogen geen kosten in rekening gebracht worden. De kopie moet schriftelijk (waaronder begrepen in elektronische vorm) verstrekt worden.

Let op: Werkaantekeningen vallen niet onder het inzagerecht, maar wel als deze in het dossier zijn opgenomen of aan anderen zijn verstrekt, dus zorg ervoor dat deze gegevens niet in het dossier worden opgenomen.

Weigeringsgronden

De verwerkingsverantwoordelijke kan een inzageverzoek ook (gedeeltelijk) weigeren in het geval van:

- een kennelijk ongegrond verzoek, omdat gevraagd wordt om iets waar men evident geen recht op heeft (bijvoorbeeld inzage in de persoonsgegevens van een ander).
- een buitensporig verzoek, bijvoorbeeld omdat de stukken al in het bezit zijn van de betrokkene of het verzoek onredelijk snel herhaald wordt.
- *Gedeeltelijke of gehele weigering van het inzageverzoek op grond van artikel 41 UAVG:*
- Het inzagerecht is niet absoluut en kan bij uitzondering op grond van artikel 41 UAVG (tijdelijk) door de verwerkingsverantwoordelijke buiten toepassing worden gelaten worden. Onder meer:
 - in het belang van de voorkoming, opsporing en vervolging van strafbare feiten (artikel 41, eerste lid, onder d, UAVG);
 - als het gaat om de bescherming van belangen van de betrokkene of van de rechten en vrijheden van anderen: bijvoorbeeld om informatie af te schermen die over iemand anders gaat (artikel 41, eerste lid, onder i, UAVG).

De verwerkingsverantwoordelijke dient de weigering met argumenten te onderbouwen door een zorgvuldige belangenafweging van alle betrokken partijen. Bij die belangenafweging moet hij in elk geval rekening houden met de in artikel 41, tweede lid, UAVG genoemde factoren.

Uitoefenen recht op rectificatie en recht op gegevenswissing (artikelen 16 en 17 AVG)

Aan de hand van de ter beschikking gestelde documenten kan de betrokkene op grond van artikel 16 AVG aan de verwerkingsverantwoordelijke verzoeken om rectificatie en aanvulling van zijn persoonsgegevens. Iemand kan een correctie vragen als zijn persoonsgegevens feitelijk onjuist zijn, onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld, op een andere manier in strijd met een wet worden verwerkt.

Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Wel mag diegene van de organisatie verwachten dat deze in ieder geval zijn schriftelijke mening toevoegt aan het dossier. Dat kan vooral een oplossing bieden bij situaties waarbij het om niet objectief vast te stellen feiten gaat.

De betrokkene heeft op grond van artikel 17 AVG ook het recht om zijn persoonsgegevens te laten wissen (het recht om vergeten te worden), maar alleen als die niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld of onrechtmatig zijn verzameld. Als de gegevens met andere partijen zijn gedeeld, moeten deze ervan op de hoogte worden gebracht dat de gegevens zijn verwijderd op verzoek van de betrokkene.

Recht van bezwaar tegen de verwerking (artikel 21 AVG)

Iemand kan bezwaar maken tegen de verwerking van zijn persoonsgegevens vanwege bijzondere persoonlijke omstandigheden. Het recht van verzet bij bijzondere persoonlijke omstandigheden. Er moet binnen vier weken over een dergelijk verzoek worden beslist.

Algemene wet bestuursrecht (Awb)

Het verlenen van inzage of de weigering daarvan door een bestuursorgaan is een besluit in de zin van de Awb (zie artikel 34 UAVG). Houd hierbij rekening met de termijn die gelden bij bezwaar en beroep.

Voorts verdient het aanbeveling om bij een inzageverzoek na te gaan of er sprake is van een inzageverzoek op grond van de AVG of een verzoek om informatie op grond van de Wet openbaarheid bestuur (Wob), of dat er sprake is van een bezwaarschriftenprocedure.

Let op: Een Wob-verzoek is breder en houdt ook in dat na openbaarmaking het dossier voor iedereen openbaar is.

Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg)

Recht op kennisneming

Op grond van artikel 25 Wpg en de artikelen 18 en 391 Wjsg kan een betrokkene aan de verwerkingsverantwoordelijke een schriftelijk verzoek om kennisneming van zijn persoonsgegevens verzenden. Het OM en de politie dienen binnen zes weken op een dergelijke verzoek te reageren.

Uitzondering recht op kennisneming

Dit recht is niet absoluut. De mededeling of en zo ja, welke gegevens zijn vastgelegd door de partijen kan op grond van artikel 27, eerste lid Wpg respectievelijk 391 Wjsg achterwege blijven als dat noodzakelijk is in het belang van bijvoorbeeld een lopend (gerechtelijke) onderzoek en het onderzoek hierdoor gevaar loopt. Het kan ook in het belang van anderen zijn dat de politie of het OM een dergelijk verzoek kan weigeren.

Een (gedeeltelijke) weigering moet schriftelijk kenbaar worden gemaakt aan de betrokkene.

Wijze van inzage verlenen

De politie doet geen schriftelijke mededelingen, inzage wordt ter plekke op het bureau verleend. In enkele gevallen, zoals bij schadeclaims voor verzekeraars, kan het noodzakelijk zijn dat de politie schriftelijke inzage verleend.

Voor het OM geldt dat ze voor inzage in justitiële gegevens verwijzen naar Justid. Aan het recht op kennisneming kan op verschillende manieren worden voldaan, bijvoorbeeld door een mededeling of inzage in de betreffende gegevens. Artikel 391 Wjsg verplicht in ieder geval niet tot afgifte van stukken.

Het verzoek kan worden gericht aan het OM-onderdeel waar de informatie waarschijnlijk verwerkt is.

Recht van verzet en correctierecht

Een betrokkene kan te allen tijde verzet aantekenen tegen gegevensverwerking wegens bijzondere persoonlijke omstandigheden met een beroep op artikel 26 Wjsg.

Tevens kan de betrokkene op grond van artikel 28 Wpg of 391 Wjsg om correctie (verbetering, aanvulling, verwijdering of afscherming van gegevens) vragen als zijn persoonsgegevens:

- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
- op een andere manier in strijd met een wet worden gebruikt.

Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Wel mag diegene van de organisatie verwachten dat deze in ieder geval zijn schriftelijke mening toevoegt aan het dossier. Dat kan vooral een oplossing bieden bij situaties waarbij het om niet objectief vast te stellen feiten gaat.

6. Informatiebeveiliging

Voor de verwerking van gegevens legt de uitvoerder gegevens vast in een (digitaal) bestand. Zie Artikel 10 van het modelconvenant. Om datalekken te voorkomen, moeten overheden die persoonsgegevens gebruiken, deze volgens de richtlijnen van de Autoriteit Persoonsgegevens beveiligen.

6.1 Informatiebeveiliging

Artikel 32 AVG gaat over de beveiliging van persoonsgegevens. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen, die een op het risico afgestemd beschermingsniveau waarborgen van de persoonsgegevens die door het samenwerkingsverband worden verwerkt. Daarbij geldt dat de te nemen maatregelen strenger zijn naar mate de persoonsgegevens gevoeliger zijn. Dat is hier het geval.

Om aan de norm van artikel 32 AVG te voldoen is het noodzakelijk dat het samenwerkingsverband maatregelen neemt die, waar passend, onder meer het volgende omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkings-systemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Voor een blijvend passend beveiligingsniveau is inbedding van de zogeheten plan-do-check-act-cyclus in de dagelijkse praktijk van de organisatie noodzakelijk. Een organisatie dient hierbij altijd de rechten van de betrokkenen te waarborgen en er moet sprake zijn van adequate, vakkundig toegepaste beveiliging waarbij de organisatie optimaal benut wat het vakgebied informatiebeveiliging te bieden heeft. Dat komt op het volgende neer:

1. Beoordeel de risico's

Beoordeel de risico's die de gegevens en de aard van de verwerking met zich meebrengen voor de betrokkenen en bepaal op basis daarvan het gewenste beveiligingsniveau. Inventariseer vervolgens de dreigingen die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voor zullen doen. Tref op basis daarvan gericht beveiligingsmaatregelen die het gewenste beveiligingsniveau kunnen waarborgen.

2. *Maak gebruik van algemeen geaccepteerde beveiligingsstandaarden*
Het vakgebied informatiebeveiliging kent vele beveiligingsmethoden, -standaarden en -maatregelen die zijn gebaseerd op ervaringen uit de dagelijkse beveiligingspraktijk. Gebruik bij het nemen van beveiligingsmaatregelen de richtsnoeren in samenhang met de beschikbare beveiligingsstandaarden. Deze standaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de beveiligingsrisico's af te dekken.

3. Controleer en evalueer regelmatig

Controleer met zekere regelmaat of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en worden nageleefd. Beoordeel periodiek of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen en of de beveiligingsmaatregelen nog steeds voldoen. Betrek daarbij ook de stand van de techniek en de nieuwste inzichten binnen het vakgebied informatiebeveiliging. Pas waar nodig de beveiligingsmaatregelen aan.

Zie ook de Beleidsregels van de Autoriteit Persoonsgegevens (nog gericht op de Wbp): https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

6.2 Datalekken

Op grond van **artikel 33 en 34 AVG** geldt met betrekking tot datalekken dat er duidelijke afspraken moeten worden gemaakt door het samenwerkingsverband over het melden van datalekken intern en uiteindelijk bij de Autoriteit Persoonsgegevens (AP). Duidelijk moet zijn op welke wijze (mail, telefonisch) moet worden gemeld bij de verwerkingsverantwoordelijke partijen van het samenwerkingsverband, door wie, binnen welk tijdsbestek etc. Dit is van belang zodat het samenwerkingsverband vervolgens binnen de daarvoor gestelde termijn melding kan doen bij de Autoriteit Persoonsgegevens en eventueel betrokkenen kan informeren over de datalek.

Dus stel vast:

- Is er sprake een datalek;
- Zo, ja is het een datalek dat moet worden gemeld bij de AP;
- Binnen welke termijn moet worden gemeld (zie richtlijnen AP);
- Moet de betrokkene worden geïnformeerd over het datalek.

Zie link: Meldloket AP en de daarbij behorende meldformulier <https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?1>
Meer informatie over de Wet meldplicht datalekken is te vinden op de website van de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

6.3 Bewaartermijnen

Ten behoeve van de weegploeg en het casusoverleg legt de uitvoerder gegevens vast in een (digitaal) bestand.

Radicalisering is een complex en dynamisch proces dat geen vaststaande oorzaken of uitkomsten heeft. Er zijn vele 'routes' en deze leiden slechts in enkele gevallen ook daadwerkelijk tot extremisme en terrorisme. Ook de wijze waarop en het tempo waarin mensen kunnen radicaliseren variëren sterk. Juist hierom is het noodzakelijk om de informatie die is gedeeld in het casusoverleg een periode te bewaren om te bezien of de inschatting van de ontwikkeling een juiste is en zo niet, alsnog in te grijpen. Daarnaast vindt bewaring plaats met het oog op eventuele afhandeling van klachten en overige juridische procedures.. Er is gekozen om aansluiting te zoeken bij de bewaartermijnen die gelden voor politiegegevens, zijnde 5 jaar.

Uiterlijk 1 jaar na de laatste verwerking worden persoonsgegevens echter gearchiveerd in een niet-actieve digitale omgeving. Dat betekent dat de gegevens niet langer raadpleegbaar zijn door casuspartners, met uitzondering van de kernpartijen. Zij kunnen de gegevens raadplegen bijvoorbeeld indien er nieuwe signalen zijn of wanneer de betrokkene een klacht indient. Zie verder artikel 13 van het convenant.

7 Referentiekader

Bij het inschatten, bespreken en beoordelen van (signalen van radicalisering met betrekking tot) een persoon wordt gebruikt gemaakt van een radicaliseringsmodel gebaseerd op wetenschappelijk onderzoek. De basis van het model ligt in de “staircase-theorie” van Fathali M. Moghaddam (Moghaddam, 2005)¹. De staircase theorie gaat uit van vier fases van radicalisering die kunnen uitmonden in terrorisme.

Ideologie	Sociale Context
Fase 4 - Bereidheid om zelf geweld toe te passen	
Fase 3 - Acceptatie van geweld als middel	
Fase 2 - Sociale vervreemding	
Fase 1 - Voorfase	

De fases kennen twee ontwikkelingsgebieden : het gebied van ideologie en het gebied van omgeving, contacten en gedragingen, oftewel de sociale context van een persoon. De ideologische kant in

het model geeft duiding aan de intenties die een persoon heeft op basis van zijn ideologische belevingswereld. Het sociale context-gebied geeft duiding aan de potentie die een persoon heeft om zijn overtuigingen in concrete daden om te zetten.

Binnen dit kader wordt gekeken naar een negental ontwikkel gebieden:

1. Opvallende contacten
2. Gedrag
3. Ideologie en overtuiging
4. Geweld en criminaliteit
5. Onvrede
6. Propaganda
7. Internationale contacten en bewegingen
8. Sociale zorgen
9. Training

¹ Moghaddam, Fathali (Feb–Mar 2005). “The Staircase to Terrorism”. American Psychologist. 60 (2): 161–169

Bijlage I Gehanteerde begrippen

In de handreiking wordt verstaan onder:

- **achterblijver:** persoon met wie een uitreiziger in gezinsverband leefde;
- **casusoverleg** persoonsgerichte aanpak radicalisering en extremisme: het casusoverleg ter voorkoming van radicalisering en extremisme bestaande uit de gemachtigde vertegenwoordiger(s) van de betrokken kernpartijen en casuspartners, belast met het opstellen en monitoren van het integraal plan van aanpak;
- **extremisme:** de benaming van het fenomeen waarbij personen of groepen, op buitenparlementaire wijze over de grenzen van de wet gaan en met (gewelddadige) acties politieke beslissingvorming proberen te beïnvloeden;
- **integraal plan van aanpak:** het document waarin het doel van de persoonsgerichte, integrale benadering van het subject en de hiertoe door partijen te treffen maatregelen zijn vastgelegd;
- **radicalisering:** Een proces van toenemende bereidheid om de uiterste consequentie uit een denkwijze te aanvaarden en die in daden om te zetten. Deze toenemende bereidheid kan leiden tot gedrag dat andere mensen diep kwetst of in hun vrijheid raakt, kan aanleiding zijn voor individuen of groepen om zich af te keren van de samenleving en kan leiden tot het gebruik van geweld;
- **referentiekader:** Het objectieve kader waarin criteria worden gegeven om te bepalen of een persoonsgerichte, integrale benadering van het subject noodzakelijk is;
- **signaal:** een feitelijke gedraging die mogelijksterwijds duidt op radicalisering, extremisme, uitreizen, of terugkeer van een natuurlijk persoon;
- **subject²:** de natuurlijke persoon die voorwerp van bespreking is in de weegploeg en / of het casusoverleg;
- **terugkeerder:** een uitreiziger die na verblijf bij een jihadistische groepering of in een jihadistisch strijdgebied terugkeert naar het land dat hij of zij voor de uitreis verlaten heeft of een ander land dat niet is aan te merken als jihadistisch strijdgebied;
- **uitreiziger:** een persoon die zijn eigen land verlaat om zich aan te sluiten bij een jihadistische groepering in een jihadistisch strijdgebied;
- **uitvoerder:** de functionaris die onder verantwoordelijkheid en in naam van de verwerkingsverantwoordelijke als bedoeld in de Wbp, zorg draagt voor een zorgvuldig beheer van de gegevens;
- **Weegploeg:** overleg, bestaande uit de gemachtigde vertegenwoordiger(s) van de burgemeester en het College van burgemeester en wethouders, de politie en het OM, belast met het verzamelen van de verschillende signalen en de selectie van de aangebrachte casuïstiek op basis van het referentiekader, teneinde te bepalen of voor het subject een persoonsgerichte, integrale benadering noodzakelijk is, en welke casuspartners hierbij betrokken dienen te worden.

² In de procesbeschrijving gebruiken we hiervoor het begrip betrokkene.



Meer informatie
info@nctv.minvenj.nl

mei 2018