Gegevensuitwisseling

bij samenwerking rond casuïstiek

in het zorg- en veiligheidsdomein

Juridisch kader
(versie 2.1 - juli 2020)

Colofon

Werkgroep gegevensuitwisseling in het zorg- en veiligheidsdomein

In opdracht van de stuurgroep Zorg en Veiligheid, juli 2020.

Ministerie van Justitie
en Veiligheid

Reclassering Nederland

POLITIE

VNG

GGZNEDERLAND

OPENBAAR
MINISTERIE

Dienst Justitiële Inrichtingen
Ministerie van Justitie en Veiligheid

LEGER
DES
HEILS

jeugdzorg
nederland

SVG
Verslavingsreclassering

Raad voor de Kinderbescherming
Ministerie van Justitie en Veiligheid

slachtoffer
HULP
NEDERLAND

vereniging van
woningcorporaties
aedes

Halt.

Samenwerkende
zorg- en veiligheidshuizen

Inhoudsopgave

1 Inleiding 6
1.1 Aanleiding 6
1.2 Waarom dit handvat 7

2 Algemeen juridisch kader gegevensverwerking 9
2.1 Grondrecht op privacy 9
2.2 AVG en Uitvoeringswet (UAVG) 9
2.3 Persoonsgegevens 13
2.4 Grondslagen voor verwerking van persoonsgegevens 14
2.5 Verwerking bijzondere- en strafrechtelijke persoonsgegevens 17
2.6 Richtlijn Gegevensbescherming Opsporing en Vervolging 18
2.7 Beroepsgeheim 19
2.8 Toestemming 20
2.9 Drang 22

3 Grondslagen per organisatie bekeken 23
3.1 DJI 24
3.2 Gemeente 28
3.3 GGZ 40
3.4 Gecertificeerde Instellingen (GI) 41
3.5 Jeugdhulp 47
3.6 Openbaar Ministerie 50
3.7 Politie 58
3.8 Raad voor de Kinderbescherming (RvdK) 62
3.9 Reclassering 64
3.10 Slachtofferhulp 69
3.11 Stichting Halt 73
3.12 Veilig Thuis (AMHK) 74
3.13 Woningcorporaties 78

4 Toepassing van het handvat in de praktijk 81
4.1 Algemeen 81
4.2 Juridische inrichting gegevensverwerking bij complexe casuïstiek 83
4.3 Rechtmatigheid bij de inrichting van de samenwerking 85
4.4 Werkproces en afspraken over zorgvuldigheid 89
4.5 Eisen aan het gebruik van ICT-systemen bij samenwerking 92

BIJLAGE 1: KERNBEGRIPPEN UIT DE AVG 94

BIJLAGE 2: VERTALING HANDVAT NAAR DE PRAKTIJK – EEN VOORBEELD 96

BIJLAGE 3: TEMPLATE SAMENWERKINGSCONVENANT 119

BIJLAGE 4: TEMPLATE PRIVACY PROTOCOL 144
BIJLAGE 5: CONTACTGEGEVENS BETROKKEN ORGANISATIES 181

1 Inleiding

1.1 Aanleiding

In 2017 verscheen het Handvat gegevensuitwisseling in het zorg- en veiligheidsdomein: een handvat voor de zorg- en veiligheidshuizen. Dat handvat was destijds specifiek geschreven voor het samenwerkingsverband zorg- en veiligheidshuis. Voor u ligt de tweede herziene uitgave van dit handvat. Het handvat is in opdracht van de landelijke Stuurgroep Zorg- en Veiligheid geactualiseerd op basis van de Algemene Verordening Gegevensbescherming Verordening (EU 2016/679), de Uitvoeringswet AVG en de - als gevolg van de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn EU 2016/680) - gewijzigde Wet Politiegegevens en Wet justitiële en strafvorderlijke gegevens. Tevens is dit handvat zodanig geschreven dat het van toepassing is op diverse samenwerkingsverbanden in het zorg- en veiligheidsdomein[1] waar professionals samenwerken rond complexe casuïstiek. De in dit handvat beschreven juridische kaders en uitgangspunten zijn breed toepasbaar. Echter, elk samenwerkingsverband dient op basis van de eigen doelen, de samenstelling van de partners en de taken op basis waarvan zij samen werken, opnieuw te kijken naar onder meer de wettelijke grondslag en het doel van het verstrekken van informatie. Dit handvat kan daarvoor als leidraad worden gebruikt.

In samenwerkingsverbanden binnen het zorg- en veiligheidsdomein werken partijen samen om maatschappelijke problemen op te pakken en gezamenlijk te komen tot oplossingen die in het belang zijn van betrokkenen en de omgeving. Het gaat dan niet alleen om het Openbaar Ministerie, politie, gemeenten en de zorgpartijen, maar ook andere maatschappelijke organisaties kunnen deelnemen om de complexe meervoudige problematiek, die vaak op meerdere leefgebieden speelt, te behandelen. Zij doen dit door in wisselende samenstelling samen te werken bij het oplossen van complexe casuïstiek.

Aan een samenwerkingsverband kunnen zowel publiekrechtelijke als privaatrechtelijke partijen deelnemen. Er is geen specifieke wetgeving voor samenwerkingsverbanden zoals het zorg- en veiligheidshuis. Dit betekent dat de deelnemende partijen hun eigen (wettelijke) verantwoordelijkheden en bevoegdheden behouden.

Misverstand
Over samenwerkingsverbanden geldt vaak het volgende misverstand: er is een convenant, dus mogen partijen persoonsgegevens uitwisselen. Een convenant kan echter nooit de grondslag zijn voor gegevensuitwisseling en een convenant kan de wettelijke regels nooit doorbreken. Het is niet mogelijk om op basis van een convenant een partij gegevens te laten ontvangen die zij normaliter niet zouden mogen hebben. Gegevensuitwisseling mag alleen plaatsvinden als daarvoor een wettelijke grondslag bestaat. Dat betekent voor overheden dat zij een allereerst moeten beschikken over een expliciete wettelijke taak. Ongeacht de inhoud van het convenant moeten partijen zich houden aan de voor hen geldende wettelijke regels voor het uitwisselen van

[1] Hieronder valt ook het sociaal domein.

persoonsgegevens. Het is aan te bevelen om een samenwerkingsconvenant - en eventueel een daarbij behorend privacy-protocol - op te stellen voor het samenwerkingsverband. Hierin wordt de intentie om samen te werken vastgelegd en worden belangrijke samenwerkingsafspraken, zoals het doel of de doelen van de samenwerking en de gegevensverwerking, dat wil zeggen de gegevensuitwisseling tussen partijen en de verwerkingsactiviteiten binnen het samenwerkingsverband, nader uitgewerkt.

1.2 Waarom dit handvat

De samenwerking bij het behandelen van complexe casuïstiek kan in het algemeen niet zonder het uitwisselen van persoonsgegevens. Het omgaan met persoonsgegevens van burgers is aan wetgeving gebonden. Het Europees Verdrag van de Rechten van de Mens, het Handvest van de grondrechten van de Europese Unie, de Grondwet en Europese en nationale wetgeving schrijven voor dat overheden c.q. bestuursorganen, instellingen en bedrijven alleen om bepaalde redenen een inbreuk mogen maken op het persoonlijk leven van burgers en uitsluitend op basis van een wettelijke regeling.

Voor samenwerkingsverbanden in het zorg- en veiligheidsdomein rondom complexe casuïstiek betekent dit dat er slechts persoonsgegevens van burgers kunnen worden uitgewisseld als daarvoor een specifieke wettelijke grondslag is aan te wijzen. Die wettelijke grondslag voor de uitwisseling van persoonsgegevens is niet in één wet te vinden. De Algemene Verordening Gegevensverwerking (hierna: AVG) vormt de basis, maar de diverse organisaties en professionals in de samenwerkingsverbanden hebben ook te maken met andere wet- en regelgeving zoals de Wet geneeskundige behandelovereenkomst (hierna: WGBO), de Jeugdwet (hierna: Jw), de Wet politiegegevens (hierna: Wpg), de Wet Justitiële en strafvorderlijke gegevens (hierna: Wjsg) en de Reclasseringsregeling 1995.

Het is hierbij goed om voor ogen te houden dat het uitwisselen van gegevens, maar ook het correct toepassen van de privacyregels een belangrijk doel dient. De samenwerking tussen het zorg- en veiligheidsdomein is gericht op hulp aan burgers die kampen met (complexe) multi-problematiek ten behoeve van een veilige samenleving. Om die hulp effectief te laten zijn, is het belangrijk dat deze personen vertrouwen hebben en houden in zorgprofessionals en zorginstellingen, in de Raad voor de Kinderbescherming, reclasseringsinstellingen, het Openbaar Ministerie, politie, gemeenten en andere overheden. Dat houdt onder andere in dat men er van op aan kan dat er bij het omgaan met zijn/haar persoonsgegevens zorgvuldigheid wordt betracht. Even belangrijk is dat partners in de samenwerking erop kunnen vertrouwen dat alle partners zorgvuldig met persoonsgegevens omgaan.

Het toepassen van de verschillende wettelijke regels kan soms lastig zijn, bijvoorbeeld omdat de wetgeving niet altijd een pasklaar antwoord biedt op de vraag of gegevens uitgewisseld mogen worden. Soms ervaren de betrokken organisaties en professionals de privacyregels als een probleem. Inzicht in de mogelijkheden die andere partijen hebben om persoonsgegevens uit te wisselen, kan helpen bij het maken van afwegingen over het uitwisselen van persoonsgegevens. Met dit handvat beogen wij de relevante wet- en

regelgeving van de organisaties die deelnemen aan samenwerkingsverbanden, in kaart te brengen. Met als doel een eenduidige uitleg van de kaders waarbinnen professionals binnen het samenwerkingsverband kunnen opereren.

In deze nieuwe versie van het handvat zijn de raakvlakken en verbindingen breder beschreven dan in het eerste handvat is gedaan. Daarom overstijgt dit handvat het domein van de zorg- en veiligheidshuizen en kan het van toepassing zijn voor meerdere samenwerkingsverbanden in het zorg- en veiligheidsdomein waar sprake is van de aanpak van (complexe) casuïstiek.

1.3 Initiatiefnemers

Dit handvat is opgesteld door de organisaties uit het zorg- en veiligheidsdomein: Nationale Politie, Openbaar Ministerie, GGZ Nederland, Leger des Heils Jeugdbescherming en Reclassering, Jeugdzorg Nederland, Reclassering Nederland, Raad voor de Kinderbescherming, Vereniging Nederlandse Gemeenten, Slachtofferhulp Nederland, de Dienst Justitiële Inrichtingen, Aedes vereniging van woningcorporaties, de Landelijke Vereniging van Managers Veiligheidshuizen, Halt, en het Ministerie van Justitie en Veiligheid.

1.4 Leeswijzer

In dit handvat wordt in hoofdstuk 2 eerst de algemene wet- en regelgeving ten aanzien van privacy en het verwerken van persoonsgegevens besproken. Vervolgens wordt in hoofdstuk 3 naar de regelgeving per organisatie gekeken. In hoofdstuk 4 wordt aandacht besteed aan de praktische invulling van de samenwerking in een samenwerkingsverband in het zorg- en veiligheidsdomein.

In bijlage 1 zijn de kernbegrippen uit de AVG opgenomen. In bijlage 2, 3, en 4 zijn de documenten opgenomen die laten zien hoe dit handvat is uitgewerkt voor de samenwerking in de zorg- en veiligheidshuizen. Het betreft de volgende documenten: vertaling van handvat naar praktijk, modelconvenant voor de zorg- en veiligheidshuizen, en model protocol voor de zorg- en veiligheidshuizen. In bijlage 5 zijn de gegevens opgenomen van de organisaties die hebben meegewerkt aan dit handvat en de contactpersonen van deze organisaties voor vragen over dit handvat.

2 Algemeen juridisch kader gegevensverwerking

Dit hoofdstuk gaat in op de regels die gelden voor het omgaan met persoonsgegevens in het algemeen, waarbij met name gekeken wordt naar de bepalingen die hierover zijn vastgelegd in de Algemene Verordening Gegevensverwerking en de Uitvoeringswet Algemene Verordening Gegevensverwerking. De grondslagen uit artikel 6 AVG worden in dit hoofdstuk nader uitgewerkt.

2.1 Grondrecht op privacy

In artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) is bepaald dat iedereen recht heeft op respect voor zijn of haar privé leven, familie- en gezinsleven, woning en correspondentie. Ingevolge het tweede lid van dit artikel is geen inmenging van enig openbaar gezag toegestaan in de uitoefening van dit recht, dan voor zover bij wet voorzien en indien voldaan is aan de voorwaarden zoals opgesomd in het tweede lid van dit artikel. Ook in nationale wetgeving (artikel 10 van de Grondwet) is bepaald dat een ieder recht heeft op eerbiediging van zijn of haar persoonlijke levenssfeer. Het grondrecht op privacy strekt zich ook uit tot de bescherming van persoonlijke informatie (persoonsgegevens). Zo wordt in artikel 8 van het Handvest van de grondrechten van de Europese Unie bepaald dat een ieder recht heeft op bescherming van de hem of haar betreffende persoonsgegevens en in lid 2 dat deze gegevens eerlijk verwerkt moeten worden. In lagere landelijke wetgeving wordt dit verder uitgewerkt. In die wetgeving, die niet altijd hoofdzakelijk op privacy is gericht, zijn ook bepalingen opgenomen die in meer specifieke omstandigheden eisen stellen aan de omgang met persoonsgegevens en de bescherming van de persoonlijke levenssfeer van het individu.

2.2 Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet (UAVG)

Op 25 mei 2018 is de Algemene Verordening Gegevensverwerking (hierna: AVG) in werking getreden. De AVG heeft de oude Wet Bescherming Persoonsgegevens vervangen. In de AVG staan de rechten en plichten genoemd met betrekking tot privacy. De AVG heeft rechtstreekse werking in Nederland. De Uitvoeringswet Algemene Verordening Gegevensverwerking (hierna: UAVG) geeft in Nederland uitvoering aan de AVG. In de UAVG worden de regels uit de AVG nader uitgewerkt.

Naast de AVG en de UAVG zijn er ten aanzien van de verwerking en het verstrekken van persoonsgegevens ook andere wetten van toepassing. Dit zijn voornamelijk materiewetten die bepalingen bevatten op grond waarvan een partner gegevens mag verwerken en onder welke voorwaarden. Organisaties die samenwerken bij het behandelen van casussen in het zorg- en veiligheidsdomein hebben bijvoorbeeld te maken met de Jeugdwet en de WMO, de Wjsg en de Wpg en andere specifieke wetten vanuit hun eigen organisatie. De regels die in deze (materie)wetten zijn opgenomen gaan vóór op de regels van de AVG. Als er geen specifieke bepaling opgenomen is in de wet dan gelden de regels uit de AVG.

In hoofdstuk 3 wordt nader gekeken naar de organisaties die kunnen deelnemen aan een samenwerkingsverband en naar de verschillende (materie)wetten die van toepassing zijn.

2.2.1 De beginselen van de AVG

De AVG kent een aantal beginselen die voor iedere verwerking van persoonsgegevens gelden:

- Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (**"rechtmatigheid, behoorlijkheid en transparantie"**) (artikel 5 lid 1 onder a AVG). Dat betekent dat persoonsgegevens door publieke organisaties (zoals overheidsorganen) of private organisaties met een wettelijke taak alleen mogen worden verwerkt wanneer de rechtsgrond voorspelbaar is op grond van een wettelijke taak: er moet sprake zijn van Europese of nationale wet- en regelgeving waarin de wettelijke taak staat verwoord. Wanneer een private organisatie geen wettelijke taak heeft, dan moet een van de andere limitatief genoemde grondslagen zoals genoemd in artikel 6 AVG van toepassing zijn. Ook moet duidelijk zijn voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt;
- Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (**"doelbinding"**) (artikel 5 lid 1 onder b AVG).[2] Een doel is pas gerechtvaardigd als er een grondslag is in artikel 6 van de AVG danwel in een andere wet die fungeert als een lex specialis, waarop de verwerking kan worden gebaseerd;
- Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (**"minimale gegevensverwerking"**) (artikel 5 lid 1 onder c AVG). Er mogen niet meer persoonsgegevens worden verwerkt dan voor het doel van de gegevensverwerking **noodzakelijk** is. De verwerking moet de subsidiariteits- en proportionaliteitstoets doorstaan. Dit houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot het te dienen doel van de verwerking. Bovendien mag dit doel in redelijkheid niet op een andere, voor de betrokkene minder nadelige, wijze kunnen worden gerealiseerd. Dit betekent dat wanneer er een wettelijke grondslag voor gegevensverwerking op grond van artikel 6 AVG is, óók altijd – dus bij iedere afzonderlijke gegevensverstrekking - weer moet worden voldaan aan de noodzakelijkheidstoets! Een bovenmatige gegevensverwerking is onrechtmatig;
- Persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren **("juistheid"**) (artikel 5 lid 1 onder d AVG);
- Persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkene niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is ("**opslagbeperking"**) (artikel

[2] Hierop zijn echter wel uitzonderingen mogelijk (art 6 lid 4 AVG)

5 lid 1 onder e AVG). Persoonsgegevens mogen daarnaast niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze verwerkt zijn;
- Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (**"integriteit en vertrouwelijkheid"**) (artikel 5 lid 1 onder f AVG);
- Bijzondere en strafrechtelijke persoonsgegevens mogen niet worden verwerkt, tenzij een wet dit uitdrukkelijk toestaat (artikel 9 lid 1 en 10 AVG) .

De verwerkingsverantwoordelijke is op grond van artikel 5 lid 2 AVG verantwoordelijk voor de naleving van de beginselen zoals genoemd in art. 5 lid 1 AVG en kan dit aantonen (**"verantwoordingsplicht"**).

Doel

Volgens de beginselen van de AVG dient de verwerking van persoonsgegevens een duidelijk doel te hebben. Het doel speelt op twee niveaus. Aan de ene kant is er een maatschappelijk doel. Door persoonsgegevens met elkaar te uit te wisselen en te verwerken kunnen bijvoorbeeld maatschappelijke problemen beter opgelost worden. Daarnaast dient het een concreet doel. Er kan bijvoorbeeld met meerdere partijen bij een casusoverleg problematiek in kaart gebracht worden.

2.2.2 Zorgvuldigheidsnormen

Naast de algemene uitgangspunten staat er ook een aantal beheersmatige eisen in de AVG en de UAVG waaraan de verwerking van de persoonsgegevens moet voldoen.
De zorgvuldigheidsnormen die relevant zijn voor de gegevensverwerking in een samenwerkingsverband worden hieronder kort beschreven:

Verantwoording

- **Registerplicht**: de verwerkingsverantwoordelijk is verplicht een register van verwerkingsactiviteiten bij te houden (artikel 30 AVG).
- Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze in een onderlinge regeling hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van de verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene (artikel 26 AVG).
- **Functionaris voor gegevensbescherming**: overheidsinstanties moeten altijd een functionaris voor gegevensbescherming hebben. Voor bedrijven en instellingen geldt dit vereiste in bepaalde gevallen (artikel 37 e.v. AVG).

Beveiliging

- De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen ter beveiliging van de persoonsgegevens (artikel 32 AVG).
- Privacy door ontwerp (**'*privacy by design*'**) en privacy door standaardinstellingen (**'*privacy by default*'**) houdt in dat de verwerkingsverantwoordelijke privacy en

gegevensbescherming meeneemt als eisen bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt (artikel 25 AVG).

- De verwerkingsverantwoordelijke moet onder omstandigheden een **datalek melden** bij de Autoriteit Persoonsgegevens en de betrokkenen (artikel 33 en 34 AVG).

Rechten van betrokkenen

- Een betrokkene moet door de verwerkingsverantwoordelijke uitvoerig geïnformeerd worden als zijn of haar persoonsgegevens worden verwerkt (artikel 13 en 14 AVG). Een betrokkene heeft het recht om te weten wat er met zijn of haar persoonsgegevens gebeurt en waarom. Ook moet hij of zij bewust worden gemaakt van de risico's van de gegevensverwerking, de regels die ervoor gelden, de waarborgen en de rechten die hij of zij heeft ten aanzien van de gegevensverwerking. Ook als de gegevens gebruikt worden voor een ander doel dan waarvoor ze verzameld zijn, moet de betrokkene daarover geïnformeerd worden. In specifieke situaties hoeft een verwerkingsverantwoordelijke geen gehoor te geven aan de rechten van betrokkenen. De uitzonderingen staan genoemd in artikel 23 AVG en worden nader uitgewerkt in artikel 41 UAVG of in andere (materie) wetgeving.

Daarnaast moet een betrokkene door de verwerkingsverantwoordelijke op de volgende rechten gewezen worden.

- het **recht op informatie**: een betrokkene heeft het recht om een instelling/organisatie te vragen of er persoonsgegevens over hem of haar zijn verwerkt en zo ja: aan wie deze gegevens zijn verstrekt;
- het **recht op inzage en afschrift**: een betrokkene heeft recht op inzage in en een afschrift van de gegevens die op hem of haar betrekking hebben (artikel 15 AVG);
- het **recht op rectificatie**: een betrokkene kan ingeval de over hem of haar verwerkte gegevens feitelijk onjuist of onvolledig zijn de instelling verzoeken om de gegevens te corrigeren, aan te vullen of te verwijderen (artikel 16 AVG);
- het **recht op vergetelheid**: de betrokkene heeft het recht om wissing van zijn of haar persoonsgegevens te vragen (artikel 17 AVG);
- het **recht op beperking**: de betrokkene heeft de mogelijkheid om de verwerking van de persoonsgegevens tijdelijk stil te laten zetten (artikel 18 AVG);
- het **recht van bezwaar**: een betrokkene kan onder omstandigheden bezwaar maken tegen de verwerking van zijn of haar persoonsgegevens in verband met zijn of haar bijzondere persoonlijke omstandigheden (artikel 21 AVG);
- Wanneer er sprake is van een gezamenlijke verwerkingsverantwoordelijken dan wordt de wezenlijke inhoud van de onderlinge regeling aan de betrokkene beschikbaar gesteld (artikel 26 lid 2 AVG).

2.2.3 Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens is de nationale toezichthouder en als zodanig belast met het toezicht op de naleving van de bepalingen uit de AVG en de overige

privacywetgeving. De belangrijkste taak is het monitoren en handhaven van de toepassing van de AVG.

Voor de uitvoering van haar taken heeft de Autoriteit Persoonsgegevens verschillende bevoegdheden gekregen: onderzoeksbevoegdheden, de bevoegdheid tot het nemen van corrigerende maatregelen en een boetebevoegdheid. In artikel 57 en 58 AVG en in hoofdstuk 2 van de UAVG zijn de taken en de bevoegdheden van de Autoriteit Persoonsgegevens geregeld.

2.3 Persoonsgegevens

De AVG is van toepassing wanneer er sprake is van verwerking van persoonsgegevens. Persoonsgegevens zijn gegevens die '*een natuurlijk persoon identificeren of aan de hand waarvan een natuurlijke persoon geïdentificeerd kan worden*' (artikel 4 lid 1 AVG).

Gegevens die geen betrekking hebben op een geïdentificeerd of identificeerbaar persoon vallen buiten het bereik van de AVG. Hiervan is bijvoorbeeld sprake wanneer over groepen personen als geheel gegevens worden verwerkt. Een voorbeeld hiervan is: *'in een wijk is een groep van ongeveer vijftien jongens actief. Deze groep hangt rond en maakt zich schuldig aan kleine criminaliteit.'* Privacywetgeving is hierop niet van toepassing en de gegevens mogen vrij worden verstrekt. Wanneer de gegevens echter de individuele leden van een groep of individuele personen betreft, is sprake van verwerking van persoonsgegevens en zijn de privacyregels wel van toepassing. Een voorbeeld hiervan is: *'Sara Janssen en Johan Pieterse zijn de leiders van de groep in Sterrenwijk. Sara en Johan hebben geen aantekening in de Justitiële Documentatie en vertonen agressief gedrag'.*

Bijzondere en strafrechtelijke persoonsgegevens
De AVG kent daarnaast nog een bijzonder regime voor bijzondere persoonsgegevens en voor strafrechtelijke persoonsgegevens. Onder **bijzondere persoonsgegevens** vallen bijvoorbeeld gegevens die iets zeggen over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging (artikel 9 AVG).
Strafrechtelijke persoonsgegevens betreffen persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen en persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag (artikel 10 AVG).

Wanneer deze gegevens verwerkt worden, zorgt dit voor een grotere inbreuk op de persoonlijke levenssfeer van de betrokken personen. De hoofdregel is dat deze persoonsgegevens níet mogen worden verwerkt (verwerkingsverbod), tenzij er een specifieke wettelijke uitzondering is die de verwerking legitimeert. In paragraaf 2.5 wordt nader ingegaan op deze uitzonderingen.

'Dat'-gegevens of 'Buitenkant'-informatie
In de praktijk wordt regelmatig gesproken over '*dát-gegevens'* of *'buitenkantinformatie'*. Daarmee wordt het gegeven bedoeld dát een organisatie bij de casus is betrokken zonder

vermelding van andere gegevens over de betrokkene of de inhoud van de hulpverlening, de begeleiding of de ondersteuning.
Ook ‘dát’-gegevens en ‘buitenkant’-informatie moeten als persoonsgegevens worden beschouwd waarop de AVG en/of sectorale wetgeving van toepassing is. Het gegeven dát iemand patiënt is van een GGZ-instelling is een bijzonder persoonsgegeven (gezondheidsgegeven). Het gegeven dát iemand als verdachte, slachtoffer of getuige voorkomt in de politiesystemen is een politiegegeven. Het gegeven dát iemand cliënt is van de reclassering is een strafrechtelijk persoonsgegeven. In bepaalde situaties kan de afweging op grond van het noodzakelijkheidsbeginsel als uitkomst hebben dat het voldoende is om alleen ‘dát’-gegevens of ‘buitenkant’-informatie te verstrekken.

2.4 Grondslagen voor verwerking van persoonsgegevens

De verwerking van persoonsgegevens is alleen mogelijk (en rechtmatig) als aan één van de voorwaarden wordt voldaan uit artikel 6 van de AVG. De AVG kent zes verschillende grondslagen. Bij samenwerking bij casuïstiek in het zorg- en veiligheidsdomein zijn vooral de grondslagen c en e belangrijk. Voor de volledigheid worden wel alle grondslagen in de volgende paragrafen nader uitgewerkt.

GRONDSLAGEN

a) de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn of haar 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** die 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

2.4.1 Toestemming

Persoonsgegevens mogen worden verwerkt als de betrokkene hiervoor toestemming heeft gegeven. Om te spreken van geldige toestemming, moet de toestemming aan een aantal voorwaarden voldoen. De voorwaarden van toestemming zijn uitgewerkt in artikel 7 AVG.

Vrij

Ten eerste moet de toestemming vrij gegeven zijn. Dit houdt in dat iemand daadwerkelijk de keuze moet hebben om te weigeren, zonder dat hier negatieve consequenties aan verbonden zijn. Met name wanneer er sprake is van een afhankelijkheidsrelatie, bijvoorbeeld in de arbeidssfeer of in de relatie overheid-burger, zal toestemming niet snel vrij zijn gegeven.

Specifiek en geïnformeerd

Ten tweede moet toestemming specifiek zijn en geïnformeerd. De betrokkene moet geïnformeerd worden over de reden(en) van de verwerking van de persoonsgegevens (het doel), maar ook over andere zaken die van belang zijn om te zorgen dat de betrokkene een goed geïnformeerd besluit kan nemen. Hierbij valt te denken aan de manier waarop de persoonsgegevens verwerkt worden, aan wie de persoonsgegevens eventueel verstrekt worden en hoe lang de gegevens bewaard worden. Voor iedere verstrekking dient opnieuw toestemming te worden gevraagd. Algemene toestemmingsverklaringen zijn niet toegestaan.

Ondubbelzinnig

Tenslotte moet toestemming ondubbelzinnig zijn. Er mag geen twijfel bestaan over het feit dat de betrokkene toestemming heeft gegeven. De bewijslast ligt bij de verwerkingsverantwoordelijke. Toestemming kan blijken uit een ondubbelzinnige wilsuiting of uit een ondubbelzinnige, actieve handeling van de betrokkene. Als toestemming wordt gegeven in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, moet aan de betrokkene in duidelijke en eenvoudige taal het onderscheid aangegeven worden tussen dat waarvoor de betrokkene toestemming geeft en de andere aangelegenheden.

Intrekken

De betrokkene mag te allen tijde zijn of haar toestemming intrekken. Deze intrekking heeft geen invloed op de legitimiteit van de verwerkingen vóór de intrekking, maar vanaf het moment dat iemand zijn toestemming intrekt, mogen de persoonsgegevens niet meer worden verwerkt. De betrokkene dient van dit recht op de hoogte gesteld te worden voordat hij of zij toestemming heeft verleend voor de verwerking van de persoonsgegevens. De intrekking van de toestemming is geregeld in artikel 7 AVG[3].

[3] Dit speelt alleen als 'toestemming' de AVG-grondslag is op basis waarvan een partij gegevens verwerkt. Bij het behandelen van casuïstiek in het Zorg- en Veiligheidsdomein is echter – m.u.v. in sommige gevallen Slachtofferhulp Nederland – een van de andere grondslagen van toepassing. Daarnaast biedt Artikel 23 van de AVG uitzonderingsgronden met betrekking tot de rechten van de betrokkene. O.a. als bij Uniestatelijke of lidstatelijke wetgeving beperkingen zijn opgelegd ter waarborging van de nationale veiligheid, openbare veiligheid, opsporing en vervolging van strafbare feiten, of belangrijke doelstellingen van algemeen belang zoals de volksgezondheid en sociale zekerheid.

In artikel 8 AVG worden extra voorwaarden genoemd voor de toestemming in de gevallen dat er persoonsgegevens van minderjarigen verwerkt worden:

- Wanneer het kind jonger is dan 16 jaar, is verwerking slechts rechtmatig indien ook de wettelijke vertegenwoordiger(s) toestemming hebben gegeven.
- Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die wettelijke vertegenwoordiger(s) is, toestemming heeft gegeven of een machtiging tot toestemming heeft verleend.

2.4.2 Uitvoeren van een overeenkomst

Deze grondslag kan gebruikt worden als voor het uitvoeren/naleven van een overeenkomst het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben. Een voorbeeld is het aangaan van een huurovereenkomst.

2.4.3 Wettelijke verplichting

Deze grondslag ziet op een uitdrukkelijk in de wet vastgelegd voorschrift. Zo is bijvoorbeeld in de Jeugdwet opgenomen dat een jeugdzorgwerker een dossier moet aanleggen en de gegevens mag vastleggen die relevant zijn voor de jeugdhulp. In de Wet op de schuldhulpverlening staat dat bestuursorganen verplicht zijn om relevante gegevens voor de schuldhulpverlening te verstrekken aan het College van burgemeester en wethouders.

2.4.4 Vitale belangen van de betrokkene

Het gaat hier om de situatie dat gegevensverwerking noodzakelijk is om een levensbelang of ander vitaal gezondheidsbelang van de betrokkene te beschermen en het niet mogelijk is om deze persoon om toestemming te vragen. Deze grondslag is van toepassing wanneer er sprake is van acuut gevaar en/of de betrokkene bewusteloos is en niet in staat is om toestemming te geven.

2.4.5 Vervulling van een taak van algemeen belang/ taak uitoefening van het openbaar gezag

Het gaat hier om (overheids-) taken die de wet uitdrukkelijk heeft opgedragen aan de verwerkingsverantwoordelijke. Bijvoorbeeld de wettelijke taak van het College van burgemeester en wethouders om te beslissen over een aanvraag voor jeugdhulp of een voorziening voor maatschappelijke ondersteuning en de wettelijke taak van de Raad voor de Kinderbescherming om zorg te dragen voor de kinderbescherming in Nederland. De verwerking moet in deze gevallen altijd een grondslag hebben in een (materie) wet, waarin ook het doel van de verwerking staat. In die wet moet zijn vastgesteld wie de taak uitvoert of aan wie het openbaar gezag is opgedragen. Dit kunnen zowel publiekrechtelijke als privaatrechtelijke organisaties zijn.

2.4.6 Gerechtvaardigde belangen

Een overheidsinstantie mag zich niet op deze grondslag baseren maar mag enkel op grond van een andere grondslag gegevens verwerken. Andere instanties kunnen zich enkel op deze grondslag baseren als aan drie voorwaarden wordt voldaan: er is een gerechtvaardigd belang, de verwerking is noodzakelijk en er is een afweging gemaakt

tussen de eigen belangen en de belangen van de personen van wie de persoonsgegevens worden verwerkt waaruit is gebleken dat het gerechtvaardigde belang van de verwerkingsverantwoordelijke zwaarder weegt dan het belang van de betrokkene op de bescherming van zijn persoonsgegevens.

2.5 Verwerking bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens

In artikel 9 AVG staat dat de verwerking van bijzondere persoonsgegevens verboden is, tenzij er aan één van de in lid 2 van dat artikel genoemde voorwaarden is voldaan. In artikel 22 e.v. van de UAVG zijn deze voorwaarden nader uitgewerkt. In het kader van de samenwerking in het zorg- en veiligheidsdomein zijn de volgende algemene uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken relevant:

- de betrokkene heeft **uitdrukkelijke toestemming** gegeven voor de verwerking van die persoonsgegevens voor een of meer bepaalde doelen, behalve indien in Europese of nationale wetgeving is bepaald dat het verwerkingsverbod niet door de betrokkene kan worden opgeheven;
- de verwerking is noodzakelijk ter bescherming van de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn of haar toestemming te geven;
- de verwerking heeft betrekking op persoonsgegevens die door de betrokkenen **kennelijk openbaar** zijn gemaakt;
- de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang.

Gezondheidsgegevens

Naast de algemene uitzonderingen zijn er een aantal specifieke uitzonderingen per categorie van bijzondere persoonsgegevens. In het kader van de gegevensuitwisseling in een samenwerkingsverband zijn met name de volgende uitzonderingen voor het verwerken van gezondheidsgegevens van belang (artikel 30 UAVG):

- Scholen mogen gezondheidsgegevens verwerken wanneer dit noodzakelijk is voor de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheid;
- Een reclasseringsinstelling, bijzondere reclasseringsambtenaren, de Raad voor de Kinderbescherming en gecertificeerde instellingen mogen gezondheidsgegevens verwerken voor zover dit noodzakelijk is voor de uitvoering van de aan hen opgedragen wettelijke taken;
- Hulpverleners en instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening mogen gezondheidsgegevens verwerken indien dit noodzakelijk is voor de goede behandeling of verzorging van de betrokkenen.

Artikel 10 AVG ziet toe op het verwerkingsverbod van strafrechtelijke persoonsgegevens. De AVG biedt zelf geen uitzonderingen op dit verbod. In artikel 32 en 33 UAVG is bepaald wanneer persoonsgegevens van strafrechtelijke aard wel mogen worden verwerkt. In het kader van dit handvat zijn de volgende algemene uitzonderingen van belang:

- de betrokkene heeft **uitdrukkelijke toestemming** gegeven voor de verwerking van die persoonsgegevens voor een of meer bepaalde doelen;
- de verwerking is noodzakelijk ter bescherming van de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn of haar toestemming te geven;
- de verwerking heeft betrekking op persoonsgegevens die door de betrokkenen **kennelijk openbaar** zijn gemaakt;

Daarnaast kent de UAVG specifieke uitzonderingsgronden voor de verwerking van strafrechtelijke persoonsgegevens:
- verwerkingen door verwerkingsverantwoordelijken die zijn belast met de toepassing van het strafrecht, of door verwerkingsverantwoordelijken die de gegevens op grond van de Wpg of de Wjsg hebben gekregen (artikel 33 lid 1 sub a UAVG);
- de verwerking is noodzakelijk in aanvulling op de verwerking van persoonsgegevens over gezondheid, zoals bedoeld in artikel 30 lid 3 sub a met het oog op een goede behandeling of verzorging van betrokkene (artikel 33 lid 1 sub c UAVG);

In hoofdstuk 3 worden de wettelijke kaders per ketenpartner uiteengezet en wordt gekeken of en in welke materiewetgeving geregeld is of een partij bijzondere en strafrechtelijke gegevens mag gebruiken.

2.6 Richtlijn Gegevensbescherming Opsporing en Vervolging

De AVG geldt niet voor bevoegde autoriteiten bij de uitvoering van hun taken voor de opsporing en vervolging van strafbare feiten en tenuitvoerlegging van straffen. Daarvoor geldt de ‘Richtlijn gegevensbescherming opsporing en vervolging’ (Richtlijn EU.2016/680). Deze richtlijn is in Nederland geïmplementeerd in de - reeds - bestaande Wpg en de Wjsg. Voor wat betreft de politie geldt dat ook de taken ter bescherming van de openbare orde en de hulpverleningstaken van de politie vallen onder de werking van de Wpg. Voor andere taken van politie (zoals vreemdelingenzaken) en voor andere taken van het OM is de AVG wel van toepassing.

De verwerking van persoonsgegevens is alleen rechtmatig indien en voor zover die verwerking noodzakelijk is voor de uitvoering van een taak door een bevoegde autoriteit voor de bovengenoemde doeleinden. In nationale wetgeving kunnen situaties opgenomen worden die regelen dat ook voor andere doelen kan worden verstrekt. In hoofdstuk 3 wordt per ketenpartner gekeken of dit het geval is.

In de Wpg en Wjsg wordt een onderscheid gemaakt tussen de verschillende categorieën van betrokkenen. Er dient een duidelijk onderscheid gemaakt te worden tussen persoonsgegevens van:
- personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
- personen die voor een strafbaar feit zijn veroordeeld;

- slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer kunnen worden van een strafbaar feit;
- andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek of informatie kunnen verstrekken.

2.7 Beroepsgeheim

Vrijwel alle beroepskrachten die werkzaam zijn in het zorg- en veiligheidsdomein hebben een beroepsgeheim. Dit beroepsgeheim is neergelegd in verschillende wetten en verdragen. Kern van het beroepsgeheim is dat de beroepskracht toestemming van zijn of haar cliënt nodig heeft om informatie over hem of haar met anderen uit te wisselen. De bedoeling van het beroepsgeheim is om de drempel tot de hulpverlening zo laag mogelijk te houden.
In een aantal gevallen mag een beroepsgeheim doorbroken worden:
- Met uitdrukkelijke toestemming van de betrokkene;
- Voor het delen van gegevens met anderen die rechtstreeks bij de behandeling zijn betrokken, als het gaat om gegevens die noodzakelijk zijn voor de door de vervanger te verrichten werkzaamheden;
- Bij een wettelijk meldrecht;
- Bij een conflict van plichten.

Het zal geregeld voorkomen dat het vragen van toestemming niet mogelijk is of dat de betrokkene weigert om toestemming te geven voor het verstrekken van zijn of haar persoonsgegevens aan een ontvanger of de betrokkene zijn of haar toestemming later intrekt.
In een aantal (uitzonderings-)situaties is een hulpverlener bevoegd of om zijn of haar beroepsgeheim te doorbreken en ook zonder toestemming gegevens te verstrekken.

Wettelijk meldrecht
Wanneer een hulpverlener grote zorgen heeft over een betrokkene, dan heeft hij het recht om dit te melden. Het is daarbij noodzakelijk dat er een afweging gemaakt wordt. We kennen de volgende wettelijke meldrechten:
- Advies- en Meldpunt Kindermishandeling en Huiselijk geweld (Veilig Thuis): bij vermoedens van kindermishandeling of huiselijk geweld (artikel 5.2.6 WMO). Men kan pas melden als de stappen uit de Meldcode Kindermishandeling en Huiselijk Geweld zijn doorlopen. Dit geldt niet voor de politie;
- Raad voor de Kinderbescherming: wanneer dit noodzakelijk is voor de uitvoering van de taken van de Raad voor de Kinderbescherming zoals een onderzoek naar de noodzaak van een kinderbeschermingsmaatregel (artikel 1:240 BW);
- Verwijsindex Risicojongeren (artikel 7.1.2.1 Jw).
- Gezinsvoogd die namens de GI een ondertoezichtstelling uitvoert. Artikel 7.3.11 vierde lid Jw. bepaalt dat derden die beroepshalve beschikken over informatie over een onder toezicht gestelde jeugdige of diens ouders/verzorgers/voogd, welke informatie noodzakelijk kan worden geacht voor de uitvoering van de ondertoezichtstelling, deze informatie aan de GI verstrekken. De informatie kan uit

eigen beweging of op verzoek van de GI worden verstrekt. Hiervoor is geen toestemming van betrokkenen nodig en de informatie kan indien nodig met doorbreking van de geheimhoudingsverplichting worden verstrekt. Het gaat hier niet alleen om hulpverleners die direct bij het kind zijn betrokken, maar ook om hulpverleners die betrokken zijn bij andere gezinsleden. Ook de jeugdhulpaanbieder die een medische behandeling biedt die onder de Wgbo valt, heeft de verplichting relevante informatie te verstrekken. De verplichte informatieverstrekking ziet alleen op de ondertoezichtstelling en geldt dus niet als sprake is van voogdij of jeugdreclassering.

Conflict van plichten
De essentie van een conflict van plichten is dat de hulpverlener dient te zwijgen op grond van zijn of haar geheimhoudingsplicht, maar dat hij of zij zich tegelijkertijd (moreel) verplicht kan voelen om derden informatie te verschaffen om gevaar af te wenden. Het is in die gevallen noodzakelijk dat er een belangafweging wordt gemaakt, waarbij de volgende criteria moeten worden afgewogen:

- bij het niet-doorbreken van het beroepsgeheim ontstaat naar alle waarschijnlijkheid ernstige schade voor de betrokkene of een ander;
- er is geen andere weg dan doorbreking van het beroepsgeheim om het te verwachten gevaar af te wenden;
- het is vrijwel zeker dat door de doorbreking van het beroepsgeheim schade aan de betrokkene of anderen kan worden voorkomen of beperkt;
- de hulpverlener verkeert in gewetensnood door het handhaven van zijn of haar zwijgplicht;
- de hulpverlener heeft alles in het werk gesteld om toestemming van de betrokkene te krijgen om informatie te verstrekken aan derden.

Al deze criteria moeten van toepassing zijn voordat het (medisch) beroepsgeheim doorbroken mag worden.

Om de geheimhoudingsplicht te doorbreken moet er dus naast een grondslag voor de verwerking van persoonsgegevens, zoals bedoeld in artikel 6 AVG, eveneens een grond voor de doorbreking van de geheimhoudingsplicht zijn.

2.8 Toestemming

Bij het spreken over de regels over het omgaan met privacy, bij het omgaan met het beroepsgeheim en bij hulpverlening wordt geregeld de term toestemming gebruikt. Dat geldt ook voor dit handvat. De term toestemming heeft echter verschillende betekenissen en heeft andere consequenties, een en ander is afhankelijk van de context waarin er over toestemming gesproken wordt. In deze paragraaf wordt kort stilgestaan bij de verschillende wijzen waarop en de verschillende contexten waarin de term toestemming gebruikt kan worden.

2.8.1 Toestemming als grondslag voor gegevensverwerking
Een van de grondslagen uit de AVG op grond waarvan persoonsgegevens kunnen worden verwerkt is toestemming van de betrokkene. Persoonsgegevens mogen dan worden

verwerkt als de betrokkene hiervoor toestemming heeft gegeven. Om te spreken van geldige toestemming, moet de toestemming aan een aantal voorwaarden voldoen, zie hierboven in paragraaf 2.4.1.

Deze grondslag voor het verwerken van persoonsgegevens zal in het zorg- en veiligheidsdomein nauwelijks een rol spelen. In een rapport uit 2016[4] heeft de Autoriteit Persoonsgegevens geconcludeerd dat er van vrije toestemming in het sociaal domein vaak geen sprake zal zijn. Er is immers in de meeste gevallen sprake van een afhankelijkheidsrelatie tussen de betrokkene en de instantie/organisatie die om de toestemming vraagt. Daarbij zal het weigeren van toestemming voor de gegevensverwerking veelal (negatieve) gevolgen hebben voor de betrokkene.

2.8.2 Toestemming voor het doorbreken van het beroepsgeheim

Zoals in paragraaf 2.7 uiteengezet hebben vrijwel alle beroepskrachten in het zorg- en veiligheidsdomein een beroepsgeheim.
Dit beroepsgeheim verhindert in beginsel dat inlichtingen worden verstrekt aan derden.
In een aantal gevallen mag een beroepsgeheim doorbroken worden:

- Met uitdrukkelijke toestemming van de betrokkene;
- Voor het delen van gegevens met anderen die rechtstreeks bij de behandeling zijn betrokken, als het gaat om gegevens die noodzakelijk zijn voor de door de vervanger te verrichten werkzaamheden;
- Bij een wettelijk meldrecht;
- Bij een conflict van plichten;
- Indien er een specifieke wettelijke verplichting dan wel bevoegdheid is.

Toestemming kan dus een grond zijn waarop een beroepsgeheim doorbroken kan worden en de beroepskracht gegevens kan verstrekken aan derden.

2.8.3 Toestemming voor (vrijwillige) hulpverlening

Veel hulpverlening in het zorg- en veiligheidsdomein vindt plaats op vrijwillige basis. Denk daarbij aan hulpverlening door een wijkteam, in het kader van de ggz, door een jeugdhulpaanbieder, door slachtofferhulp.
Basis voor het starten van deze hulpverlening is de toestemming van de betrokkene. Het is in veel gevallen de betrokkene die een hulpvraag heeft en zich daarvoor (vrijwillig) wendt tot de daartoe geschikte instantie.

De toestemming voor het starten van de hulpverlening dient onderscheiden te worden van de toestemming voor het verstrekken van gegevens aan derden, al dan niet met doorbreking van het beroepsgeheim.
Het feit dat een betrokkene instemt met de hulpverlening betekent dus niet dat deze toestemming ook de grondslag is voor de bijbehorende verwerking (zoals het uitwisselen) van persoonsgegevens. Daarvoor moet er immers sprake zijn van vrije, specifieke en op informatie berustende toestemming. En als dat niet mogelijk is moet er dus een andere grondslag uit artikel 6 van de AVG zijn.

[4] Autoriteit Persoonsgegevens april 2016: De rol van toestemming in het sociaal domein.

2.9 Drang

In het sociaal domein wordt geregeld de term ‘drang’ genoemd. Onder drang verstaan we vrijwillige hulpverlening waarbij sprake is van intensivering van de hulp middels een actieve, indringende en soms confronterende aanpak, bijvoorbeeld omdat hulp wordt vermeden of afgewezen. Het is van belang voor ogen te houden dat drang feitelijk vrijwillige hulpverlening, ondersteuning en/of begeleiding is waar betrokkenen toestemming voor moeten geven. De betrokkene kan niet gedwongen worden om mee te werken.

Als een betrokkene dan echter nog steeds niet wil meewerken c.q. de hulp weigert, dan is de enige mogelijkheid om de hulpverlening op te schalen naar hulpverlening binnen een gedwongen kader, maar er moet dan wel een noodzaak zijn tot onvrijwillige zorg. Daarmee is de fase van drang voorbij. Betrokkene heeft ook rechten binnen het gedwongen kader. Die rechten zijn bijvoorbeeld vastgelegd in de Wet verplichte geestelijke gezondheidszorg en de Wet zorg en dwang[5].

Drang en bemoeizorg heeft geen betrekking op het feitelijk verlenen van hulp – er is immers nog geen hulp - maar heeft betrekking op het toeleiden naar hulp. Zij vormt als zodanig onderdeel van de taken van het College in het kader van de Wmo artikel 1.2.1 a, en in het geval van jeugdigen de Jeugdwet artikel 2.3. Drang kan ook alleen toegepast worden door partijen die daartoe door het College van B&W zijn aangewezen. De grondslag voor de gegevensverwerking is dat geval artikel 6 lid e van de AVG: noodzakelijk voor de uitoefening van openbaar gezag.

In sommige gevallen is de situatie zo ernstig dat een melding bij Veilig Thuis (bij vermoedens van huiselijk geweld of kindermishandeling) of de Raad voor de Kinderbescherming moet worden overwogen. De omschrijving van huiselijk geweld in de MvT bij de WMO is zeer breed geformuleerd. In die gevallen dient de Verplichte Meldcode huiselijk geweld en kindermishandeling, toegepast te worden.

[5] Deze wetten vervangen de Wet BOPZ. Zie voor meer informatie het addendum bij dit Handvat over de Wet verplichte geestelijke gezondheid, Wet zorg en dwang en de Wet forensische zorg.

3 Grondslagen per organisatie bekeken

In het vorige hoofdstuk zijn de grondslagen uit artikel 6 AVG beschreven.
Bij het behandelen van complexe casussen in het zorg- en veiligheidsdomein werken partijen samen om tot een samenhangende aanpak te komen. Zonder afstemming zullen de afzonderlijke interventies niet leiden tot het oplossen van de problematiek.
Toestemming als grondslag conform de AVG speelt in deze situaties in de regel geen rol omdat de toestemming niet vrij gegeven kan worden. De grondslag voor de gegevensverwerking van elke partner vloeit voort uit de eigen taak die geregeld is in de voor de partner geldende materiewetgeving. Afhankelijk van de partner is dan een van de volgende AVG-grondslagen van toepassing.

Wettelijke verplichting (artikel 6 onder c AVG)
In verschillende materiele wetten staan wettelijke verplichtingen op grond waarvan organisaties gegevens mogen delen.
Wanneer er een wettelijke verplichting geldt, betekent dit nog niet dat gegevens ook met alle instanties gedeeld mogen worden. De gegevens mogen uitsluitend verstrekt worden aan bevoegde instanties. Wie deze bevoegde instantie is, is voor iedere partij verschillend.

Uitvoering taak (artikel 6 onder e AVG)
Ook worden er in verschillende materiele wetten taken omschreven op grond waarvan organisaties bevoegd zijn om bij de uitoefening van die taak gegevens te delen met bepaalde andere partijen. Partijen moeten goed in de gaten houden welke taak zij uitvoeren en checken of zij ook voor die taak bepaalde bevoegdheden hebben gekregen in de wet. Zo is Veilig Thuis enkel bevoegd om gegevens te delen of op te vragen als zij onderzoek doen. Doen zij geen onderzoek naar huiselijk geweld of kindermishandeling maar geven zij enkel advies, dan hebben zij geen specifieke bevoegdheden gekregen.

In onderstaande tabel staan de organisaties en gemeente (op alfabetische volgorde) die achtereenvolgens in dit hoofdstuk aan bod komen.

Organisaties
DJI
Gemeente
GGD/GGZ en overige gezondheidszorg
Gecertificeerde Instelling
Jeugdhulp
Openbaar Ministerie (OM)
Politie
Raad voor de Kinderbescherming
Reclassering
Slachtofferhulp Nederland
Stichting Halt

Veilig Thuis
Woningbouwvereniging/woningbouwcorporaties

3.1 DJI

3.1.1 Doelstelling en taken
De Dienst Justitiële Inrichtingen (DJI) is een agentschap van het Ministerie van Justitie en Veiligheid.

DJI is verantwoordelijk voor de tenuitvoerlegging van vrijheidsstraffen en vrijheidsbenemende maatregelen. De tenuitvoerlegging vindt plaats in een door de Minister aangewezen penitentiaire inrichting (PI), justitiële jeugdinrichting (JJI) of instelling voor verpleging van ter beschikking gestelden (ook wel Forensisch Psychiatrisch Centrum of FPC genoemd). Met inachtneming van het karakter van de straf of maatregel, wordt de tenuitvoerlegging zoveel mogelijk dienstbaar gemaakt aan de voorbereiding van de terugkeer van de betrokkene in de maatschappij. De tenuitvoerlegging van een straf of maatregel kan, met het oog op de resocialisatie en/of gespecialiseerde zorg en hulpverlening, geheel of gedeeltelijk buiten de inrichting plaatsvinden.
DJI is belast met de toeleiding van personen aan wie in een strafrechtelijk kader forensische zorg is opgelegd naar een instelling forensische zorg (PPC, FPC of gecontracteerde zorginstelling).
Bij de beslissingen tot uitplaatsing of deelname aan een extramuraal programma, het verlenen van vrijheden aan een gedetineerde, jeugdige, of verpleegde, en de toeleiding naar een instelling forensische zorg, wordt rekening gehouden met de veiligheid van de samenleving en de belangen van slachtoffers en nabestaanden.
DJI beheert detentiecentra en is daar verantwoordelijk voor het verblijf van personen die in vreemdelingenbewaring of grensdetentie zijn gesteld, waarbij nauw wordt samengewerkt met de partners uit de vreemdelingenketen.
DJI behandelt verzoeken van en aan het buitenland tot overname van de tenuitvoerlegging van strafvonnissen.

Het Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP) en de Dienst Vervoer en Ondersteuning (DV&O) zijn landelijke diensten van DJI:
- het NIFP draagt (onder meer) zorg voor het (laten) uitvoeren van advisering, en psychologisch - of psychiatrisch onderzoek, ambulant of in een observatiekliniek, in opdracht van de rechter, het Openbaar Ministerie (OM), of de Minister van Justitie en Veiligheid;
- de DV&O verzorgt (onder meer) in opdracht van de selectiefunctionaris van DJI of de directeur van de inrichting het transport en de bewaking van personen en goederen op weg naar de verschillende inrichtingen en van en naar instanties als de rechtbank.

3.1.2 Toepasselijke regelgeving
- Penitentiaire beginselenwet (Pbw), Penitentiaire maatregel (Pm);

- Beginselenwet justitiële jeugdinrichtingen (Bjj),Reglement justitiële jeugdinrichtingen (Rvt);
- Beginselenwet verpleging ter beschikking gestelden (Bvt), Reglement verpleging ter beschikking gestelden (Rvt);
- Wetboek van Strafrecht, Besluit tenuitvoerlegging jeugdstrafrecht 1994, Uitvoeringsbesluit voorwaardelijke invrijheidstelling;
- Wetboek van Strafvordering, Besluit identiteitsvaststelling verdachten en veroordeelden;
- Wet forensische zorg[6];
- Vreemdelingenwet 2000, Reglement regime grenslogies.

3.1.3 Wettelijk kader gegevensverwerking en verstrekken van gegevens
Voor iedere persoon die in een inrichting wordt ingesloten, dan wel (in het geval van een extramurale tenuitvoerlegging) administratief staat ingeschreven, moet een dossier worden aangelegd waarin de persoonsgegevens van de betrokkene worden opgenomen. Bij en krachtens de Beginselenwetten (Pbw, Bjj en Bvt) is geregeld welke informatie dit betreft.

Op grond van zijn wettelijke taken is DJI, met name de selectiefunctionaris en de directeur van de inrichting, ingevolge de bovengenoemde wet- en regelgeving bevoegd of verplicht om advies te vragen en inlichtingen in te winnen bij bevoegde instanties in verband met de handhaving van de orde en de veiligheid in de inrichting, de beslissingen en afspraken ten aanzien van een betrokkene in het kader van plaatsing, overplaatsing of terugplaatsing in een inrichting, verlening van (proef)verlof, deelname aan een (extramuraal) programma, en toeleiding naar een instelling forensische zorg.
Op grond van de Wet forensische zorg en het Besluit forensische zorg moet DJI persoonsgegevens verwerken ten behoeve van de indicatiestelling, de toeleiding naar forensische zorg en de verlening van forensische zorg.

Tot 25 mei 2018 was de Wet bescherming persoonsgegevens (Wbp) van toepassing op de verwerking van persoonsgegevens van strafrechtelijk gedetineerden (met inbegrip van jeugdigen en ter beschikking gestelden). In de plaats van het algemene verstrekkingenregime van de Wbp komt met ingang van de wijziging van de Wjsg, ter implementatie van de Europese richtlijn gegevensbescherming opsporing en vervolging (EU) 2016/680, een op deze gegevens toegespitst verstrekkingenregime in de Wjsg. De verwerking van die persoonsgegevens valt onder de categorie “tenuitvoerleggingsgegevens” en is geregeld in titel 3A, artikelen 51a tot en met 51d van de Wjsg. In artikel 1, onder d, zijn tenuitvoerleggingsgegevens gedefinieerd als: “persoonsgegevens of gegevens van een rechtspersoon inzake de tenuitvoerlegging van strafrechtelijke beslissingen, die in een dossier of een ander gegevensbestand zijn of worden verwerkt”.

De verwerking van persoonsgegevens van een persoon die op grond van een niet-strafrechtelijke titel staat ingeschreven bij een inrichting van DJI valt niet onder de

[6] Zie voor meer informatie het addendum bij dit Handvat over de Wet verplichte geestelijke gezondheid, Wet zorg en dwang en de Wet forensische zorg.

reikwijdte van de Wjsg. Met name kan worden gedacht aan personen die in vreemdelingenbewaring of in grensdetentie zijn gesteld en in een detentiecentrum verblijven op grond van de Vreemdelingenwet 2000 en het Reglement regime grenslogies. Op de verwerking van persoonsgegevens door DJI zijn dan de AVG en de UAVG van toepassing.

Bijzondere persoonsgegevens
Van de verwerking van tenuitvoerleggingsgegevens in de zin van de Wjsg kunnen ook bijzondere persoonsgegevens deel uitmaken, voor zover dit voor het doel van de verwerking onvermijdelijk is, in aanvulling op de verwerking van andere tenuitvoerleggingsgegevens betreffende de gedetineerde, jeugdige of tbs-gestelde (artikel 51b, eerste lid, in samenhang met artikel 39c derde lid) [7].
Wanneer het gaat om de tenuitvoerlegging van niet- strafrechtelijke beslissingen, kunnen bijzondere persoonsgegevens worden verwerkt door DJI op grond van:
- artikel 30, tweede lid, onder c, UAVG (gegevens over gezondheid) ;
- artikel 25, onder a, UAVG (gegevens waaruit ras of etnische afkomst blijkt), en
- artikel 27 UAVG (gegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken).

De verwerking van persoonsgegevens door een ambtenaar van DJI valt onder de verantwoordelijkheid van de Minister van Justitie en Veiligheid. Voor deze ambtenaren geldt de ambtelijke geheimhoudingsplicht (artikel 125a, derde lid, van de Ambtenarenwet).

In de Pm (artikel 58), het Rjj (artikel 87) en het Rvt (artikel 80) is een geheimhoudingsbepaling opgenomen voor een ieder die is betrokken bij de uitvoering van de wet, en voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt.

Verstrekken van gegevens
Op grond van de gewijzigde Wjsg verwerkt DJI tenuitvoerleggingsgegevens indien dit noodzakelijk is voor een goede vervulling van een wettelijke taak of het nakomen van een andere wettelijke verplichting. Verder kan DJI uitsluitend voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang aan personen of instanties tenuitvoerleggingsgegevens verstrekken. Het zwaarwegend algemeen belang moet

[7] TBS staat voor ter beschikking gesteld. De rechter kan deze maatregel opleggen aan personen die een zwaar misdrijf hebben gepleegd en daarvoor geheel of gedeeltelijk 'ontoerekeningsvatbaar' zijn verklaard. Het misdrijf kan de dader niet (volledig) aangerekend worden, doordat hij lijdt aan een persoonlijkheidsstoornis en/of een ernstige psychiatrische stoornis waardoor het gevaar bestaat tot recidive. Er zijn 2 varianten: tbs met bevel tot verpleging van overheidswege (vrijheidsbenemende maatregel) en tbs met voorwaarden. In het eerste geval wordt de tbs-gestelde in een tbs-kliniek geplaatst en behandeld. In het tweede geval stelt de rechter voorwaarden aan het gedrag waarbij de persoon bijvoorbeeld een verplichte (ambulante) behandeling moet ondergaan of geen alcohol of drugs mag gebruiken. Als men zich niet houdt aan die voorwaarden, kan de rechter de tbs omzetten in een tbs met bevel tot verpleging. Als het delict de dader gedeeltelijk wel kan worden aangerekend, kan de rechter hem voor dat deel een gevangenisstraf opleggen. In bepaalde gevallen kan de rechter ook afzien van het opleggen van een straf, omdat er sprake is van volledige ontoerekeningsvatbaarheid. De tbs-maatregel start dan direct.

voldoen aan één van de volgende (limitatief opgesomde) doeleinden (artikel 51c, tweede lid):

a. de tenuitvoerlegging van een strafrechtelijke beslissing;
b. de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten;
c. schuldhulpverlening of resocialisatie van betrokkenen;
d. bestuurlijk handelen of het nemen van een bestuursrechtelijke beslissing, of
e. het verlenen van hulp aan slachtoffers.

Als aanvullende eisen voor de verstrekking geldt dat die gegevens voor die personen of instanties (artikel 51c, derde lid):

a. noodzakelijk zijn met het oog op een zwaarwegend algemeen belang of de vaststelling, de uitoefening of de verdediging van een recht in rechte, en
b. in zodanige vorm worden verstrekt dat herleiding tot andere personen dan betrokkene, redelijkerwijs wordt voorkomen.

Elke verstrekking moet worden vastgelegd en ten minste vier jaar worden bewaard (artikel 51c, vierde lid).

Verstrekkingen in het kader van de tenuitvoerlegging van niet-strafrechtelijke beslissingen kunnen veelal overeenkomstig de AVG en de UAVG worden gedaan met een beroep op een wettelijke verplichting (artikel 6, eerste lid, onder c, AVG) of de vervulling van een taak van algemeen belang (artikel 6, eerste lid, onder e, AVG).

Met inachtneming van het voorgaande en in samenhang met bepalingen bij of krachtens de Beginselenwetten (Pbw, Bjj, Bvt), het Wetboek van Strafrecht, het Wetboek van Strafvordering, de Wet forensische zorg, de Vreemdelingenwet 2000, en bijvoorbeeld de Participatiewet (Pw), en de Wet Structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI) kan DJI persoonsgegevens over een betrokkene verstrekken aan ketenpartners in de strafrecht- en vreemdelingenketen, zorgaanbieders en gemeenten. Bijvoorbeeld aan:

- AMHK/Veilig Thuis: meldingen overeenkomstig het Besluit verplichte meldcode huiselijk geweld en kindermishandeling (artikelen 5b Pbw, 5a Bjj en 7b Bvt);
- OM: advisering in het kader van voorwaardelijke invrijheidstelling (artikel 2 van het Uitvoeringsbesluit voorwaardelijke invrijheidstelling);
- Reclassering of jeugdreclassering en de RvdK: gezamenlijke opstelling van het perspectiefplan voor een jeugdige in een JJI (artikel 25 Rjj), en overleg in het netwerkberaad en trajectberaad bij de voorbereiding van een jeugdige op terugkeer in de samenleving (artikel 21a Besluit tenuitvoerlegging jeugdstrafrecht 1994);
- Burgemeester: ten behoeve van de handhaving van de openbare orde in verband met terugkeer van de (ex)gedetineerde in de maatschappij (artikel 11a Bjsg), bijvoorbeeld in geval van de BIJ-regeling;
- College van B&W: ten behoeve van begeleiding door jeugdreclassering van een jeugdige die gaat deelnemen aan een scholings- en trainingsprogramma (artikel 11c Bjsg in samenhang met Jeugdwet);
- College van B&W: ten behoeve van afspraken met gemeente over huisvesting, arbeid, dagbesteding en kosten (zoals een uitkering) tijdens de laatste – extramurale - fase van de ISD-maatregel (artikel 44f Pm); (Maatregel Inrichting Stelselmatige Daders);

- College van B&W/UWV: voor de uitvoering van de Participatiewet i.v.m. (uitsluiting van) het recht op bijstand aan gedetineerden (artikel 64, lid 1, onder k, en lid 12 Pw) en voor openstelling van het recht op een socialezekerheidsuitkering voor personen die deelnemen aan een penitentiair programma of proefverlof genieten (13, lid 1 en 3 Besluit extramurale vrijheidsbeneming en sociale zekerheid);
- UWV/Sociale Verzekeringsbank/Ministerie en Inspectie SZW: voor de uitvoering van de Wet SUWI, in verband met het recht op uitkering (artikel 54, lid 3, onder h, en lid 9).

3.1.4 Belang van samenwerking in een samenwerkingsverband

De missie van DJI luidt: 'De Dienst Justitiële Inrichtingen levert een bijdrage aan de veiligheid van de samenleving door de tenuitvoerlegging van vrijheidsstraffen en vrijheidsbenemende maatregelen en door de aan onze zorg toevertrouwde personen de kans te bieden een maatschappelijk aanvaardbaar bestaan op te bouwen.' Dit betekent dat tijdens het verblijf bij DJI een (veelal) zeer complexe groep justitiabelen op hun re-integratie wordt voorbereid. Het oogmerk daarbij is een bijdrage te leveren aan de vermindering van recidive. Een straf of maatregel is in de meeste gevallen een (vaak korte) onderbreking van het maatschappelijk leven. Het is van belang dat interventies op de diverse 'leefgebieden' die voorafgaand aan de straf of maatregel al in gang zijn gezet, zoveel mogelijk worden gecontinueerd. Daarom willen de inrichtingen van DJI samen met gemeenten, reclassering en maatschappelijke - en zorginstanties, bij aanvang van de straf of maatregel gezamenlijk bepalen welk traject wordt ingezet of voortgezet. Na afloop van een langere vrijheidsbeneming, zoals na een ISD-maatregel, PIJ-maatregel[8], of tbs-maatregel, moet opnieuw aansluiting worden gevonden bij voorzieningen die lokaal beschikbaar zijn. Ketenoverleg in een ZVH kan noodzakelijk zijn om tot een goede oplossing te komen in zaken met veiligheidsproblematiek in de gemeente en/of de sociale omgeving van betrokkene (afglijdend gedrag). Soms moeten personen worden (terug)geplaatst door DJI in een justitiële inrichting, instelling forensische zorg of detentiecentrum. Door de individuele trajecten samen met netwerkpartners te bepalen draagt DJI bij aan het bevorderen van de continuïteit van maatschappelijke hulp/begeleiding die zowel binnen als buiten het strafrecht wordt geboden. Op deze wijze worden dubbelingen en onderbreking van trajecten zoveel mogelijk voorkomen, hetgeen bijdraagt aan de maatschappelijke veiligheid die door alle betrokken organisaties wordt voorgestaan.

3.2 Gemeente

Een gemeente heeft te maken met allerlei soorten veiligheidsproblemen en sociale problemen in haar wijken en onder haar burgers. De problemen lopen uiteen van criminaliteit, openbare ordeproblemen, drugs- of geluidsoverlast op straat of vanuit woningen tot schoolverzuim, werkloosheid, schulden en gezondheidsproblemen, waaronder psychiatrische problemen. Hierbij kan sprake zijn van meervoudige complexe problematiek, bijvoorbeeld bij gezinnen waarbij problemen alleen in samenhang met elkaar kunnen worden opgelost. De gemeente speelt daarom een belangrijke rol in zowel

[8] PIJ staat voor "Plaatsing in een Inrichting voor Jeugdigen". De maatregel staat ook wel bekend als Jeugd-tbs maar dat is geen officiële term

het veiligheidsdomein als het sociale domein. De gemeentelijke taken in het zorg- en veiligheidsdomein zijn neergelegd in diverse wetgeving.

Het is van belang om hierbij in het oog te houden dat de verschillende wettelijke taken niet door ‘de gemeente’ uitgevoerd worden: de gemeente zelf is geen bestuursorgaan. De bestuursorganen van de gemeente zijn: de burgemeester, het college van Burgemeester en Wethouders (hierna: het college van B&W) en de gemeenteraad. ‘De gemeente’ kan in privacy-rechtelijke zin dus ook geen persoonsgegevens verwerken, noch als verwerkingsverantwoordelijke voor een verwerking van persoonsgegevens worden aangemerkt. Als verwerkingsverantwoordelijke kan enkel een bestuursorgaan van de gemeente worden aangemerkt. Ook kan voor een speciale taak op grond van de Wet gemeenschappelijke regelingen (hierna: Wgr) een openbaar lichaam worden ingesteld (bijvoorbeeld de GGD).

De gemeente heeft een beleidsmatige taak om te zorgen dat er een verband is waarbinnen de samenwerking tussen partijen bij complexe problematiek kan worden georganiseerd. Daartoe zijn bijvoorbeeld de zorg- en veiligheidshuizen opgericht. Deze beleidsmatige taak heeft echter geen betrekking op de behandeling van individuele casussen. Voor de behandeling van individuele casussen kan de gemeente alleen deelnemen vanuit een specifieke wettelijke taak. Bijvoorbeeld de OOV-taken van de burgemeester, de WMO-taken van het college van B&W in het geval van bemoeizorg, of de Jeugdwettaken van het college van B&W. De persoonsgegevens die een gemeente in verband met een dergelijke taak verkrijgt, mag zij niet voor andere doeleinden gebruiken tenzij de wet dat uitdrukkelijk toestaat.

De gemeente moet net als andere partijen terughoudend zijn met het verzamelen en uitwisselen van persoonsgegevens. Het is verstandig de betreffende inwoner zoveel mogelijk te betrekken als het om zijn of haar persoonsgegevens gaat. Het vragen van toestemming is echter vaak geen oplossing. De AVG bepaalt namelijk dat mensen zich vrij moeten voelen om toestemming te geven. In het sociaal domein zal van vrije toestemming over het algemeen geen sprake kunnen zijn, omdat burgers afhankelijk zijn van de gemeente voor hulp of ondersteuning. Als gemeenten in die gevallen tóch toestemming vragen en persoonsgegevens verwerken op basis van toestemming, kan dat worden beschouwd als onrechtmatig.
Verder beschikken de gemeente door de breedte van hun wettelijke taken over heel veel en diverse gegevens van hun burgers. Een integraal persoonsbeeld of klantbeeld opstellen over haar burgers is niet toegestaan op grond van de doelbindingsvereisten en zeker ook niet op grond van de diverse geheimhoudingsbepalingen in de gemeentelijke wetgeving.

De grondslag voor gegevensverwerking door de verschillende bestuursorganen zal in de meeste gevallen gelegen zijn in hun taakuitoefening die in een materiele wet is vastgelegd. We bekijken achtereenvolgens de taakuitoefening van de burgemeester en het college van B&W.

3.2.1 Taakuitoefening burgemeester

In artikel 172 Gemeentewet worden de bevoegdheden van de burgemeester beschreven. De taak ziet op het gebied van handhaving van de openbare orde en veiligheid[9]. De AVG is van toepassing op de verwerkingen door de gemeente die in het kader van de openbare orde en veiligheid worden gedaan, de Gemeentewet geeft immers geen aparte bepalingen met betrekking tot de gegevensverwerking, m.u.v. art. 151c Gemeentewet over camerabeelden waarvan de wetgever heeft bepaald dat dit politiegegevens betreffen.

Op grond van artikel 172a Gemeentewet is de burgemeester bevoegd een burger een locatieverbod, locatiegebod of een meldplicht op te leggen (de 'Voetbalwet').

Op grond van artikel 8a juncto 39f Wjsg kunnen met het oog op een zwaarwegend algemeen belang strafvorderlijke gegevens worden verstrekt aan de burgemeester voor het handhaven van de openbare orde en veiligheid. Verder is de Minister van Justitie en Veiligheid ten behoeve van de handhaving van de openbare orde op grond van artikel 11a lid 1 Bjsg bevoegd om de burgemeester of de door hem aangewezen ambtenaar Justitie en Veiligheid te informeren over de terugkeer in de maatschappij of het verlof van een bepaalde groep (ex-)justitiabelen die onherroepelijk is veroordeeld. Het moet gaan om een onvoorwaardelijke veroordeling tot een gevangenisstraf voor een ernstig geweld- of zedenmisdrijf, een verlengbare PIJ-maatregel of de maatregel tbs met dwangverpleging. Alleen de justitiële gegevens als bedoeld in artikel 6, eerste lid en artikel 7, eerste lid, onder a, b, c, d, f, j, k en l Bjsg kunnen worden verstrekt (Bestuurlijke Informatievoorziening Justitiabelen, BIJ-regeling). Aan een speciaal daartoe aangewezen ambtenaar van de gemeente kunnen bepaalde justitiële gegevens worden verstrekt over personen ten aanzien van wie in het kader van een strafrechtelijke beslissing is bepaald dat zij in aanmerking komen voor een vorm van jeugdhulp of jeugdreclassering, als bedoeld in artikel 1.1 van de Jeugdwet. Dit kan op grond van artikel 11a Bjsg. Het gaat dan om justitiële gegevens als bedoeld in artikel 6, eerste lid, onderdeel f, en artikel 7, eerste lid, onder j, onderdelen 5 en 6 van de Bjsg.

Andere taken die de burgemeester heeft zijn:

- De Wet Tijdelijk huisverbod maakt het mogelijk voor de burgemeester om een persoon van wie een ernstige dreiging van huiselijk geweld uitgaat tijdelijk (in beginsel tien dagen) de toegang tot zijn woning te ontzeggen. De burgemeester kan zich, voor een rechtmatige gegevensverwerking om tot het oordeel te komen om wel of geen huisverbod op te leggen, baseren op artikel 6 sub e AVG. De politie kan een zorgmelding doen bij Veilig Thuis en gegevens verstrekken aan het college van B&W t.b.v. taken op grond van de Jeugdwet (art. 4:2 lid 1 onder i Bpg). In de praktijk is de toepassing van de Wet Tijdelijk huisverbod geheel of grotendeels gemandateerd aan de politie.

[9] Openbare orde wordt niet gedefinieerd in Gemeentewet. Uit kamerstukken blijkt dat: "De openbare orde wordt beheerst door een complex van rechtsregels dat ziet op het gewenste niveau van orde en rust in het openbare leven. Handhaving van de openbare orde betreft de zorg voor de naleving van die regels. De regels kunnen in wetten in formele zin en in lagere regelingen zijn neergelegd. Het begrip 'handhaving van de openbare orde' bevat twee elementen: de daadwerkelijke voorkoming en beëindiging van zich concreet voordoende of dreigende verstoringen van de openbare orde enerzijds én de algemene, bestuurlijke voorkoming van strafbare feiten anderzijds".

- De burgemeester heeft de bevoegdheid om een inwoner voor korte tijd te laten opnemen op grond van een crisismaatregel op basis van de Wet verplichte geestelijke gezondheidszorg of een inbewaringstelling op grond van de Wet zorg en dwang.[10]

3.2.2 Taakuitoefening Burgemeester en Wethouders

Het college van B&W heeft verschillende taken, waaronder in het bijzonder taken in het sociaal domein zoals bedoeld in:

- WMO (artikel 2.3.1. tot en met 2.3.5)
- Jeugdwet (artikel 2,3 en 2.4.)
- Participatiewet (artikel 7.1)
- Wet gemeentelijke schuldhulpverlening (artikel 3)

Taken vanuit de Wet Maatschappelijke Ondersteuning (WMO 2015)

Het college van B&W heeft op grond van de WMO de opdracht en taak tot maatschappelijke ondersteuning. Het gaat hierbij om beleid gericht op de sociale samenhang, het bevorderen van de toegankelijkheid van voorzieningen, diensten en ruimten voor mensen met een beperking, het bevorderen van de veiligheid en leefbaarheid in de gemeente, alsmede het voorkomen en bestrijden van huiselijk geweld. De vereisten die voortvloeien uit de AVG, zijn in deze wet geborgd in het proces waarbij de cliënt zelf het merendeel van de gegevens levert die het college van B&W nodig heeft om de ondersteuningsbehoefte (integraal) te kunnen beoordelen. Het gaat hierbij primair om burgers die zichzelf bij de gemeente melden met een hulp- en ondersteuningsvraag.

Zie met name artikel 5.1.1 e.v. WMO over de bevoegdheden tot gegevensverwerking van het college van B&W, aanbieders van maatwerkvoorziening, het CAK (Het Centraal Administratiekantoor) en de SVB (Sociale Verzekeringsbank).[11]

Veel gemeenten hebben de uitvoering van de WMO neergelegd bij sociale wijkteams. Het college van B&W is ingevolge de WMO de verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens. Als de gemeente samen met zorginstanties een separate stichting in het leven heeft geroepen voor de sociale wijkteams, dan is de stichting de verwerkingsverantwoordelijke.

Het uitgangspunt van de WMO is dat de eigen verantwoordelijkheid van burgers vooropstaat. Daarbij hoort dat de burger zelf regie kan voeren over zijn eigen gegevens. Waarborgen voor een zorgvuldige verwerking van persoonsgegevens die in het kader van de WMO zijn getroffen, zijn onder meer:

[10] Deze wetten vervangen de Wet BOPZ. Zie voor meer informatie het addendum bij dit Handvat over de Wet verplichte geestelijke gezondheid, Wet zorg en dwang en de Wet forensische zorg.

[11] Rapport AP, april 2016, p. 13: Daar waar bredere verwerking van persoonsgegevens mogelijk is, gaat het doorgaans om hulpverleningstaken (en dus niet publiekrechtelijke taken zoals de intake). Bovendien gaat het dan om domein overstijgende verwerking van persoonsgegevens ten behoeve van het specifieke doel uit de materie wetgeving (dus niet om domein overstijgende hulpverlening). In dit kader moeten ook artikel 5.1.1, vierde en vijfde lid, en artikel 5.2.1, eerste lid, onderdeel b, van de Wmo 2015 worden genoemd. Deze bepalingen zien op de verwerking van gegevens uit andere domeinen voor het domein van de Wmo 2015. Ook artikel 5.1.1, vierde en vijfde lid, van de Wmo zien alleen op het gebruik van gegevens ten behoeve van taken in het domein van de Wmo 2015. Deze bepalingen voorzien dus niet in gebruik van gegevens uit alle domeinen voor de bepaling van de aanspraak op integrale (domein overstijgende) hulp of ondersteuning.

- aan de hand van bepalingen is per actor concreet en nauw omschreven voor welke specifieke taken gegevensverwerking en -verstrekking is toegestaan;
- als criterium voor de beoordeling van de proportionaliteit en de noodzaak van gegevensverwerking en -verstrekking is in de bepalingen in de WMO zo nauwkeurig mogelijk aangegeven dat de bevoegdheid tot verwerken van (bijzondere) persoonsgegevens alleen bestaat voor zover die persoonsgegevens voor een welomschreven specifiek doel noodzakelijk zijn. Bijvoorbeeld voor de beoordeling van de behoefte aan ondersteuning van participatie of zelfredzaamheid;
- in de WMO is zo precies mogelijk aangegeven dat het moet gaan om persoonsgegevens die zijn verkregen langs een daarbij aangegeven weg;
- instemming van en transparantie voor de cliënt is voor bepaalde verwerkingen van persoonsgegevens van belang;
- gepaste beveiligingsmaatregelen dienen te worden getroffen.

Als de betrokkene zelf aangeeft dat hij te maken heeft gehad met detentie, kan het noodzakelijk zijn om dit te vermelden in de integrale analyse. Dit staat vermeld in de Memorie van Toelichting bij de WMO, maar er is geen aparte wettelijke grondslag voor gecreëerd in de WMO. In dit geval is dus de AVG van toepassing. Dat betekent dat het gaat om strafrechtelijke persoonsgegevens, en die vallen onder de categorie bijzondere persoonsgegevens (artikel 9 AVG). Het college van B&W kan dergelijke gegevens alleen verwerken op grond van artikel 6 lid 1 onder a AVG, dat wil zeggen na uitdrukkelijke en in vrijheid gegeven toestemming van de betrokkene. Om een dergelijke toestemming te krijgen, zou de betrokkene uit zichzelf moeten hebben aangegeven dat hij ex-gedetineerde is. Het college mag niet vooraf de suggestie hebben gewekt dat deze informatie benodigd is of er op enigerlei (andere) wijze naar hebben gevist.

De medewerker van het sociale wijkteam kan tijdens het onderzoek naar de situatie en de zorg- en ondersteuningsbehoefte van betrokkene ook aangeven dat het belangrijk is om gegevens op te vragen bij een huisarts of behandelend arts. Hij vraagt daar uitdrukkelijke toestemming voor. De wettelijke grondslag hiervoor is artikel 2.3.2 lid 4 sub f WMO juncto artikel 5.1.1 lid 1 WMO. Dit is in overeenstemming met artikel 6 lid 1 onder a AVG. De arts zal vervolgens de afweging maken wat hij wel en niet kan verstrekken aan het college van B&W en daarbij op zijn beurt uitdrukkelijke toestemming vragen aan zijn patiënt. De arts moet dit doen op grond van de WGBO.

Taken vanuit de jeugdwet
De Jeugdwet heeft het college van B&W verantwoordelijk gemaakt voor jeugdhulp, inclusief kinderbeschermingsmaatregelen, en jeugdreclassering. Deze nieuwe gemeentelijke verantwoordelijkheid brengt de volgende taken mee:
- toeleiding naar de jeugdhulp op grond van artikel 2.3 (toegang);
- jeugdhulpplicht: zorgen voor een toereikend aanbod aan jeugdhulp waaronder voorzien in een toereikend aanbod van gecertificeerde instellingen (art 2.3 Jeugdwet, art. 2.4 tweede lid onder a en artikel 2.6 Jeugdwet);
- op grond van artikel 2.4, eerste lid Jeugdwet kan het college van B&W een verzoek tot onderzoek doen bij de Raad van de Kinderbescherming zodra het tot het oordeel

komt dat een maatregel met betrekking tot het gezag over een minderjarige die zijn woonplaats heeft binnen zijn gemeente moet worden overwogen;
- op grond van artikel 2.4. tweede lid Jeugdwet is de gemeente verantwoordelijk voor het uitvoeren van de kinderbeschermingsmaatregelen en de jeugdreclassering. Een gecertificeerde instelling (GI) voert deze taken uit. De gemeente heeft hierin uitsluitend tot taak om de uitvoering van de taken door de GI te financieren;
- er voor zorgdragen dat wordt nagegaan of de meldingsbevoegden die een jeugdige aan de Verwijsindex Risicojongeren hebben gemeld en vervolgens daaruit een signaal hebben ontvangen, met elkaar contact hebben opgenomen (art.7.1.3.2 Jeugdwet).

Zie het rapport van de AP uit april 2016, p. 13, eerste alinea: *"de Jeugdwet voorziet dus wel in het gebruik van gegevens uit andere domeinen maar slechts voor de bepaling van de behoefte aan jeugdhulp. Deze bepaling biedt dus geen grondslag voor het gebruik van deze gegevens voor doelen die de Jeugdwet overstijgen. Daardoor is bijvoorbeeld een integrale intake niet mogelijk."*

Taken vanuit de Participatiewet en Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (Wet SUWI)

De gemeente is op grond van de Participatiewet belast met het verstrekken van uitkeringen en het toeleiden naar werk en scholing van burgers met een afstand tot de arbeidsmarkt. De gegevensverwerking is geregeld in de Participatiewet, maar ook in de Wet SUWI. In de Wet SUWI wordt de onderlinge gegevensverstrekking geregeld van de gemeenten en andere instanties met betrekking tot de sociale zekerheid, in dit geval het UWV en de SVB. De Wet SUWI gaat uit van een gesloten verstrekkingenregime. Dat regime houdt in dat werk- en inkomensgegevens uitsluitend mogen worden hergebruikt als daar een wettelijke grondslag voor is of als de burger daar toestemming voor heeft gegeven. In de WMO is geregeld dat de gemeente de gegevens die zij ten behoeve van de Participatiewet heeft verkregen ook mag gebruiken voor de WMO-taak, mits de burger toestemming heeft gegeven. De Participatiewet en de Wet SUWI bieden geen mogelijkheden om gegevens te verstrekken aan samenwerkingsverbanden, tenzij met toestemming van de betrokken burger. Gezien het hierboven genoemde rapport van de AP van april 2016 over toestemming in het sociale domein moet hiermee zeer terughoudend worden omgegaan. (Bij een verstrekking aan de samenwerkingsverbanden van de Regionale Coördinatie en Fraudeteams (RCF's) is toestemming niet nodig).

Bij het uitvoeren van de Participatiewet maakt de gemeente, in dit geval de afdeling Werk en Inkomen, gebruik van de GeVS (Gezamenlijke elektronische voorzieningen SUWI) ook wel SUWI-net genoemd met daarbij de landelijk beschikbare applicatie Suwinet-Inkijk. Suwinet-Inkijk mag niet voor andere doeleinden dan voor de uitvoering van de Participatiewet worden gebruikt. Via deze inkijkvoorziening mogen alleen gegevens in het kader van de Wet SUWI tussen organisaties binnen het SUWI-stelsel worden ingezien en uitgewisseld, voor het doel van die wet. Dat betekent dat voor wat betreft de gemeente alleen medewerkers van een dienst Werk en Inkomen/Sociale Dienst toegang hebben tot Suwinet-Inkijk. Andere gemeentelijke afdelingen, zoals de afdeling Openbare orde en Veiligheid, worden niet beschouwd als SUWI-partijen en aan

hen kunnen geen gegevens worden verstrekt. Binnengemeentelijke verstrekking van uitkeringsgegevens is dus aan strenge regels gebonden; gegevens van bijstandsgerechtigden en andere uitkeringsgerechtigden mogen in beginsel alleen aan organisaties buiten SUWI worden verstrekt als daar een uitdrukkelijke wettelijke grondslag of verplichting voor bestaat. Voor medewerkers van de gemeente die belast zijn met de uitvoering van WMO-taken geldt dat zij op grond van artikel 5.1.1 lid 4 WMO wel uitkeringsgegevens kunnen verwerken voor zover betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend. Uitkeringsgegevens kunnen alleen aan de politie of het OM worden verstrekt op grond van een vordering op grond van artikel 126nd Wetboek van Strafvordering. Dat betekent dat dit alleen kan in het kader van een strafrechtelijk onderzoek. In dat geval moet er dus sprake zijn van een concrete verdenking van een strafbaar feit dat vordering van deze gegevens rechtvaardigt.

Taken vanuit de ISD-maatregel
Sinds 1 oktober 2004 is de Maatregel Inrichting Stelselmatige Daders (hierna: de ISD-maatregel) van kracht (artikelen 38m tot en met 38u Wetboek van Strafrecht). De penitentiaire maatregel art 44b t/m 4q geeft verdere invulling aan de ISD maatregel. De ISD-maatregel maakt het mogelijk om meerderjarige stelselmatige daders die door het plegen van reeksen delicten veel criminaliteit en onveiligheid veroorzaken, in een daartoe aangewezen inrichting te plaatsen voor maximaal 2 jaar. Met deze wet heeft de wetgever beoogd stelselmatige daders, voor een periode van maximaal twee jaar in een inrichting te plaatsen die specifiek voor hen bestemd is.
De maatregel ISD beoogt het uitzichtloze patroon van vastzitten, vrijkomen en terugvallen dat stelselmatige daders kenmerkt, te doorbreken, en heeft de volgende doelstellingen:

- Het terugdringen van ernstige criminaliteit en onveiligheid als gevolg van, door stelselmatige daders, gepleegde strafbare feiten.
- Alleen bij duidelijke aanknopingspunten voor gedragsverandering en recidivevermindering zal aan de stelselmatige *dader* een aanbod voor een intensieve programma worden gedaan.

De ISD-maatregel kan ook worden opgelegd voor relatief 'lichte' misdrijven indien er sprake is van stelselmatigheid waarmee een verdachte delicten heeft gepleegd. ISD wordt beschouwd als de allerlaatste-kans-voorziening, bestemd voor de zwaarste groep stelselmatige daders.

Binnen de ISD bestaan er twee fasen; een intramurale fase en een extramurale fase. De duur van de fasen wordt individueel bepaald. Het college van B&W heeft een adviesrol ten aanzien van de extramurale fase van een ISD-maatregel. Op grond van het advies van de directeur van de inrichting en het college van B&W, beslist een selectiefunctionaris over de aanvang van de extramurale fase.

Doel van de extramurale fase is om de betrokkene te leren zijn stoornissen en/of verslavingen te beheersen en hem te laten re-integreren in de maatschappij. Deze fase bestaat uit een zorgtraject binnen een GGZ-instelling en een re-integratietraject, waarbij aandacht wordt besteed aan begeleid wonen en een dagbesteding.

Naast algemene voorwaarden kunnen door het college van B&W bijzondere voorwaarden worden gesteld aan de extramurale fase. De reclassering houdt toezicht op de naleving van de voorwaarden. Indien de gestelde voorwaarden niet worden nageleefd of de veroordeelde zich onttrekt aan opname of begeleiding, kan (tijdelijke) terugplaatsing in de inrichting volgen. De selectiefunctionaris beslist over de (tijdelijke) terugplaatsing op basis van advies van de directeur die hiertoe informatie inwint bij het college van B&W. De algemene verantwoordelijkheid tijdens de laatste fase van de ISD-maatregel buiten de inrichting ligt bij de directeur van de inrichting. De gemeente waar de gedetineerde tijdens de extramurale fase verblijft, is verantwoordelijk voor de invulling van de extramurale fase met betrekking tot de basisvoorzieningen inkomen, arbeid of dagbesteding en huisvesting. Daartoe worden nadere afspraken gemaakt tussen de gemeente en de directeur van de penitentiaire inrichting

Taken vanuit de wet Gemeentelijke schuldhulpverlening
De gemeente is verantwoordelijk voor de schuldhulpverlening aan haar burgers. Onder schuldhulpverlening wordt verstaan het ondersteunen bij het vinden van een adequate oplossing gericht op de aflossing van schulden, indien redelijkerwijs is te voorzien dat een natuurlijke persoon niet zal kunnen voortgaan met het betalen van zijn schulden of indien hij in de toestand verkeert dat hij heeft opgehouden te betalen, alsmede de nazorg. Het gaat hierbij om een zogeheten minnelijk traject met schuldeisers. Indien dit traject faalt, krijgt de schuldenaar te maken met de Wet schuldsanering natuurlijke personen (WSNP), een onderdeel van de Faillissementswet.
In artikel 8 van de Wet gemeentelijke schuldhulpverlening wordt ingegaan op de gegevensuitwisseling. Volgens dit artikel kan het vragen en het verstrekken van gegevens door het college van B&W aan en door de in het eerste en tweede lid bedoelde bestuursorganen en instanties geschieden door tussenkomst van het Inlichtingenbureau, bedoeld in artikel 63 van de Wet SUWI.

Taak vanuit Wet Victoria
Het college van B&W heeft de bevoegdheid om een woning te sluiten naar aanleiding van overlast veroorzaakt door de bewoner op grond van onder ander artikel 174a Gemeentewet (Wet Victoria). Dit kan van belang zijn wanneer er bijvoorbeeld bij multi-probleem casuïstiek sprake is van woonoverlast in combinatie met strafbare feiten.

3.2.3 De gemeente bij een casusoverleg
Bij de vraag naar de juridische basis voor deelname van gemeenten in een casusoverleg moet men steeds helder voor ogen hebben vanuit welke specifieke wettelijke taak de gemeente aan tafel zit in die specifieke casus. Is dat bijvoorbeeld: het mogelijk opleggen van een gebiedsverbod bij een overlast gevende jongere, het sluiten van een pand van iemand die woonoverlast veroorzaakt, of de mogelijkheid tot het inzetten van jeugdhulp of een WMO-voorziening, etc. De opsomming van wettelijke taken in dit Handvat moet er niet toe leiden dat men denkt dat er in alle gevallen wel een wettelijke basis aanwezig is voor deelname van de gemeente aan het casusoverleg. Het is ook voor de andere

deelnemers aan het overleg van belang vanuit welke taak de gemeente aan tafel zit om te kunnen beoordelen welke informatie zij aan de gemeente kunnen of willen verstrekken.
In de praktijk komt het vaak voor dat gemeenteambtenaren met teveel petten tegelijk op bij een casusoverleg zitten.

Een ander belangrijk punt om in het oog te houden is de scheiding tussen de wettelijke taken van de burgemeester of het college van B&W zoals hierboven genoemd, en de proces coördinerende taken. De procesregisseur staat ten dienste van het proces van samenwerking en afstemming en acteert dan namens de partij die de casus heeft aangemeld. Hoewel de procesregisseur vaak in dienst zal zijn van de gemeente, is hij in die rol niet de vertegenwoordiger van een van de wettelijke taken van de gemeente. En het verdient aanbeveling die rollen gescheiden te houden. De procesregisseur staat geheel los van de inhoudelijke bijdrage van de gemeente aan een casusoverleg.

Driehoeksoverleg:
Op grond van artikel 13 Politiewet voert de burgemeester overleg met de officier van justitie en de politiechef over de taakoefening en de inzet van de politie, het zogenoemde driehoeksoverleg. In het driehoeksoverleg worden onder meer afspraken gemaakt over lokale prioriteiten en criminaliteitsbestrijding. De gemeente stelt op grond van artikel 38b Politiewet 2012 in het integraal veiligheidsplan (IVP) de doelen vast die de gemeente nastreeft op het gebied van handhaving van de openbare orde. In het IVP worden door de gemeente in samenspraak met de politie en het OM de beleidsdoelstellingen geformuleerd, en de wijze waarop deze gerealiseerd zullen gaan worden. Het IVP is een plan primair voor de gemeente en wordt besproken in de gemeenteraad.
Op grond van artikel 39 Politiewet stellen de burgemeesters en de hoofdofficier van justitie eens in de vier jaar een regionaal beleidsplan voor de politie op, waarbij rekening wordt gehouden met het IVP van de gemeenten in de regio. Het regionaal beleidsplan is een plan primair voor de politie. Het wordt besproken in het regionaal overleg van de burgemeesters (vroeger Regionaal College).
In al deze plannen worden allereerst de doelstellingen geformuleerd die de gemeenten en de partners in de driehoek – vaak samen met andere maatschappelijke partners – op het gebied van openbare orde en veiligheid willen bereiken. Het gaat hierbij om de prioriteitstelling (het wat) maar ook de aanpak, in dit geval strategie en uitvoering (het hoe). Er kan worden gekozen voor een persoonsgerichte, delictgerichte en/of gebiedsgerichte aanpak.

Deze wettelijke bepalingen vormen de grondslag voor de gemeente(n) om het veiligheidsbeleid te bepalen en de gemeentelijke doelstellingen op het gebied van openbare orde en veiligheid te formuleren. In het IVP en in het regionale beleidsplan worden de beleidsdoelstellingen geformuleerd, als ook de wijze waarop deze gerealiseerd zullen gaan worden. De afgelopen jaren vormen de Veiligheidshuizen een vast onderdeel in alle lokale IVP's en alle regionale beleidsplannen voor de politie.
Uit de bevoegdheid tot het opstellen van een integraal veiligheidsplan volgt als het ware logischerwijs dat de gemeente ook regie voert over de uitvoering van dat plan en de activiteiten van de daarbij betrokken partijen (overheden en instellingen). Als echter bij

de uitvoering van het IVP activiteiten plaatsvinden door betrokken partijen waarbij persoonsgegevens moeten worden verwerkt, geeft dat de gemeente nog geen recht op het automatisch verkrijgen van die persoonsgegevens van alle bij de uitvoering van het veiligheidsbeleid betrokken organisaties enkel en alleen voor de regietaak van de gemeente. Daar zijn weer andere grondslagen voor nodig, zoals hierboven is uiteengezet.

Op grond van de Jeugdwet is het Besluit Politiegegevens (hierna: Bpg) gewijzigd. Aan het college van B&W en Veilig Thuis kunnen ten behoeve van de uitvoering van de taken bedoeld in de artikelen 2.3, eerste en zesde lid, en 2.4, eerste lid Jw, op grond van artikel 4:2 lid 1 sub i Bpg over jeugdigen worden verstrekt. Dit betekent dat zogenaamde 'zorgmeldingen' van de politie over jeugdigen worden verzonden aan daartoe gemandateerde ambtenaren van de gemeente en aan Veilig Thuis. Deze meldingen vinden plaats via de Collectieve Opdracht Routeer Voorziening (CORV).

3.2.4 Domein overstijgende informatie

Op grond van de huidige wetgeving is het niet mogelijk om een gemeente-breed geïntegreerd klantbeeld samen te stellen. Dit zou ook een grove inbreuk betekenen op de persoonlijke levenssfeer van burgers. Een gemeente bestaat uit verschillende afdelingen die verschillende taken en bevoegdheden van de gemeente uitvoeren. Het is niet vanzelfsprekend dat persoonsgegevens die door de ene afdeling zijn verzameld ook aan de andere afdeling mogen worden verstrekt. Er zal steeds bekeken moeten worden krachtens welke bevoegdheid de gemeentelijke afdeling de persoonsgegevens heeft verzameld en voor welke andere wettelijke bevoegdheid zij deze gegevens verder wil verwerken in een andere afdeling.

3.2.5 Positie van wijkteams en jeugdteams

Binnen gemeenten zijn er vaak één of meerdere wijkteams of jeugdteams actief. De wijze waarop deze zijn georganiseerd en de taken die zij uitoefenen verschilt per gemeente. In veel gevallen zijn sociale (wijk)teams opgezet als samenwerkingsverband. In andere gevallen zijn professionals van zorginstanties gedetacheerd bij een gemeente, in dienst getreden bij een gemeente, of is er een separate rechtspersoon opgericht. Het verschilt ook per gemeente welke zorg- en welzijnsorganisaties participeren in het wijk- of jeugdteam en welke taken door de teams worden uitgevoerd.

In veel gemeenten is het team een multidisciplinair team bestaande uit professionals afkomstig van de gemeente en/of publieke en private organisaties. Het wijkteam voert dan veelal twee verschillende taken uit, die beide een ander juridisch regime kennen met betrekking tot gegevensverwerking. De ene taak is de publiekrechtelijke taak van het college van B&W voor toeleiding naar voorzieningen of jeugdhulp. De andere is het verlenen van hulp in het kader van (meestal vrij toegankelijke) jeugdhulp of een algemene voorziening.

In de Privacy Impact Assessment 3D van het kabinet uit 2014[12] wordt uitgebreid ingegaan op de verschillende organisatievormen en werkzaamheden van wijk- en jeugdteams. Daarin wordt ook geschetst hoe gemeenten bij de inrichting van teams en bij de afspraken met organisaties rekening moeten houden met deze juridische complexiteit. In lijn met de PIA 3D hebben ook de Privacy Advies Commissie van Amsterdam en het Service Centrum Veiligheid en Privacy van het Ministerie van Justitie en Veiligheid adviezen uitgebracht. De essentie daarvan wordt hier onder kort weer gegeven.

Bij teams die zowel werkzaamheden verrichten in het kader van de gemeentelijke toeleiding naar hulp of voorzieningen, als hulp verlenen, moet een onderscheid gemaakt worden tussen deze twee taken. De toeleidingstaken voert de professional uit in het kader van de taken en bevoegdheden van het college van B&W. Dit zijn publiekrechtelijke taken. En hierop is het juridisch kader van de publiekrechtelijke taak van het college van B&W van toepassing. Het maakt daarbij voor de uitvoering van de gemeentelijke toeleidingstaken niet uit of de medewerker rechtspositioneel een ambtenaar is of een medewerker van bijvoorbeeld een hulpverleningsorganisatie.

De werkzaamheden in het kader van zorg- of hulpverlening voert de medewerker uit als zorg- of hulpverlener. Voor de jeugdhulpverlener en de medisch professional is voor die werkzaamheden hun dossierplicht van belang. Ook zijn hun wettelijke geheimhoudingsverplichtingen en beroepscodes van belang.
Publiekrechtelijke taken zijn bijvoorbeeld de collegetaak inzake de toeleiding naar maatwerkvoorzieningen of jeugdhulp. Het gaat dan om het onderzoeken van een melding in het kader van de WMO conform paragraaf 2.3 WMO, of het bepalen of en zo ja welke jeugdhulp een jeugdige of ouder nodig heeft inzake de Jeugdwet conform artikel 2.3 Jw. Andere taken die onder de verantwoordelijkheid van het college van B&W vallen zijn het zorgen voor de beschikbaarheid van voorzieningen, het opstellen van beleid, contractering van zorgaanbieders en de financieel-administratieve afhandeling van facturen en declaraties van zorgaanbieders.

De feitelijke hulpverlening houdt de daadwerkelijke levering in van de voorziening of zorg die iemand krijgt op grond van de Jeugdwet, de WMO, of de Wet gemeentelijke schuldhulpverlening. Hierbij kan men denken aan het aanmeten van een traplift of het verlenen van jeugdhulp. In nagenoeg alle gevallen wordt hulpverlening uitgevoerd door hulpverleningsorganisaties. Een gemeente kan er – in beginsel - ook voor kiezen hulpverlening zelf te leveren. Als een gemeente zelf hulpverlening levert, dan treedt zij daarbij op als maatwerkaanbieder of jeugdhulpverlener. Zij onderscheidt zich bij hulpverlening niet wezenlijk van andere dienstverleners of zorgaanbieders. Hulpverlening valt bij de WMO en de Jeugdwet niet onder de publiekrechtelijke taak van het college van B&W. Deze dienst- of hulpverleningstaken worden veelal uitgevoerd door professionals die zijn gebonden aan een beroepsgeheim.

[12] Privacy Impact Assessment Gemeentelijke 3D Informatiehuishouding, den Haag 2014, https://www.gemeentenvandetoekomst.nl/themas/sociaal-domein/publicatie/privacy-impact-assessment-3d-rapport-2014/

Grondslagen voor gegevensverwerking
Voor de gegevens die een wijkteammedewerker verwerkt in het kader van de toeleidingstaken is de grondslag conform de AVG artikel 6, lid 1, onder e: 'noodzakelijk voor de goede uitvoering van een taak in het kader van de uitoefening van openbaar gezag' (publiekrechtelijke taak).

Voor de gegevens die een wijkteammedewerker verwerkt in het kader van hulpverlening kunnen meerdere grondslagen conform de AVG van toepassing zijn. Als het echt om een medische behandelrelatie gaat is de grondslag artikel 6, lid 1, onder b: 'noodzakelijk voor de uitvoering van een overeenkomst'. Als het bijvoorbeeld gaat om het uitvoeren van individuele hulp of een algemene voorziening, zijn artikel 6, lid 1, onder e, 'noodzakelijk voor de uitvoering van een taak van algemeen belang' of artikel 6, lid 1, onder f, 'noodzakelijk voor de behartiging van een gerechtvaardigd belang' van toepassing.

Op de persoonsgegevens die een medewerker van het wijkteam verwerkt in het kader van het verlenen van jeugdhulp, of medische zorg zijn de dossierplicht en het beroepsgeheim van de jeugdhulpverlener of de medisch professional van toepassing. Gegevens kunnen verstrekt worden als het college van B&W die gegevens nodig heeft in het kader van de toeleiding naar jeugdhulp of het doen van een verzoek tot onderzoek bij de Raad voor de Kinderbescherming. Hierbij geldt een wettelijke verplichting voor jeugdhulpaanbieders, om – voor zover noodzakelijk - gegevens aan het college van B&W te verstrekken (artikel 7.4.0, lid 2 en 3 Jw).

Verwerkingsverantwoordelijkheid sociale wijkteams m.b.t. de toeleidingstaak
Indien het wijkteam als aparte rechtspersoon of als samenwerkingsverband is georganiseerd, blijft het college van B&W veelal de verwerkingsverantwoordelijke voor de gegevensverwerking in het kader van de toeleidingstaken. De organisatie of deelnemende organisaties hebben ten aanzien van deze taken veelal de juridische positie van verwerker. Het is ook mogelijk dat het college van B&W op een andere manier de bevoegdheid regelt, waarbij de medewerkers van het wijkteam handelen onder het gezag van het college van B&W.

Consequenties voor het betrekken van een wijkteammedewerker bij een casus
Indien een wijkteam gevraagd wordt om deel te nemen aan het behandelen van een casus in het zorg- en veiligheidsdomein, zal eerst duidelijk moeten zijn vanuit welke taak deelname gevraagd wordt. Betreft het feitelijk een verzoek aan het college van B&W om deel te nemen vanuit haar verantwoordelijkheden met betrekking tot de Jeugdwet, WMO, Participatiewet of Wet schuldhulpverlening? Of wordt een specifieke medewerker gevraagd vanuit zijn of haar betrokkenheid als behandelaar of jeugdhulpverlener? De betrokkenheid vanuit de taken van het college van B&W zal aan de orde zijn als het noodzakelijk is om zicht te krijgen op reeds ingezette voorzieningen of de mogelijkheden om voorzieningen in te zetten. De betrokkenheid vanuit de rol van de hulpverlener kan aan de orde zijn als het noodzakelijk is om tot afstemming te komen tussen een ingezet hulpverleningstraject en andere interventies.

3.3 GGZ

3.3.1 Doelstelling en taken
GGZ Nederland behartigt de belangen van de bij haar aangesloten instellingen en ondersteunt en adviseert de leden op diverse onderwerpen. Ook verricht zij lobby activiteiten in Den Haag om de wet en regelgeving beter te laten aansluiten op de praktijk van het veld.

De aangesloten instellingen van GGZ Nederland leveren gespecialiseerde ggz aan volwassenen, kinderen en jeugdigen, aan verslaafden en aan forensische patiënten. Zij hebben een publieke taak bij verplichte (al dan niet forensische) zorg. Ook bieden zij zo nodig maatschappelijke ondersteuning, beschermd wonen en bemoeizorg.
De doelstelling van de leden is door de verschillende in te zetten interventies bij te dragen aan een veilige, en mentaal gezondere samenleving. Indien dat niet mogelijk is, de patiënten te ondersteunen om terugval te voorkomen en/of in hun herstel.

3.3.2 Toepasselijke wet- regelgeving
De grondslag voor het verstrekken en ontvangen van gegevens kan gebaseerd worden op:
- de Wet verplichte ggz;
- de Wet forensische zorg en het Besluit forensische zorg (en eventuele ministeriële regelingen);
- de WGB;
- de Jeugdwet;
- de Wet BIG;
- de Penitentiaire Beginselenwet;
- de Penitentiaire Maatregelen;
- de Beginselenwet Verpleging Terbeschikkinggestelden;
- het Reglement Verpleging Terbeschikkinggestelden;
- de Wet Justitiële en strafvorderlijke gegevens;
- het Besluit JSG;
- de AVG.

3.3.3 Wettelijk kader gegevensverwerking en verstrekken van persoonsgegevens
De grondslag voor het verstrekken van gegevens zijn de Wet verplichte ggz, de Wet forensische zorg en het Besluit forensische zorg en de WGBO, de Jeugdwet, de Wet BIG, Pbw, PM, Bvt, de Rvt, Wsjg, Besluit JSG, en de AVG.[13]

Geheimhoudingsplicht en beroepsgeheim
Op grond van de WGBO rust op de GGZ-hulpverlener een geheimhoudingsplicht. Dat betekent dat er naast een wettelijke grondslag voor het uitwisselen van gegevens ook toestemming moet zijn om het beroepsgeheim te doorbreken. Doorbreking van het beroepsgeheim zonder wettelijke grondslag en zonder toestemming van de cliënt is alleen mogelijk wanneer er sprake is van een conflict van plichten. In de bovengenoemde wetten is er voor een aantal situaties een wettelijke verplichting dan wel bevoegdheid

[13] Zie voor meer informatie over gegevensverwerking in het kader van de Wvggz, Wzd en Wfz het addendum bij dit Handvat.

gecreëerd om gegevens te verstrekken aan specifieke partijen voor een specifieke taak. In die situaties mag de GGZ-hulpverlener gegevens verstrekken zonder toestemming. Voor meer informatie over het beroepsgeheim wordt verwezen naar paragraaf 2.7.

3.3.4 Belang van samenwerking in een samenwerkingsverband
Samenwerking kan leiden tot een ketenoverstijgende aanpak, waardoor de verschillende in te zetten interventies beter op elkaar afgestemd kunnen worden.
Daarnaast kan de samenwerking bijdragen aan verhoging van de kwaliteit van de door de ketenpartners in te zetten interventies; daarmee sluiten de doelstellingen op elkaar aan. Betrokkenen krijgen de juiste zorg hetgeen weer een bijdrage levert aan de veiligheid van de maatschappij.

Risico's bij niet samenwerken: je mist mogelijke risico's bij betrokkenen, bij kinderen en dat kan ook een gevaar opleveren voor de maatschappij

Door de input van de lidinstellingen, kan elkaars perspectief worden verrijkt zodat er nog betere afgestemde zorg geleverd kan worden. En dus de maatschappij weer veiliger gemaakt wordt.

3.4 Gecertificeerde Instellingen (GI)

De GI zijn verenigd in de branchevereniging Jeugdzorg Nederland, welke organisatie de belangen behartigt van alle organisaties die verantwoordelijk zijn voor jeugdhulp en de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering en die vallen onder de Jeugdwet. Een overzicht van de GI is te vinden op https://www.jeugdzorgnederland.nl/onze-leden/.

3.4.1 Doelstelling en taken
Kinderen hebben het recht om veilig op te groeien zodat ze later als evenwichtige volwassenen volwaardig kunnen meedoen in de maatschappij. Ouders zijn hiervoor het eerst verantwoordelijk. Als die hun pedagogische verantwoordelijkheid niet nemen of waarmaken, kan de veiligheid en ontwikkeling van het kind ernstig bedreigd worden. Dan is soms jeugdbescherming nodig. Jeugdreclassering is een vorm van gedwongen jeugdbescherming wanneer een jongere met het strafrecht in aanraking is gekomen, waarbij de jongere wordt geholpen, begeleid en gecontroleerd. Het doel van jeugdreclassering is om in samenwerking met ouder(s) of netwerk, het gedrag van de jongere te veranderen en recidive te voorkomen.

Soms dreigt een onveilige situatie voor een jeugdige maar kan in samenwerking met (lokale) professionals, ouders en het netwerk een justitiële maatregel worden afgewend. Dit wordt preventieve jeugdbescherming genoemd. Preventieve jeugdbescherming is tijdelijk, gericht op het herstel en versterking van de eigen kracht van het kind of de jongere en het gezin.

De GI voert de gedwongen en preventieve jeugdbescherming uit. De GI heeft de volgende wettelijke taken:

- het uitvoeren van kinderbeschermingsmaatregelen als bedoeld in artikel 1.1 Jeugdwet, te weten voogdij en voorlopige voogdij op grond van boek 1 van het Burgerlijk wetboek (BW), de ondertoezichtstelling als bedoeld in artikel 1:255 eerste lid BW en de voorlopige ondertoezichtstelling als bedoeld in artikel 1:257 BW;
- het uitvoeren van jeugdreclasseringstaken als bedoeld in artikel 1.1 Jeugdwet, te weten reclasseringswerkzaamheden genoemd in artikel 77hh Sr, eerste en tweede lid, het begeleiden van en toezicht houden op jeugdigen die deel nemen aan een scholings- en trainingsprogramma als bedoeld in artikel 3 Beginselenwet justitiële jeugdinrichtingen, het geven van aanwijzingen als bedoeld in artikel 12, vijfde lid van die wet of de overige taken die bij of krachtens de wet aan de GI zijn opgedragen.

In het kader van de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering bepaalt de GI in overleg met de gemeente welke jeugdhulp moet worden ingezet (artikel 3.5 Jeugdwet).

Daarnaast kan de GI nog overige taken aanbieden, anders dan het aanbieden van jeugdhulp, zoals het betrokken zijn voordat een kinderbeschermingsmaatregel wordt ingezet of het bieden van nazorg na afloop van een kinderbeschermingsmaatregel zodat de duur van de maatregel bekort kan worden (ook wel ‘drangkader’ genoemd). Of het bieden van nazorg na afloop van een jeugdreclasseringsmaatregel (nazorgtraject). Ook worden door bepaalde GI (een deel van) de taken van Veilig Thuis uitgevoerd.

3.4.2 Toepasselijke wet- en regelgeving

De grondslag voor het verwerken van persoonsgegevens is gelegen in de wetten waarin de taken van de GI staan vermeld:

- boek 1 van het Burgerlijk Wetboek (o.a. de artikelen 255 eerste lid, 257, eerste lid, 268 tweede en derde lid en artikel 302 eerste lid);
- de Jeugdwet (o.a. artikel 1.1, artikel 3.1 eerste en vierde lid, artikel 3.2, artikel 3.5, artikel 7.3.1, 7.3.8 en artikel 7.3.11);
- In het kader van de Jeugdwet zijn tevens van belang het Besluit Jeugdwet (o.a. artikel 4.2.5), de Invoeringswet Jeugdwet, de Regeling Jeugdwet;
- het Wetboek van Strafrecht (o.a. artikel 77hh eerste en tweede lid);
- Beginselenwet justitiële jeugdinrichtingen (o.a. artikel 3 en artikel 12, vijfde lid);
- WMO (o.a. artikelen 1.1.1, eerste lid en 4.1.1, tweede lid).

3.4.3 Wettelijk kader gegevensverwerking en verstrekking van persoonsgegevens

Verwerking van persoonsgegevens

Voor de uitvoering van de wettelijke taken van de GI is de grondslag gelegen in:

- artikel 6 lid 1 sub c AVG: “een wettelijke verplichting”;
- artikel 6 lid 1 sub e AVG: “een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag”.

Voor het verwerken in het kader van de taken op het gebied van nazorg en preventieve jeugdbescherming is de wettelijke verplichting gelegen in artikel 2.1 Jeugdwet.

Verder geldt voor de GI een dossierplicht. Nu de wetgever de inzet van deskundigheid van de GI in het vrijwillig kader mogelijk acht, past deze taak binnen de wettelijke taken van de GI. In het privacyreglement GI is er expliciet voor gekozen om de bepalingen van de Jeugdwet inzake dossierplicht, inzage en toestemming ook van toepassing te verklaren op de verslaglegging van de GI buiten het gedwongen kader. Voor het inzetten van jeugdhulp binnen nazorg en preventieve jeugdbescherming heeft de GI een mandaat van het College van burgemeester en wethouders nodig. Het college is op grond van artikel 2.3 Jw verantwoordelijk voor het bieden van jeugdhulp indien een jeugdige of ouder hulp nodig heeft in verband met opgroei- en opvoedingsproblemen, psychische problemen en stoornissen en voor zover de eigen mogelijkheden en het probleemoplossend vermogen ontoereikend zijn.

Privacyreglement
De GI hebben de wettelijke regelingen over het omgaan met persoonsgegevens verwerkt in een privacyreglement, te weten het Privacyreglement gecertificeerde instelling.

Beroepscode
De GI is verplicht de taken uit te laten voeren door medewerkers die zijn geregistreerd in het Kwaliteitsregister Jeugd (zie artikel 4.1.6 Jw en artikel 5.1.1 Besluit Jw) of het BIG register (zie artikel 4.1.6 Jw en artikel 5.1.1. Besluit Jw). Voor geregistreerde jeugdzorgwerkers is de Beroepscode voor de Jeugdzorgwerker van toepassing, voor geregistreerde psychologen de Beroepscode voor psychologen en voor geregistreerde (ortho)pedagogen de Beroepscode van de NVO. In artikel J van de beroepscode voor jeugdzorgwerkers, in artikel 71 t/m 87 van de beroepscode voor psychologen en in artikel 11 van de beroepscode van de NVO is bepaald dat de professional vertrouwelijk omgaat met informatie over de jeugdige, diens ouders/verzorgers en hun omstandigheden.

Bijzondere en strafrechtelijke persoonsgegevens
Op grond van artikel 7.3.8 lid 1 Jw dient de GI een dossier in te richten met betrekking tot de uitvoering van de jeugdbescherming. In dit dossier moet informatie worden opgenomen omtrent de geconstateerde opgroei- en opvoedingsproblemen, psychische problemen en stoornissen en de uitgevoerde verrichtingen en andere stukken voor zover deze voor een goede hulpverlening aan de betrokkene noodzakelijk is. Hierbij kan het ook gaan om bijzondere persoonsgegevens en gevoelige informatie als het BSN en strafrechtelijke gegevens.

Op grond van artikel 30 lid 2 sub b UAVG is de GI bevoegd om gegevens over de gezondheid te verwerken voor zover dat noodzakelijk is voor de uitvoering van de wettelijke taken.

Op grond van artikel 33 lid 1 UAVG mogen strafrechtelijke gegevens worden verwerkt door “organen die krachtens de wet zijn belast met de toepassing van het strafrecht”. De jeugdreclassering is krachtens haar wettelijke taken aan te merken als een orgaan dat krachtens de wet is belast met de toepassing van het strafrecht en valt derhalve onder de uitzondering van het verbod op het verwerken van strafrechtelijke gegevens.

Op grond van artikel 30 lid 5 UAVG mag de GI strafrechtelijke persoonsgegevens verstrekken aan instellingen en hulpverleners voor gezondheidszorg of maatschappelijke dienstverlening voor zover die instellingen de strafrechtelijke persoonsgegevens nodig hebben in aanvulling op de gegevens die zij verwerken voor een goede zorgverlening.

Daarnaast kan de GI ook gegevens verwerken op grond van artikel 22 lid 2 sub a en b UAVG, waarin (onder meer) de uitdrukkelijke toestemming van de betrokkene voor een verwerking is geregeld of de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven.

Artikel 7.3.11 vierde lid Jw bepaalt dat derden die beroepshalve beschikken over informatie over een onder toezicht gestelde jeugdige of diens ouders/verzorgers/voogd, welke informatie noodzakelijk kan worden geacht voor de uitvoering van de ondertoezichtstelling, deze informatie aan de GI verstrekken. De informatie kan uit eigen beweging of op verzoek van de GI worden verstrekt. Hiervoor is geen toestemming van betrokkenen nodig en de informatie kan indien nodig met doorbreking van de geheimhoudingsverplichting worden verstrekt. Het gaat hier niet alleen om hulpverleners die direct bij het kind zijn betrokken, maar ook om hulpverleners die betrokken zijn bij andere gezinsleden. Ook de jeugdhulpaanbieder die een medische behandeling biedt die onder de Wgbo valt, heeft de verplichting relevante informatie te verstrekken. De verplichte informatieverstrekking ziet alleen op de ondertoezichtstelling en geldt dus niet als sprake is van voogdij of jeugdreclassering.

Op grond van artikel 9 Wjsg juncto artikel 17 Bjsg is de jeugdreclassering bevoegd om voor de uitvoering van haar (wettelijke) taken over justitiële gegevens te beschikken. Artikel 52 Wjsg verplicht de jeugdreclassering tot geheimhouding van deze gegevens "*behoudens voor zover een bij of krachtens deze wet gegeven voorschrift mededelingen toelaat, dan wel de uitvoering van de taak met het oog waarop de gegevens zijn verstrekt tot het ter kennis brengen daarvan noodzaakt*".

Verstrekking van persoonsgegevens

De gegevensverstrekking aan andere instanties van (bijzondere) persoonsgegevens moet berusten op een wettelijke grondslag. Voor de uitwisseling met de volgende instanties (voor zover relevant in het kader van dit Handvat) is een wettelijke grondslag:

1. Rechtstreeks bij de verlening van de jeugdhulp betrokkenen en de vervanger van de medewerker van de GI (artikel 7.3.11 lid 2 sub a Jw). De betrokken (gezins)voogdijwerker en diens vervanger zijn in ieder geval rechtstreeks betrokken bij de uitvoering van een kinderbeschermingsmaatregel. Op grond van de toelichting op de Jeugdwet is niet geheel duidelijk wie nog meer als rechtstreeks betrokken kunnen worden beschouwd. Gelet op de toelichting van de wet voorafgaand aan de Jeugdwet, de Wet op de jeugdzorg, en de toelichting bij de Wgbo kunnen ook de gedragsdeskundige die wordt geconsulteerd, collega's met wie samen beslissingen betreffende het gezin worden genomen, de betrokken jeugdhulpaanbieder en het betrokken pleeggezin worden beschouwd als 'rechtstreeks bij de uitvoering betrokken'.

De gemeente kan niet worden aangemerkt als rechtstreeks bij de uitvoering betrokken, tenzij het college zelf de jeugdhulp verstrekt (bijv. d.m.v. het wijkteam).

2. De rechterlijke macht en OM in het kader van de wettelijke taken, zie o.a. de artikelen 1:260 tweede lid BW, 1:265c tweede lid BW op grond waarvan de GI de bevoegdheid heeft om verlenging van de ondertoezichtstelling en de machtiging tot uithuisplaatsing te verzoeken. Zie ook bijv. art. 77 f eerste lid Sr op grond waarvan de Officier van Justitie in de strafbeschikking de aanwijzing kan geven dat de jeugdige zich dient te houden aan de aanwijzingen van de jeugdreclassering voor een te bepalen termijn van max. 6 maanden.

3. De Raad voor de Kinderbescherming. Op grond van artikel 3.1 eerste lid Jw kan de GI de RvdK verzoeken om onderzoek te doen naar de noodzaak van een kinderbeschermingsmaatregel. De RvdK heeft verder een toezichthoudende taak op de uitvoering van de jeugdreclassering ingevolge artikel 77 hh eerste lid Sr en de tenuitvoerlegging van taakstraffen zie artikel 77o Sr. Ook heeft de RvdK een verantwoordelijkheid in het kader van netwerk- en trajectberaden om jeugdigen weer voor te bereiden op terugkeer in de samenleving na verblijf in een justitiële jeugdinrichting op grond van artikel 21a Besluit tenuitvoerlegging jeugdstrafrecht 1994. Tevens biedt art. 1:240 BW de mogelijkheid voor professionals met een beroepsgeheim of zwijgplicht om de RvdK gevraagd en ongevraagd gegevens verstrekken indien dit noodzakelijk is voor de uitvoering van de taken van de Raad.

4. Veilig Thuis. Op grond van artikel 5.2.6 WMO kunnen derden die beroepshalve beschikken over inlichtingen die noodzakelijk kunnen worden geacht om een situatie van huiselijk geweld of kindermishandeling te beëindigen of een redelijk vermoeden daarvan te onderzoeken, aan een Veilig Thuis deze inlichtingen desgevraagd of uit eigen beweging verstrekken zonder toestemming van degene die het betreft en indien nodig met doorbreking van de plicht tot geheimhouding op grond van een wettelijk voorschrift of op grond van hun ambt of beroep. Deze derden dienen wel de stappen uit de in hun organisatie geldende meldcode te doorlopen.

5. Aan een gezinsvoogd van de GI, als die erom vraagt wanneer een minderjarige onder toezicht is gesteld (artikel 7.3.11 lid 4 Jw).

6. De gemeente voor zover dit voortvloeit uit een wettelijke taak (zie o.a. § 7.4 Jw). Het verstrekken van gegevens aan de gemeente is slechts in bepaalde situaties een wettelijke verplichting. Buiten deze situaties mogen geen gegevens verstrekt worden anders dan met toestemming. Binnen de wettelijke verplichting dient zorgvuldig en proportioneel omgegaan te worden met het verstrekken van cliëntgegevens. De informatieverstrekking over het feit dat een maatregel is opgelegd, verloopt bijv. via CORV waar ook de RvdK, de politie, het CJIB, Veilig Thuis en het OM op zijn aangesloten. De betreffende rechterlijke uitspraak wordt niet naar de gemeente gezonden.

Op grond van artikel 7.4.0 Jw jo. artikel 6 Regeling Jeugdwet dient de GI aan het college van B&W persoonsgegevens van de jeugdige of zijn ouders te verstrekken waaronder het BSN en andere bijzondere persoonsgegevens die voor het college van B&W noodzakelijk zijn voor de uitvoering van:

- de toeleiding naar, advisering over, bepaling van of het inzetten van een voorziening op het gebied van de jeugdhulp
- het doen van een verzoek tot onderzoek bij de RvdK
- de bekostiging van o.a. preventie, jeugdhulp, kinderbeschermings-maatregelen en jeugdreclassering.

Artikel 3.5 Jw bepaalt dat overleg over de inzet van jeugdhulp plaatsvindt met de gemeente. Dit overleg is er primair op gericht om te weten welke jeugdhulp door de gemeente is gecontracteerd. Uit de Memorie van Antwoord (EK 2013-2014, 33684 F p. 45 e.v.) blijkt dat alleen overleg op individueel inhoudelijk niveau zal plaatsvinden als het gaat om jeugdhulp die niet door de gemeente is gecontracteerd zodat met de gemeente afgestemd kan worden over de nog in te kopen jeugdhulp. Dit betreft uitdrukkelijk niet het standaard verstrekken van (delen uit) dossiers of plannen van aanpak.

7. Externe deskundigen voor zover informatieverstrekking aan hen nodig is als toelichting op vragen van de GI of een door de rechterlijke macht gelast onderzoek in het kader van de uitvoering van de wettelijke taken. Voor dergelijke diagnostiek wordt toestemming van de cliënt verzocht of vervangende toestemming van de kinderrechter op grond van artikel 1:265 h of artikel 1:265 e eerste lid sub b BW.

8. De justitiële jeugdinrichting en de selectiefunctionaris, in het kader van de uitvoering van een toezicht of begeleiding in het kader een scholings- en trainingsprogramma als bedoeld in artikel 3 Beginselenwet justitiële jeugdinrichtingen of in het kader van het geven van aanwijzingen als bedoeld in artikel 12 vijfde lid van deze wet. Aan de justitiële jeugdinrichting en de gemeente kunnen tevens gegevens worden verstrekt in het kader van nazorg jeugd, om de terugkeer van de jeugdige in de maatschappij voor te bereiden, op grond van artikel 21a Besluit tenuitvoerlegging jeugdstrafrecht 1994.

9. De rechtbank in het kader van jeugdstrafzaken van onder haar voogdij gestelde jeugdigen (artikel 496 eerste lid Sv). De GI is verplicht om te verschijnen maar bevoegd om in te brengen wat tot verdediging kan dienen (artikel 496 tweede lid Sv).

10. De Verwijsindex Risicojongeren (VIR). De jeugdhulpaanbieder is bevoegd om zonder toestemming van de jeugdige of zijn wettelijk vertegenwoordiger(s) en zo nodig met doorbreking van het beroepsgeheim, een jeugdige te melden aan de verwijsindex indien hij een redelijk vermoeden heeft dat de jeugdige door een of meer risico's in de noodzakelijke condities voor een gezonde en veilige ontwikkeling naar volwassenheid wordt bedreigd op basis van artikel 7.1.4.1 Jw en artikel 7.1.1 Besluit Jw. Indien er na melding in de VIR een 'match' ontstaat tussen meldingsbevoegde instellingen, kunnen gegevens alleen verstrekt worden indien

hiervoor een wettelijke grondslag is, uitdrukkelijke toestemming is verleend of er sprake is van een situatie van conflict van plichten.

In de hierboven aangehaalde wetgeving wordt de politie niet specifiek genoemd. De geheimhoudingsplicht van de medewerker van de GI zal doorgaans aan verstrekking van informatie aan de politie in de weg staan. In de situatie van overmacht zal de GI wel overgaan tot verstrekking van gegevens, doorgaans wordt dan ook aangifte of melding gedaan bij de politie.

Met uitdrukkelijke toestemming van de cliënt is het in de regel wel mogelijk om (bijzondere) persoonsgegevens uit te wisselen met instanties waarvoor geen wettelijke basis bestaat. Dat zou alleen anders kunnen zijn als deze toestemming niet in vrijheid gegeven wordt.

Geheimhoudingsplicht en beroepsgeheim
Voor medewerkers van een GI geldt een beroepsgeheim op grond van artikel 7.3.11 Jw: zonder toestemming van de jeugdige en/of zijn ouder mogen zij geen gegevens over hen aan derden verstrekken. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van de betrokkene(n) niet wordt geschaad. Voor de uitleg van het beroepsgeheim en mogelijke uitzonderingen daarop wordt verwezen naar hoofdstuk 2.7 van dit handvat.

3.4.4 Belang van samenwerking in een samenwerkingsverband
De GI komt pas in beeld als inzet van hulp in het vrijwillig kader stagneert. Veelal is er in deze situaties sprake van complexe problematiek en zijn er problemen op verschillende leefgebieden. De GI streeft naar een zo verantwoord mogelijke ontwikkeling en opvoedingssituatie van de jeugdige. Dit sluit aan bij de doelstelling van de samenwerkingsverbanden in het zorg- en veiligheidsdomein om maatschappelijke uitval bij complexe problemen te voorkomen en verminderen. Voor zover het de uitoefening van de jeugdreclassering betreft, streeft de jeugdreclassering naar minder crimineel gedrag, het voorkomen van recidive en daarmee een veiliger samenleving. Samenwerking kan bijdragen aan het bundelen van expertise en om tot een integrale aanpak te komen als er een keten overstijgende aanpak nodig is.

3.5 Jeugdhulp

3.5.1 Doelstelling en taken
De organisaties die in het kader van de Jeugdwet jeugdhulp bieden in opdracht van gemeenten kunnen verschillende achtergronden hebben. In grote lijnen zijn de volgende doelgroepen te onderscheiden:

- Jeugdigen met psychiatrische problematiek die jeugdhulp ontvangen van leden van GGZ Nederland: deze zorg viel voor 2015 onder de Zorgverzekeringswet;
- Jeugdigen met een handicap die jeugdhulp ontvangen van leden van de Vereniging Gehandicaptenzorg Nederland (VGN): deze zorg viel voor 2015 onder de Algemene Wet Bijzondere Ziektekosten (AWBZ) en
- Jeugdigen met opvoed- en opgroeiproblemen die jeugdhulp ontvangen van leden

Jeugdzorg Nederland geholpen worden: deze zorg viel voor 2015 onder de Wet op de Jeugdzorg.

3.5.2 Toepasselijke wet- en regelgeving

De grondslag voor de jeugdhulpaanbieder voor het verwerken van persoonsgegevens is gelegen in de wetten waarin de taken en bevoegdheden van de jeugdhulpaanbieder staan vermeld:

- de Jeugdwet (o.a. artikel 1.1, 4.1.1, 7.3.1, 7.3.11 en 7.1.4.1 Jw.);
- het Besluit Jeugdwet (o.a. artikel 7.1.1);
- de Invoeringswet Jeugdwet;
- de Regeling Jeugdwet;
- de Verzamelwet VWS 2016.

3.5.3 Wettelijk kader gegevensverwerking en verstrekken van persoonsgegevens

De jeugdhulpaanbieder verwerkt naast 'gewone' persoonsgegevens ook bijzondere persoonsgegevens zoals gezondheidsgegevens. Artikel 30 UAVG biedt voor de jeugdhulpaanbieders een expliciete grondslag voor de verwerking van persoonsgegevens betreffende de gezondheid. De jeugdhulpaanbieders mogen op grond van deze bepaling gezondheidsgegevens verwerken voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene noodzakelijk is.

De gegevensverstrekking aan andere instanties van (bijzondere) persoonsgegevens van cliënten moet rusten op een wettelijke grondslag. Voor de uitwisseling met de volgende instanties is een wettelijke grondslag:

- De gezinsvoogd. Op grond van artikel 7.3.11 lid 4 Jw. is de jeugdhulpaanbieder bevoegd de gezinsvoogd te informeren over feiten en omstandigheden die de persoon van een onder toezicht gestelde minderjarige, diens verzorging en opvoeding of de persoon van een ouder of voogd betreffen èn deze inlichtingen noodzakelijk kunnen worden geacht voor de uitvoering van de ondertoezichtstelling;
- De jeugdhulpverlener heeft de mogelijkheid op basis van art. 7.3.11 tweede lid Jw. om met degene die rechtstreeks bij de hulpverlening betrokken is informatie uit te wisselen, ook als de cliënt daar geen toestemming voor geeft. Dit is echter een beperkte kring (in ieder geval de eigen vervanger, gedragswetenschapper en interne collega's met wie over het gezin wordt overlegd);
- De Raad voor de Kinderbescherming. Art. 1:240 BW biedt professionals met een beroepsgeheim of zwijgplicht de mogelijkheid om de RvdK gevraagd en ongevraagd gegevens te verstrekken indien dit noodzakelijk is voor de uitvoering van de taken van de RvdK;
- Veilig Thuis. Op grond van artikel 5.2.6 WMO kunnen derden die beroepshalve beschikken over inlichtingen die noodzakelijk kunnen worden geacht om een situatie van huiselijk geweld of kindermishandeling te beëindigen of een redelijk vermoeden daarvan te onderzoeken, aan Veilig Thuis deze inlichtingen desgevraagd of uit eigen beweging verstrekken zonder toestemming van degene die het betreft en indien nodig met doorbreking van de plicht tot geheimhouding op grond van een wettelijk voorschrift of op grond van hun ambt of beroep. Deze derden dienen wel de stappen uit de voor hun branche geldende meldcode te doorlopen;

- De gemeente voor zover dit voortvloeit uit een wettelijke taak (zie o.a. § 7.4 Jw). Deze informatieverstrekking ziet onder andere op de verplichting om informatie te verstrekken ten behoeve van de toeleiding naar jeugdhulp,op beleidsmatige informatie, informatie ten behoeve van de bekostiging van preventie, jeugdhulp, kinderbeschermingsmaatregelen, jeugdreclassering of werkzaamheden in het kader van het verzoeken van een machtiging gesloten jeugdhulp en het verrichten van controle of fraude-onderzoek. Het verstrekken van gegevens aan de gemeente is slechts in bepaalde situaties een wettelijke verplichting. Buiten deze situaties mogen geen gegevens verstrekt worden anders dan met toestemming. Binnen de wettelijke verplichting dient zorgvuldig en proportioneel omgegaan te worden met het verstrekken van cliëntgegevens;
- Instanties die bevoegd zijn een oordeel te geven over de handelwijze van de jeugdhulpverlener naar aanleiding van een klacht zoals de klachtencommissie van de jeugdhulpverlener, de Inspectie Jeugdzorg, Landelijk Toezicht Jeugd, SKJ (College van Toezicht/College van Beroep) en de Kinderombudsman zie o.a. artikel 4.2.1 vierde lid Jw, artikel 9.1 Jw en artikel 11b tweede lid Wet Nationale Ombudsman;
- De verwijsindex Risicojongeren. De jeugdhulpaanbieder is bevoegd om zonder toestemming van de jeugdige of zijn wettelijk vertegenwoordiger en zo nodig met doorbreking van het beroepsgeheim, een jeugdige te melden aan de verwijsindex indien hij een redelijk vermoeden heeft dat de jeugdige door een of meer risico's in de noodzakelijke condities voor een gezonde en veilige ontwikkeling naar volwassenheid wordt bedreigd op basis van artikel 7.1.4.1 Jw en artikel 7.1.1 Besluit Jw;
- Verder is de jeugdhulpverlener verplicht om gevolg te geven aan een vordering verstrekking gegevens van het OM (artikel 126nd Sv).

In de hierboven aangehaalde wetgeving wordt ook de politie niet specifiek genoemd. De geheimhoudingsplicht van de jeugdhulpaanbieder zal doorgaans aan verstrekking van informatie aan de politie in de weg staan.

In de situatie van een conflict van plichten zal de jeugdhulpaanbieder wel kunnen overgaan tot verstrekking van gegevens aangezien dat de enige oplossing lijkt om gevaar af te wenden. De essentie van een conflict van plichten is dat jeugdhulpverlener dient te zwijgen op grond van de geheimhoudingsplicht, maar dat hij zich tegelijkertijd (moreel) verplicht kan voelen derden informatie te verschaffen om gevaar af te wenden. Hij stelt zich de vraag: zijn er andere belangen zo groot dat ik wel informatie moet delen om gevaar voor een ander, de patiënt of mezelf te voorkomen? Voor een uitgebreide uitleg van het beroepsgeheim en een conflict van plichten wordt verwezen naar paragraaf 2.7 van dit handvat.

Met uitdrukkelijke toestemming van de cliënt is het in de regel wel mogelijk om (bijzondere) persoonsgegevens uit te wisselen met instanties waarvoor geen wettelijke basis bestaat. Dat zou alleen anders kunnen zijn als deze toestemming niet in vrijheid gegeven wordt.

Beroepsgeheim
Jeugdhulpverleners hebben een beroepsgeheim op grond van artikel 7.3.11 Jw: zonder toestemming van de jeugdige en/of diens wettelijk vertegenwoordiger(s) mogen zij geen gegevens over hen aan derden verstrekken. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. Voor jeugdhulpverleners, die in de jeugdgezondheidszorg werkzaam zijn, geldt tevens het beroepsgeheim dat is vastgelegd in de WGBO. Dit beroepsgeheim is niet van toepassing voor de hier boven genoemde bepalingen die een wettelijke verplichting, dan wel bevoegdheid inhouden om gegevens te verstrekken aan de betreffende partij voor zover noodzakelijk en zo nodig met doorbreking van het beroepsgeheim.

3.6 Openbaar Ministerie

3.6.1 Doelstelling en taken
Het OM is op grond van art. 124 Wet op de Rechterlijke Organisatie (Wet RO) belast met de strafrechtelijke handhaving van de rechtsorde. Het OM heeft op grond van art. 12 Politiewet (PW) het gezag over de opsporing van strafbare feiten en is verantwoordelijk voor het vervolgen daarvan, alsmede voor de tenuitvoerlegging van de opgelegde straffen (artikel 124 Wet op de rechterlijke organisatie). Het Openbaar Ministerie is de enige instantie in Nederland die verdachten voor de strafrechter kan brengen. Het OM verricht ook civiel-rechterlijke en bestuursrechtelijke taken.

3.6.2 Toepasselijke wet- en regelgeving
Voor gegevensuitwisseling bij casuïstiek is vooral de volgende wet- en regelgeving van toepassing[14]:
- de Wet op de Rechterlijke organisatie (Wet RO), de Aanwijzing gebruik sepotgronden;
- het Wetboek van Strafrecht (WvSr) [15];
- het Wetboek van Strafvordering (WvSv), waaronder de Wet OM afdoening (WOa), de Wet minimumnormen Slachtoffers[16] en de Richtlijnen voor strafvordering [17];

[14] Hier wordt alleen de wetgeving genoemd die op het moment van verschijnen van dit Handvat al in werking is getreden en geen wetten die nog aanhangig zijn in de Tweede en Eerste Kamer. Er wordt ook nog niet ingegaan op wetsvoorstellen waarover een internetconsultatie heeft plaatsgevonden of wetten die al zijn aangenomen in de Eerste Kamer maar die nog niet in werking zijn getreden, zoals bijv. de Wet USB, of de Wet verplichte GGZ (WvGGZ). De Wet USB (Herziening Tenuitvoerlegging strafvorderlijke Beslissingen): treedt in werking per 1/1/2020. Kst. 34086, Stbld 2017 nr 82. Deze wet heeft veel consequenties voor het OM en andere partijen in de strafrechtketen. In de eerstvolgende actualisering van het Handvat zal ook een hoofdstuk worden opgenomen over de gevolgen van de Wet USB.

[15] Sinds 1 april 2014 geldt het adolescentenstrafrecht. Jongeren tot 23 jaar kunnen volgens het strafrecht voor volwassenen worden berecht.

[16] Omzetting van de EU Richtlijn 2012/29/EU van het Europees parlement en de Raad van 25 oktober 2012 tot vaststelling van minimumnormen voor de rechten, de ondersteuning en de bescherming van slachtoffers van strafbare feiten, en ter vervanging van Kaderbesluit 2001/220/JBZ (PbEU 2012, L 315)(Kst 34236).

[17] Momenteel wordt gewerkt aan een wijziging van het Wetboek van strafvordering.

- de Wet Justitiële en Strafvorderlijke gegevens (Wjsg), de Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (Aanwijzing Wjsg) [18],en het Besluit justitiële en strafvorderlijke gegevens (Bjsg);
- indirect ook de Politiewet 2012 (PW); de Wpg, de Aanwijzing Wet politiegegevens (Wpg) en de rol van de Officier van Justitie;
- de Wet Bijzondere opnemingen psychiatrische ziekenhuizen (Wet BOPZ)[19]
- de Wet zorg en dwang (Wzd);
- de Wet forensische zorg (Wfz)[20];
- de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Deze zijn van toepassing op de civiele en bestuursrechtelijke taken van het OM[21] en op de verwerking van persoonsgegevens van al het OM personeel (bedrijfsvoering).

3.6.3 Wettelijk kader gegevensverwerking en verstrekken van gegevens

In de Wjsg staan de bepalingen met betrekking tot de verwerking van strafrechtelijke persoonsgegevens. Strafrechtelijke persoonsgegevens worden specifiek genoemd in art. 10 van de AVG. De strafrechtelijke taken van het OM vallen onder het bereik van de Richtlijn Gegevensbescherming Opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen (EU) 2016/680. De Richtlijn is in Nederland omgezet in de (reeds bestaande) Wpg en Wjsg. De Wjsg is een 'lex specialis' ten opzichte van de AVG en ook ten opzichte van de UAVG.

De Wjsg kent verschillende categorieën strafrechtelijke persoonsgegevens:
- strafvorderlijke gegevens (artikel 1 onder b Wjsg);
- justitiële gegevens (artikel 1 onder a Wjsg);
- persoonsdossier (artikel 1 onder c Wjsg).

Na de implementatie van de Richtlijn in de nieuwe Wjsg zijn daaraan toegevoegd:
- tenuitvoerleggingsgegevens (artikel 1 onder d Wjsg);
- gerechtelijke strafgegevens (artikel 1 onder e Wjsg).

[18] Het College van procureurs-generaal kan op grond van art. 130 zesde lid Wet RO algemene en bijzondere aanwijzingen geven betreffende taken en bevoegdheden van het OM. Aanwijzingen kunnen ook betrekking hebben op de uitvoering van (opsporings)taken die door de politie en andere opsporingsinstanties onder het gezag van het OM worden uitgevoerd. Aanwijzingen over de sanctietoepassing en het transactie- en rekwireerbeleid heten Richtlijnen voor strafvordering.

[19] Per 1-1-2020 treden de opvolgers van de Wet BOPZ in werking i.c. de Wet verplichte ggz (Wvggz, Kst 32399, Stbld 2018, nr. 37)),) en de Wet zorg en dwang (Wzd, Kst 31996, Stbld 2018 nr. 36)) De Wvggz ziet op personen met een psychische stoornis. Binnen de Wvggz heeft het OM een verzoekersrol, d.w.z. dat de OvJ een verzoek tot een zorgmachtiging kan doen bij de civiele rechter. De Wzd ziet op personen met een psychogeriatrische aandoening of verstandelijke beperking. De verzoekersrol ligt bij het CIZ tenzij er sprake is van strafbare feiten. Beide wetten hebben veel consequenties voor het OM en andere partijen binnen en buiten de strafrechtketen. In de eerstvolgende actualisering van het Handvat zal ook een hoofdstuk worden opgenomen over de gevolgen van deze wetten. Zie voor meer informatie het addendum bij dit Handvat over de Wet verplichte geestelijke gezondheid, Wet zorg en dwang en de Wet forensische zorg.

[20] De Wet forensische zorg (Wfz) Kst 32398 Stbl 2018 nr.38 is reeds in werking getreden, met uitzondering van artikel 2.3 Wfz. De Wfz ziet op personen die een strafbaar feit hebben gepleegd en waarbij er sprake is van een psychische stoornis of psychogeriatrische aandoening of verstandelijke beperking. De verzoekersrol ligt bij het OM indien betrokkene een strafbaar feit heeft gepleegd. In de volgende actualisering van het Handvat zal dieper worden ingegaan op de rol van het Zorg en Veiligheidshuis of andere overleggremia bij de Wfz zoals genoemd in Kst 32398 nr. P. Bijlage 857780. Zie voor meer informatie het addendum bij dit Handvat over de Wet verplichte geestelijke gezondheid, Wet zorg en dwang en de Wet forensische zorg.

[21] Voor de Wet administratiefrechtelijke handhaving verkeersvoorschriften (Wet Mulder) is de Wjsg van toepassing als de beslissing een strafrechtelijke afdoening inhoudt. Indien gelet op de geringere aard en ernst van de overtreding een administratiefrechtelijke beslissing is getroffen, is op de tenuitvoerlegging daarvan de AVG en de UAVG van toepassing.

Het College van procureurs- generaal is de verwerkingsverantwoordelijke voor de verwerking van strafvorderlijke gegevens en voor tenuitvoerleggingsgegevens (voor zo ver die door het OM worden verwerkt). De Minister van Justitie en Veiligheid is de verwerkingsverantwoordelijke voor de justitiële gegevens en rapporten in een persoonsdossier en tenuitvoerleggingsgegevens. De gerechten zijn de verwerkingsverantwoordelijke voor gerechtelijke strafgegevens. (artikel 1 onder k Wjsg).

Voor het OM geldt een geheimhoudingsplicht (art. 144 jo. art. 13 van de Wet RO). Deze geheimhouding is nodig voor een goede taakuitoefening van het OM en een goed verloop van het strafproces. De Wjsg kent ook een geheimhoudingsbepaling, op grond van art. 52 Wjsg is een ieder die krachtens de Wjsg de beschikking krijgt over deze gegevens verplicht tot geheimhouding daarvan, behoudens voor zover een bij of krachtens de Wjsg gegeven voorschrift mededelingen toelaat, dan wel de uitvoering van de taak met het oog waarop de gegevens zijn verstrekt tot het ter kennis brengen daarvan noodzaakt.

Verwerking van bijzondere categorieën van persoonsgegevens is mogelijk voor het OM. Op grond van art. 39c derde lid Wjsg mag het OM ook strafvorderlijke gegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt, even als genetische gegevens, biometrische gegevens (met het oog op de unieke identificatie van een natuurlijke persoon), of gegevens over gezondheid, seksuele leven en seksuele gerichtheid, registreren. Deze verwerking vindt slechts plaats voor zover dit voor het doel van de verwerking onvermijdelijk is, in aanvulling op de verwerking van andere strafvorderlijke gegevens betreffende de persoon.

Het OM kan overgaan tot de verstrekking van strafvorderlijke gegevens en in sommige gevallen ook van justitiële gegevens.[22] De verstrekkingsgrondslag voor het verstrekken van strafvorderlijke gegevens voor buiten het strafrecht gelegen doeleinden is gelegen in artikel 39f Wjsg. De verstrekkingsgrondslag voor de verstrekking door het OM van justitiële gegevens is gelegen in artikel 8a juncto artikel 39f Wjsg. Op grond van deze artikelen kan het OM, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, aan personen of instanties voor de volgende buiten de strafrechtspleging gelegen doeleinden respectievelijk strafvorderlijke gegevens en justitiële gegevens verstrekken:

- het voorkomen en opsporen van strafbare feiten;
- het handhaven van de orde en veiligheid;
- het uitoefenen van toezicht op het naleven van regelgeving;
- het nemen van een bestuursrechtelijke beslissing;
- het beoordelen van de noodzaak tot het treffen van een rechtspositionele of tuchtrechtelijke maatregel;

[22] Zodra de nieuwe Wet USB in werking is getreden volgt er een andere uitwerking over de ten uitvoerleggingsgegevens, gerechtelijke strafgegevens en gegevens in persoonsdossiers.

- het verlenen van hulp aan slachtoffers en anderen die bij een strafbaar feit betrokken zijn;
- het verrichten van een privaatrechtelijke rechtshandeling door een persoon of instantie die met een publieke taak is belast.

Het OM kan zowel actief (op eigen initiatief) als passief (op verzoek) strafvorderlijke gegevens verstrekken voor buiten de strafrechtspleging gelegen doeleinden. Het OM is op grond van artikel 39f Wjsg niet verplicht om deze gegevens te verstrekken. Alvorens tot verstrekking wordt overgegaan, wordt steeds een afweging gemaakt van het belang dat de ontvanger heeft bij het verkrijgen van de informatie ten opzichte van bijvoorbeeld de belangen van opsporing en vervolging en het belang van de bescherming van de persoonlijke levenssfeer van de betrokkene(n). Indien de uitkomst van een strafrechtelijk onderzoek nog onzeker is, dient door het OM meer terughoudendheid te worden betracht bij een verstrekking. Aan de andere kant betekent dit dat bij een bewijsbare zaak eerder de inbreuk op de persoonlijke levenssfeer van de betrokkenen gerechtvaardigd is. Bij deze belangenafweging dienen de beginselen van noodzakelijkheid, subsidiariteit en proportionaliteit te worden betrokken. Strafvorderlijke gegevens mogen niet worden verstrekt op grond van het enkele belang dat de derde daarbij heeft.

In de Aanwijzing Wjsg voor buiten de strafrechtspleging gelegen doeleinden staat dit nader uitgewerkt. In de Aanwijzing zijn de volgende uitgangspunten verwoord: geen plicht maar bevoegdheid, moet passen binnen de taakuitoefening van het OM, meer zekerheid omtrent de strafrechtelijke vervolging, passief en actief, subsidiair, noodzakelijk, proportioneel en evenredig.

Voor de vraag of het OM strafvorderlijke gegevens kan verstrekken wordt de algemene beoordelingsstructuur gevolgd. Daarin komen de volgende vragen aan de orde:
- Is de verstrekking nodig voor de goede taakvervulling van het OM?
- Is de verstrekking noodzakelijk met het oog op een zwaarwegend algemeen belang?
- Is het doel in lid 1 van artikel 39f Wjsg genoemd?
- Is de ontvangen informatie noodzakelijk voor de ontvangers met het oog op een zwaarwegend algemeen belang?
- Is sprake van een contra-indicatie (reden om niet te verstrekken)?

Er is sprake van een zwaarwegend algemeen belang wanneer het gaat om:
- het belang van de nationale veiligheid;
- de openbare veiligheid of het economisch welzijn van het land;
- het voorkomen van wanordelijkheden en strafbare feiten;
- de bescherming van de gezondheid of de goede zeden;
- de bescherming van rechten en vrijheden van anderen.

Uit jurisprudentie is gebleken dat de verstrekking ook legitiem, noodzakelijk en voorzienbaar moet zijn.

Contra-indicaties voor het OM om niet tot verstrekking over te gaan, zijn:

- er is nog geen definitieve vervolgingsbeslissing;
- de zaak is geëindigd in een sepot of vrijspraak.

Uitgangspunt is dat bij een contra-indicatie geen informatie wordt verstrekt, tenzij sprake is van een zwaarwegend belang dat de verstrekking toch rechtvaardigt. Een dergelijk geval is in ieder geval aanwezig in de volgende situaties:

- door middel van het verstrekken van informatie kan ernstig en acuut gevaar worden afgewend;
- het gedrag (nalaten daaronder begrepen) dat voorwerp is geweest van strafrechtelijk onderzoek past niet binnen een integere uitoefening van een overheidsfunctie;
- het gedrag (nalaten daaronder begrepen) dat voorwerp is geweest van strafrechtelijk onderzoek is relevant voor de vraag of een rechtspositionele dan wel tuchtrechtelijke maatregel moet worden genomen tegen iemand die als zelfstandige, werknemer, vrijwilliger of stagiaire een gevoelige functie bekleedt, indien dat vastgestelde handelen twijfels doet rijzen over zijn behoorlijk (beroepsmatig) functioneren;
- het verstrekken van informatie maakt het treffen van noodzakelijke organisatorische of bestuurlijke maatregelen mogelijk;
- het gedrag dat naar voren komt uit het strafrechtelijk onderzoek levert civielrechtelijk aansprakelijkheid op tussen het slachtoffer/de betrokkene en de (gewezen) verdachte.

Wanneer een zaak is geëindigd met een sepot of een vrijspraak geldt als uitgangspunt dat geen informatie wordt verstrekt, tenzij er sprake is van een zwaarwegend belang dat de verstrekking in dat geval rechtvaardigt. Wanneer nog geen definitieve vervolgingsbeslissing is genomen, geldt als uitgangspunt dat geen informatie wordt verstrekt tenzij sprake is van een spoedeisend belang dat de verstrekking in dat geval rechtvaardigt.

Als nog geen vervolgingsbeslissing is genomen, dient tevens sprake te zijn van een spoedeisend belang.

De Minister van Justitie en Veiligheid is de verwerkingsverantwoordelijke voor justitiële gegevens. Op grond van artikel 8a juncto artikel 39f Wjsg is het OM (i.c. het College van pg's) bevoegd om ook – alleen die justitiële gegevens (justitiële documentatie/historische overzichten) waarover het in het kader van de eigen taakuitvoering reeds beschikt,- door te verstrekken aan derden in die gevallen waarin op grond van 39f Wjsg strafvorderlijke gegevens aan derden kunnen worden verstrekt. Ook hier geldt dat justitiële gegevens niet mogen worden verstrekt op grond van het enkele belang dat een derde daarbij heeft. Per geval dient nadrukkelijk te worden nagegaan of de verstrekking van justitiële gegevens (mede) aangewezen is. Daarbij dient nadrukkelijk de noodzakelijkheid van de verstrekking door het OM te worden afgewogen. Artikel 8a Wjsg biedt geen grondslag voor het structureel verstrekken van justitiële gegevens aan derden.
Er worden ook zaken aangeleverd aan het ZVH door andere partijen, zonder dat hierbij sprake is van een aanhouding door de politie.

Steeds vaker werkt het Openbaar Ministerie ook voor buiten de strafrechtspleging gelegen doelen samen met verschillende partijen, zoals hulpverleningsinstellingen en gemeenten. Het doel van die samenwerking kan het verstrekken van strafvorderlijke en justitiële gegevens door het Openbaar Ministerie ten behoeve van die samenwerking rechtvaardigen. Teneinde die gegevensuitwisseling in te kaderen en zodoende oog te houden op de bescherming van de belangen van de verschillende betrokkenen, moet er een samenwerkingsconvenant annex Privacyprotocol worden afgesloten. Verder dient onder andere een workflow annex werkprocesbeschrijving, een privacystatement en een Privacy Impact Assessment (PIA) ofwel Gegevensbeschermingseffectbeoordeling (GEB) te zijn opgesteld. Alle documenten dienen ter goedkeuring te worden voorgelegd aan - in ieder geval- de Helpdesk Privacy van het Parket Generaal voordat tot ondertekening door het OM kan worden overgegaan.

Bij verstrekking geldt:

- Er mogen geen risico's voor de strafzaken ontstaan. Het "Gazo principe" (geen actie zonder overleg) is cruciaal. Daarnaast moet worden voorkomen dat – in de concrete strafzaak - een beroep wordt gedaan op artikel 359a Sv (vormverzuimen), omdat een onrechtmatige inbreuk is gemaakt op de privacy van betrokkenen of dat onrechtmatig gegevens zijn verstrekt door het OM of door degenen die onder het gezag van het OM opereren. Maar ook onrechtmatige verwerkingen door derden kunnen in bepaalde gevallen gevolgen hebben voor de strafzaak, in het ergste geval wordt het OM niet ontvankelijk verklaard[23]l;
- Te allen tijde zijn de ontvangende partijen gebonden aan de geheimhoudingsplicht van artikel 52 Wjsg. Dat wil zeggen dat de gegevens na verstrekking weliswaar vallen onder het regime van de AVG en dus persoonsgegevens zijn geworden, de geheimhoudingsplicht van de Wjsg is - net als bij de Wpg - nog steeds van toepassing op de door het OM verstrekte gegevens;
- Een groot deel van de strafvorderlijke gegevens zijn tevens politiegegevens. Daarom is afstemming met de politie nodig over wie wat verstrekt. Als een proces-verbaal is ingediend bij het OM (en de gegevens zich fysiek bij het OM bevinden) of gegevens in de OM-systemen zijn verwerkt, vindt de verstrekking in principe plaats door het OM. Wat het OM mogelijk nog aan relevante aanvullende strafvorderlijke gegevens heeft zijn o.a.: verhoren bij de rechter-commissaris, proces-verbaal onderzoek ter terechtzitting, (mededeling) uitspraak;
- Niet altijd is het nodig om persoonsgegevens te verstrekken. Soms kan ook worden volstaan met geanonimiseerde informatie. Verder dienen gegevens van andere personen dan betrokkenen geanonimiseerd te worden (artikel 39f, lid 2, Wjsg);

[23] Dit is een formele einduitspraak in het strafrecht waarmee wordt uitgedrukt dat het OM niet gerechtigd is om de zaak bij de strafrechter aanhangig te maken. De rechter beslist over de ontvankelijkheid van het OM. Gronden voor niet-ontvankelijkheid zijn onder andere de (grove) overschrijding van termijnen, de verjaring van het tenlastegelegde feit, het feit dat eerder een transactie is aangegaan voor hetzelfde feit, het feit dat een verdachte reeds vervolgd is voor het tenlastegelegde feit (schending van het beginsel van ne bis in idem) en de dood van de natuurlijke persoon dan wel de ontbinding van de rechtspersoon. Niet-ontvankelijkheid kan ook worden uitgesproken indien geconstateerd wordt dat ernstige fouten zijn gemaakt in het opsporings- en vervolgingstraject. In de praktijk blijkt dat de rechter veelal eerder beslist tot bewijsuitsluiting of strafvermindering.

- Verstrekking gebeurt alleen schriftelijk en moeten geprotocolleerd worden op grond van art. 32a Wjsg.

3.6.4 Belang van samenwerking in een samenwerkingsverband
De gegevensverstrekking aan het samenwerkingsverband moet noodzakelijk zijn vanwege een gemeenschappelijke doelstelling die verenigbaar is met de taken van het OM en waarbij er tevens sprake moet zijn van een zwaarwegend algemeen belang. Het moet voor het OM niet mogelijk zijn om de gemeenschappelijke doelstelling op een andere wijze te bereiken.

Het OM kan zaken bijvoorbeeld aandragen bij het Zorg- en Veiligheidshuis daar waar er sprake is van complexe meervoudige casuïstiek. Primair worden door het OM de meeste zaken echter behandeld op ZSM met de ketenpartners in het ZSM werkproces.

ZSM en de OM strafbeschikking
Een groot deel van de strafzaken die door de politie bij het OM worden aangebracht, verloopt via de ZSM werkwijze en wordt besproken op een van de 10 ZSM locaties in Nederland. Het overgrote deel van de personen die verdacht worden van een zogenaamd VVC misdrijf[24] worden aangemeld bij een ZSM locatie[25].

De ZSM werkwijze is een versnelde afhandeling van strafzaken door het OM in samenwerking met de ketenpartners. ZSM staat voor een werkwijze die “zo, selectief, snel, slim, simpel, samen en samenlevingsgericht” mogelijk” is. Binnen ZSM wordt samengewerkt door de strafrechtketenpartners: OM, Politie, Reclassering, Raad voor de Kinderbescherming, Slachtofferhulp Nederland en Bureau Halt. De verhouding van de ketenpartners binnen ZSM is anders dan de verhouding in andere samenwerkingsverbanden, in die zin dat het doel van het ZSM werkproces is om te komen tot een betekenisvolle afdoening waarbij de Officier van Justitie geïnformeerd wordt door de ZSM ketenpartners om tot een betekenisvolle afdoeningsbeslissing te komen. De Officier van Justitie voert de regie over het ZSM werkproces. Al tijdens de fase Intake & Selectie bepaalt de ZSM-officier of de zaak in aanmerking komt voor een directe behandeling op de ZSM-locatie, waarbij de bewijsbaarheid van de zaak, alsmede de nog benodigde activiteiten en onderzoek belangrijke criteria zijn. De Officier van Justitie kan ook besluiten dat de zaak wordt doorverwezen om elders te worden behandeld dan wel besluiten tot dagvaarding zodat de strafzaak bij de rechter zal moeten aangebracht. Op grond van artikel 257a van het Wetboek van Strafvordering (Wet OM afdoening) kan de officier van justitie ook, indien hij vaststelt dat een overtreding is begaan dan wel een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf is

[24] VVC: Veelvoorkomende criminaliteit

[25] Uitzondering op ZSM zijn in principe alleen de zaken waarbij het OM als gevolg van beleidsafspraken of van complexiteit van de zaak besluit tot toewijzing van de zaak aan een zaaksofficier van justitie. Ook voor ontboden verdachten geldt dat deze via ZSM afgehandeld worden. Aangemeld worden over het algemeen, minderjarige verdachten, verdachten van veelvoorkomende criminaliteit, huiselijk geweld. In principe worden niet via bij ZSM afgehandeld: alle zaken die in aanmerking komen voor een Team Grootschalig Opsporen (TGO)GO, alle zaken waar een zaaksofficier aan gekoppeld is, zeden misdrijven (m.u.v. schennis); mensenhandel, alle “kale” artikel 6, 8, 9 WVW zaken tenzij minderjarig, alle overtredingen.

gesteld van niet meer dan zes jaar, een strafbeschikking uitvaardigen (OM-strafbeschikking).

Hiermee kunnen o.a. de volgende straffen worden opgelegd:
- een geldboete;
- een taakstraf tot 180 uur (minderjarigen 60 uur);
- de verplichting tot betaling aan de staat van een geldbedrag ten behoeve van het slachtoffer.

Daarnaast kunnen door de Officier van justitie voorwaarden worden opgelegd, zoals deelname aan een afkickprogramma of een straatverbod of contactverbod en de maatregel van het onttrekken aan het verkeer van in beslag genomen voorwerpen. Op basis van de door het OM opgelegde strafbeschikking zullen organisaties als de Reclassering of de Jeugdreclassering zorgen voor de begeleiding. Zo kan de Officier van Justitie in de strafbeschikking de aanwijzing geven dat een jeugdige zich dient te houden aan de aanwijzingen van de jeugdreclassering. In deze situatie gaan reclassering of jeugdreclassering actie ondernemen zonder dat dit vooraf wordt afgestemd met de andere partijen die betrokken zijn bij de samenwerking rond die casus, of zonder dat deze partijen hierover worden geïnformeerd.

Gezien de wettelijke termijnen uit het Wetboek van strafvordering[26] moet er binnen ZSM snel worden beslist over de afdoening, daarnaast wil het OM snel handelen met het oog op het slachtoffer en de verdachte en vanuit efficiency en effectiviteit. De ZSM locaties zijn 7 dagen in de week gedurende 16 uur open.

Een betekenisvolle afdoening is een context- en persoonsgerichte (selectieve) en waar mogelijk snelle interventie, die betekenisvol is zowel voor de verdachte, als voor het slachtoffer en voor de samenleving. Een interventie kan zowel straf (vergelding) als zorgcomponenten hebben en daartoe wordt er ook gecheckt of er sprake is van recidive en/of er sprake is van zorgsignalen bij de strafrechtketenpartners (RvK, Reclassering). Er kan bijvoorbeeld sprake zijn van een (zeer actieve) veelpleger, of van een stelselmatige dader die reeds eerder in een Zorg- en Veiligheidshuis is besproken, en die in de laatste extramurale fase zit van een ISD-maatregel. Ook wordt ook nagegaan of de verdachte bekend is in het Zorg- en Veiligheidshuis of in een ander casusoverleg in het zorg- en veiligheidsdomein waaraan politie en/ of het OM deelnemen. Hierbij is steeds de vraag aan de orde of de gegevens die worden verwerkt door partijen in het zorgdomein daadwerkelijk mogen worden verstrekt aan de partijen in het strafrechtdomein.

Op de gecompliceerde zaken die niet voor versnelde afdoening in aanmerking komen wordt wel regie gevoerd. Zaken die leiden tot een voorgeleiding, gaan naar de backoffice.

De officier van Justitie kan ook besluiten om een zaak door te verwijzen naar een Zorg- en Veiligheidshuis of een ander samenwerkingsverband. Dan is er sprake van een

[26] Ophouden voor onderzoek: 6 uur dit kan ten hoogste eenmaal met 6 uur worden verlengd (de tijd tussen middernacht en negen uur 's morgens wordt niet meegerekend); inverzekeringstelling alleen voor strafbare feiten waarop de wet een gevangenisstraf van vier jaar of meer gesteld heeft en een aantal specifieke feiten omschreven in artikel 67 wetboek van strafvordering 72 uur (3 x 24 uur (dit kan ten hoogste eenmaal met 72 uur worden verlengd)). Na drie dagen en vijftien uur wordt de verdachte voor de rechter-commissaris geleid, die toetst of de inverzekeringstelling juridisch in orde is.

verstrekking van strafvorderlijke gegevens voor buiten de strafrechtpleging gelegen doeleinden.

3.7 Politie

3.7.1 Doelstelling en taken
De politieorganisatie is belast met de uitvoering van de politietaak als genoemd in artikel 3 Politiewet 2012: *'in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'*
De daadwerkelijke handhaving van de rechtsorde behelst het handhaven van de openbare orde onder het bevoegd gezag van de burgemeester alsmede de strafrechtelijke handhaving onder het bevoegd gezag van het Openbaar Ministerie.

Naast de politietaak kunnen ook andere taken van toepassing zijn op de werkzaamheden van de politie in het samenwerkingsverband. Bijvoorbeeld de zogenaamde Burgemeesterstaak. In de Algemeen Plaatselijke Verordening (APV) is de politie door de gemeenteraad aangewezen als toezichthouder voor specifieke taken. De grondslag voor de APV is de Gemeentewet.

3.7.2 Toepasselijke wet- en regelgeving
In relatie tot de samenwerkingsverbanden in het zorg- en veiligheidsdomein is voor de politie de volgende wet- en regelgeving van toepassing:
- de Politiewet 2012 (PW);
- het Wetboek van Strafrecht (Sr) en het Wetboek van Strafvordering (Sv);
- de Wet Politiegegevens (Wpg);
- het Besluit Politiegegevens (Bpg);
- de Algemene Verordening Gegevensbescherming (AVG).

3.7.3 Wettelijk kader gegevensverwerking en verstrekken van gegevens
Bij de verwerking van gegevens voor de uitoefening van de politietaak is er sprake van politiegegevens en is de Wpg van toepassing. Bij de verwerking van gegevens voor andere taken door de politie, zoals de Burgemeesterstaak, is er sprake van persoonsgegevens en is de AVG van toepassing.

De wettelijke grondslagen voor het verzamelen van gegevens betreft art. 3 Politiewet 2012 en voor wat betreft bijzondere opsporingsbevoegdheden het Wetboek van Strafvordering.

Verwerking van persoonsgegevens
De politie kan als dat nodig is meerdere soorten persoonsgegevens verzamelen, afhankelijk van het soort onderzoek en het doel, zoals personalia (naam, voornaam, adres, geboortedatum), telefoon en email, IP-adres en financiële gegevens

De politie heeft, voor de uitvoering van haar politietaak, daarnaast toegang tot de persoonsgegevens in een aantal van de basisregistraties. Dit zijn registraties van andere overheidsinstellingen met publiekrechtelijke taken, zoals:

- de Basisregistratie personen (Brp) van de Rijksdienst voor Identiteitsgegevens (RvIG)
- het Kentekenregister van de Rijksdienst voor het wegverkeer (Rdw)
- de Basisregistraties adressen en gebouwen (Bag) van het Kadaster
- het Handelsregister van de Kamer van Koophandel (KvK)

De politie mag, indien dit onvermijdelijk is voor het doel van de verwerking, in aanvulling op gewone persoonsgegevens de volgende bijzondere persoonsgegevens verzamelen: ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, lidmaatschap van een vakbond, genetische en biometrische gegeven, gezondheidsgegevens, seksuele leven en seksuele gerichtheid.

In de Wpg wordt de verwerking van politiegegevens geregeld voor verschillende doelen. Een aantal van die doelen heeft een relatie met de doelstellingen van samenwerkingsverbanden in het zorg- en veiligheidsdomein:

- artikel 8 regelt de verwerking van persoonsgegevens met het oog op de uitvoering van de dagelijkse politietaak (artikel 3 en 4 PW). Het gaat hierbij om handhaving van wetten en regels, hulpverlening, surveillance, verkeerszaken en eenvoudige opsporingsonderzoeken;
- artikel 9 regelt de verwerking ten behoeve van de handhaving van de rechtsorde in een bepaald geval, bijv. rechercheonderzoeken;
- artikel 10 regelt de verwerking met het oog op het inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde. Het gaat hier om het opbouwen van een informatiedossier over mensen, maar los van concrete handhavings- of opsporingsacties (TOOI, TCI e.d.);
- artikel 13 regelt de verwerking ten behoeve van de ondersteuning van de politietaak.

Politiegegevens die zijn verwerkt op basis van artikel 8, 9 of 10 kunnen ook voor andere doeleinden worden gebruikt. De wetgever heeft limitatief bepaald voor welke doelen de politie politiegegevens kan verwerken, bijv. om verdachten of betrokkenen te identificeren.

Verstrekking van politiegegevens

De Wpg is van toepassing voor de politie, de Koninklijke Marechaussee, de bijzondere opsporingsdiensten en voor Buitengewoon Opsporingsambtenaren (BOA's). Voor partijen die onder het regime van de Wpg vallen is het onderlinge motto: *'delen, tenzij…'*. Dat betekent dat op grond van artikel 15 politiegegevens ter beschikking moeten worden gesteld, tenzij in bijzondere gevallen en indien dit noodzakelijk is voor een goede uitvoering van de politietaak, de terbeschikkingstelling van politiegegevens wordt geweigerd ofwel beperkende voorwaarden worden gesteld stellen aan de verdere verwerking.

Alle andere partijen vallen buiten het regime van de Wpg. Hierbij is het motto: *'niet delen tenzij…'*. Dit betekent dat er in principe geen politiegegevens worden verstrekt, tenzij de wetgever dit expliciet mogelijk heeft gemaakt. De Wpg kent een gesloten verstrekkingenregime. Zo is er sprake van een geheimhoudingsbepaling (artikel 7 Wpg): iedereen aan wie politiegegevens worden verstrekt, is gehouden tot geheimhouding. Dit geldt niet alleen voor ontvangers die zijn belast met de verwerking van politiegegevens of die de gegevens direct van de politie hebben gekregen, maar ook voor eventuele tweede en volgende ontvangers, die de gegevens doorverstrekt hebben gekregen.

Artikel 20 Wpg
Op grond van artikel 20 Wpg kan de politie op lokaal niveau structureel in een samenwerkingsverband samenwerken met partijen die op zichzelf niet als ontvanger van politiegegevens in de Wpg zijn aangewezen, zowel met publiekrechtelijke als private partijen. Omdat de verstrekking van politiegegevens aan derden in het kader van een samenwerkingsverband alleen kan plaatsvinden indien het doel van de verstrekking overeenstemt of verenigbaar is met de politietaak, zijn nadere voorwaarden van toepassing: de politie kan, voor zover dit met het oog op een zwaarwegend algemeen belang noodzakelijk is voor een samenwerkingsverband van politie met personen of instanties, in overeenstemming met het bevoegd gezag, beslissen tot het verstrekken van politiegegevens aan die personen en instanties voor het voorkomen en opsporen van strafbare feiten, het handhaven van de openbare orde, het verlenen van hulp aan hen die deze behoeven of het uitoefenen van toezicht op het naleven van regelgeving.

Aan de verstrekking op grond van artikel 20 Wpg is de voorwaarde verbonden dat het bevoegd gezag instemming geeft en dat betekent dat zowel de burgemeester als het OM moeten instemmen met de structurele verstrekking van politiegegevens aan het samenwerkingsverband.

In de hiervoor bedoelde beslissing tot gegevensverstrekking wordt vastgelegd voor welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, voor welk samenwerkingsverband de politiegegevens worden verstrekt en het doel waartoe dit is opgericht, welke gegevens worden verstrekt, de voorwaarden waaronder de gegevens worden verstrekt en aan welke personen of instanties de gegevens worden verstrekt.

Uit de definitie zwaarwegend algemeen belang volgt dat dit belang een beperktere reikwijdte heeft dan het algemeen belang. Voorkomen moet worden dat deze gegevens al te makkelijk worden verstrekt. Een gegevensverwerking is vanuit het oogpunt van een zwaarwegend algemeen belang gerechtvaardigd indien de verwerking voor de samenleving van meer dan gewone betekenis is.

Toepassing van het criterium van het zwaarwegend algemeen belang impliceert een belangenafweging. Het belang dat gediend wordt met de verstrekking van de gegevens wordt afgewogen tegen het belang van de persoonlijke levenssfeer van degene op wie de politiegegevens betrekking hebben. Bij deze belangenafweging moeten ook de beginselen van proportionaliteit en subsidiariteit worden betrokken.

Om in ‘artikel 20-situaties’ (samenwerking van meerdere partijen/casusoverleg) politiegegevens te kunnen verstrekken, is verder de interne beleidslijn van de politie dat de relevante afspraken tussen de samenwerkende partijen worden vastgelegd in een convenant. Een convenant is voor de politie niet wettelijk verplicht, maar het is wel de beste manier om ervoor te zorgen dat de ontvangers die vallen onder de reikwijdte van de AVG voldoen aan hun wettelijke verplichtingen als gevolg van de AVG. Verder heeft ook het OM de interne beleidsregel dat er een convenant moet zijn opgesteld. Een Artikel 20-beslissing alleen is dus onvoldoende om te kunnen voldoen aan de privacywetgeving.

In het Besluit politiegegevens wordt vervolgens nader bepaald hoe moet worden gehandeld wanneer op grond van artikel 20 Wpg politiegegevens worden verstrekt. Op grond van artikel 4:5 eerste lid Bpg, kunnen er alleen artikel 8 en 13 politiegegevens worden verstrekt. Alleen indien dit strikt noodzakelijk is voor het doel van de verstrekking, kan de verantwoordelijke in afwijking van het huidige artikel 4:5 eerste lid Bpg beslissen tot verstrekking van politiegegevens die worden verwerkt overeenkomstig artikel 9 of artikel 10, eerste lid onder a en c Wpg. Hierbij moet worden gedacht aan situaties waarbij er sprake is van *‘ernstig gevaar voor de gezondheid of het leven van bepaalde personen.’*

Verder heeft de politie bij de verstrekking op grond van artikel 20 Wpg te maken met de documentatieplicht van artikel 6:4 lid 5 Bpg. Dit betekent dat de politie van elke verstrekking de volgende gegevens moet vastleggen: de identiteit van de verzoeker, de datum van de verstrekking, een omschrijving van de verstrekte gegevens en het het doel van de verstrekking.

Artikel 20 Wpg is een bepaling over de structurele verstrekking van politiegegevens aan samenwerkingsverbanden. Dit is een unieke bepaling. De Wpg is de enige wet waarin de wetgever een generieke uitzonderingsbepaling heeft opgenomen om ondanks een geheimhoudingplicht toch persoonsgegevens te kunnen verstrekken aan partijen in een samenwerkingsverband.

Geheimhouding
Wanneer de politiegegevens vervolgens worden doorgegeven aan een van de overige convenantpartners, is de Wpg niet meer van toepassing maar de AVG. De gegevens zijn dan binnen het samenwerkingsverband geen politiegegevens, maar persoonsgegevens c.q. strafrechtelijke persoonsgegevens (ex artikel 10 AVG). De ontvangers van de politiegegevens vallen overigens wel onder de eerder genoemde geheimhoudingsplicht van artikel 7 Wpg. Dat wil zeggen dat de geheimhoudingsverplichting nog steeds op de persoonsgegevens rust en de geheimhoudingsplicht als het ware “meeverhuist” naar de ontvanger. Dit betekent dat ontvangen politiegegevens door de ontvanger met bronvermelding dienen te worden verwerkt, om ze te kunnen onderscheiden van de overige verwerkte persoonsgegevens. Dit geldt voor de tweede en derde ontvanger. Dit betekent dat wanneer de eerste ontvanger de – inmiddels strafrechtelijke - persoonsgegevens wil door verstrekken, hij eerst moet bezien of er sprake is van een bij of krachtens de wet gegeven voorschrift dat tot verstrekking verplicht (artikel 7 lid 2 Wpg) of zijn taak daartoe noodzaakt (artikel 7 lid 2 Wpg).

Ten aanzien van persoonsgegevens die oorspronkelijk als politiegegevens zijn verstrekt, is de geheimhoudingsplicht van artikel 7 Wpg van toepassing op de ontvangers in het samenwerkingsverband. Derhalve worden verzoeken om inzage, correctie en verwijdering beoordeeld in samenspraak met de politie. De politie heeft het recht om een verzoek geheel of gedeeltelijk af te wijzen op grond van de criteria zoals genoemd in artikel 27 Wpg of artikel 41 UAVG.

3.7.4 Belang van samenwerking in een samenwerkingsverband
De gegevensverstrekking aan een samenwerkingsverband kan noodzakelijk zijn vanwege een gemeenschappelijke doelstelling die verenigbaar is met de politietaak, en er is sprake van een zwaarwegend algemeen belang, waarbij het voor de politie niet mogelijk is om op een andere wijze deze doelstelling te bereiken. Het gaat daarbij om het uitwisselen van informatie en inzichtelijk maken van problemen en risico's die ten grondslag liggen aan multidisciplinaire complexe casussen op basis van de door de politie aangeleverde gegevens. Het snel en adequaat handelen bij het in samenhang organiseren van de nodige zorg en ondersteuning voor zowel dader alsook slachtoffer(s) is verenigbaar met de politietaak.

3.8 Raad voor de Kinderbescherming (RvdK)

3.8.1 Doelstelling en taken
Rechten van kinderen, zoals deze in diverse wetten en mensenrechtenverdragen, waaronder het Internationaal Verdrag inzake de Rechten van het Kind (IVRK) zijn vastgelegd, dienen door de overheid gewaarborgd te worden. Kinderen hebben, gelet op het IVRK, recht op een gezonde en evenwichtige ontwikkeling en uitgroei naar zelfstandigheid.

Beschermingstaken
- De RvdK onderzoekt de situatie van het kind en zijn gezinsomgeving en vraagt zo nodig aan de rechter om een (voorlopige) kinderbeschermingsmaatregel uit te spreken (art 1:255, 1:260, 1:265b, 1:265c, 1:267, 1:268 BW);
- De RvdK doet, bij (vermoedens van) het ontbreken van het gezag over een kind, onderzoek naar de wijze waarop in het gezag moet worden voorzien en doet hiertoe een verzoek of geeft advies aan de rechter (art.1: 241, art 1:253ha BW);
- De RvdK toetst de voorgenomen beslissingen van de Gecertificeerde Instelling met betrekking tot de niet verlenging van een ondertoezichtstelling en de niet verlenging dan wel tussentijdse beëindiging van een uithuisplaatsing van een kind. Hierbij beoordeelt de RvdK of de gronden voor de ondertoezichtstelling en/of uithuisplaatsing wel of niet (nog) aanwezig zijn. Daarnaast heeft de RvdK een adviserende taak indien een Gecertificeerde Instelling na een ondertoezichtstelling met machtiging uithuisplaatsing van 2 jaar of langer om een verlenging daarvan verzoekt. Hier is de vraag of het in het belang van het kind is de huidige maatregelen te continueren, te beëindigen of dat een gezag beëindigende maatregel moet worden overwogen.(art. 265j lid 1)

Adviestaak Gezag en Omgang na scheiding
Op verzoek van de rechter doet de RvdK onderzoek en brengt de RvdK, ook ter zitting, advies uit aan de rechter over beslissingen rond gezag, verdeling van zorg- en opvoedtaken,
de hoofdverblijfplaats van de kinderen, informatie- en consultatieplicht van de verzorgende
ouder naar de andere ouder, omgang met ouder zonder gezag en omgang met derden. (art. 810 Rv)

Afstand, Screening, Adoptie en Afstammingsvragen (ASAA)-taken
- De RvdK doet een screeningsonderzoek naar aspirant-adoptiefouders in verband met hun wens om een (buitenlands) kind op te nemen;
- De RvdK doet een justitiële screening naar aspirant pleegouders in verband met (een voornemen tot) de opneming van een pleegkind (art. 5.1 lid 1 sub d JW);
- De RvdK doet onderzoek indien een ouder afstand wil doen van een kind;
- De RvdK beslist op verzoeken om inzage in dossiers en afgifte van stukken bij afstammingsvragen;
- De RvdK doet onderzoek bij vermoedens van illegale opneming van een kind;
- De RvdK doet onderzoek ingeval van afstand van een kind na draagmoederschap;
- Op verzoek van de rechter doet de RvdK onderzoek naar en adviseert de rechter over een voorgenomen (Nederlandse) adoptie;
- De RvdK doet onderzoek naar uitvoering van verplichtingen uit internationale verdragen ten behoeve van kinderen/jongeren.

Straftaken
- De RvdK stelt een onderzoek in naar aanleiding van een melding van de politie over het plegen van een strafbaar feit of een melding van de leerplichtambtenaar van schoolverzuim. De RvdK doet onderzoek naar de situatie van het kind en geeft een advies aan de officier van justitie en de rechter over de pedagogisch meest wenselijke straf op basis van de ontwikkeling en omstandigheden van dit kind;
- De RvdK coördineert de tenuitvoerlegging van de taakstraf van een kind;
- De RvdK voert de (casus)regie met betrekking tot de instanties die betrokken zijn bij de afhandeling van de strafzaak van een kind. In geval van detentie wordt onder voorzitterschap van de RvdK hiervoor het netwerk- en trajectberaad ingezet;
- De RvdK doet Persoonlijkheidsonderzoek (PO) in het kader van de advisering van een gedragsbeïnvloedende maatregel (GBM).

3.8.2 Toepasselijke regelgeving
Op nationaal niveau vloeien de wettelijke taken van de Raad voort uit boek 1 van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht, het Wetboek van Strafvordering, de Algemene Wet Bestuursrecht, de Jeugdwet en de Wet Opneming Buitenlandse Kinderen ter Adoptie (wobka).

Voorts geldt het Kwaliteitskader 2016 van de Raad voor de Kinderbescherming en artikel J van de Beroepscode van de Jeugdzorgwerker alsmede art. 71 t/m 87 van de

beroepscode voor de psycholoog (beroepscode NIP) en art. 11 van de beroepscode voor de pedagoog (beroepscode NVO).

3.8.3 Wettelijk kader gegevensverwerking en verstrekken van gegevens
De RvdK kan zich bij het verwerken van persoonsgegevens beroepen op de volgende grondslagen:
- De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden (art. 6 lid 1 sub a AVG)
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (art. 6 lid 1 sub c AVG)
- 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 (art. 6 lid 1 sub e AVG);

3.8.4 Belang van samenwerking in een samenwerkingsverband
De gegevensverwerking is noodzakelijk vanwege een gemeenschappelijke doelstelling die verenigbaar is met de taken van de RvdK, er is sprake van een zwaarwegend algemeen belang waarbij het voor de RvdK niet mogelijk is om op een andere manier deze doelstelling te bereiken. Het gaat daarbij om het uitwisselen van informatie en inzichtelijk maken van risico's voor de veiligheid van de minderjarige binnen het kader van complexe gezinsproblematiek op basis van mede door de RvdK aangeleverde gegevens. Het snel en adequaat handelen wordt mede hierdoor mogelijk gemaakt en draagt bij aan de doelstelling van de RvdK.

3.9 Reclassering
Er zijn drie reclasseringsorganisaties
- Stichting Reclassering Nederland (RN);
- Stichting Verslavingsreclassering GGZ (SVG). De SVG is de koepelorganisatie van tien zelfstandige regionale verslavingsreclasseringsinstellingen;
- Stichting Leger des Heils, Jeugdbescherming en Reclassering.

De drie reclasseringsorganisaties vormen een samenwerkingsverband: de 3RO.

3.9.1 Doelstelling en taken
De reclasseringsinstellingen (hierna te noemen: de reclassering) zijn onafhankelijke organisaties. Zij dragen bij aan een veiliger samenleving door het voorkomen en verminderen van crimineel gedrag. Officieren van justitie, rechters, gevangenisdirecties en gemeenten schakelen de reclassering in. Ze adviseert over de aanpak van verdachten en veroordeelden. Ze houdt toezicht, traint, voert taakstraffen uit, indiceert en leidt toe naar zorg, en begeleidt de terugkeer in de maatschappij. Het strafrecht is haar werkterrein, met als specialiteit het voorkomen van terugval in de misdaad. Haar werk concentreert zich op het veranderen van gedrag.

De wettelijke reclasseringstaken zijn:
- het doen van onderzoek naar en het geven van voorlichting en advies over personen die worden verdacht van of zijn veroordeeld wegens een strafbaar feit,

ten behoeve van te nemen beslissingen inzake de vervolging, de afdoening, de berechting of de tenuitvoerlegging van straffen of maatregelen;
- vroeghulp van een verdachte die in verzekering is gesteld op een politiebureau of huis van bewaring;
- het houden van toezicht op de naleving van aan verdachten of veroordeelden bij of krachtens de wet opgelegde voorwaarden of ontzetting van rechten en hen ten behoeve daarvan te begeleiden;
- het voorbereiden en begeleiden van en het houden van toezicht op de uitvoering van de taakstraf;
- het opstellen van een indicatiestellingsadvies als bedoeld in de Wet Forensische zorg;
- zorgtoeleiding namens Onze Minister, bedoeld in de Wet Forensische zorg.

Naast de wettelijke taken begeleidt de reclassering ook personen op vrijwillige basis met als doel het veranderen van crimineel gedrag zoals vrijwillige nazorg van ex-gedetineerden.

3.9.2 Toepasselijke wet- en regelgeving
Wetboek van Strafvordering:
- 59 lid 5, 63 lid 6 (vroeghulp en vroeghulpadvies);
- 147, 177 en 310 (adviesopdracht voor rechtszitting door resp. de OvJ, de RC en de rechter);
- 509o lid 3 (advies verlenging maatregel tbs);
- 80 (toezicht bij schorsing voorlopige hechtenis);
- 167 lid 2 (toezicht bij voorwaardelijk sepot)

Wetboek van Strafrecht:
- 15a lid 6 (advisering bij voorwaardelijke invrijheidsstelling);
- 38z (advies inzake gedrags-beïnvloedende en vrijheidsbeperkende maatregel (GVM));
- 14d lid 2 (toezicht bij voorwaardelijke veroordeling);
- 15b lid 2 (toezicht bij voorwaardelijke invrijheidsstelling);
- 32 (toezicht bij ontzetting uit ambt of beroep);
- 38 lid 1 (toezicht bij tbs met voorwaarden);
- 38g lid 2 (toezicht bij voorwaardelijke beëindiging tbs);
- 38p (toezicht bij voorwaardelijke ISD-maatregel)
- 38ad (toezicht bij gedragsbeïnvloedende en vrijheidsbeperkende maatregel (GVM)),
- 22e tot en met 22k (taakstraffen);
- 16 (grondslag voor Amvb reclasseringstoezicht).

Gratiewet
- Artikel 15 lid 1 (toezicht bij gratie onder voorwaarden).

Penitentiaire Beginselenwet
- artikel 4 (elektronisch toezicht bij een penitentiair programma);
- artikel 43 lid 3 (toezicht bij plaatsing in een zorginstelling of verslavingskliniek).

Penitentiaire Maatregel

- artikel 7 lid 2 (advies in opdracht van de directeur P.I. voor een penitentiair programma);
- artikel 4 en artikel 7a (elektronisch toezicht bij een penitentiair programma).

Wet forensische zorg en het Besluit forensische zorg[27]

Uitvoeringsbesluit voorwaardelijke veroordeling;
Uitvoeringsbesluit voorwaardelijke invrijheidstelling;
Reglement verpleging ter beschikking gestelden.
Besluit ten uitvoerlegging taakstraffen.
Wet justitiële en strafvorderlijke gegevens en Besluit Justitiële en strafvorderlijke gegevens

Reclasseringsregeling 1995

- Artikel 8 (opsomming wettelijke reclasseringstaken);
- Artikel 37 (geheimhoudingsverplichting reclasseringsmedewerkers).

Uitvoeringsregeling reclassering 2005

Privacyreglement
De reclasseringsorganisaties hebben de wettelijke regelingen over het omgaan met persoonsgegevens verwerkt in een privacyreglement. Iedere RO heeft een eigen privacyreglement. De inhoud daarvan is voor de 3RO nagenoeg hetzelfde.

3.9.3 Wettelijk kader gegevensverwerking en verstrekken van persoonsgegevens

Verwerking van persoonsgegevens
Gegevensverwerkingen zijn alleen rechtmatig indien er een grondslag uit artikel 6 AVG aanwezig is. Voor de uitvoering van de wettelijke reclasseringstaken is die grondslag gelegen in:

- artikel 6 lid 1 sub c AVG: "*een wettelijke verplichting*";
- artikel 6 lid 1 sub e AVG: "*een taak van algemeen belang*".

Bijzondere en strafrechtelijke persoonsgegevens
Op grond van de AVG zijn verwerkingen van bijzondere categorieën van persoonsgegevens en de verwerking van strafrechtelijke persoonsgegevens in beginsel verboden tenzij een wettelijke uitzondering van toepassing is (artikel 9 en 10 AVG juncto de artikelen 22 tot en met 33 UAVG). Voor de uitvoering van haar taken verwerkt de reclassering onder meer strafrechtelijke persoonsgegevens en gezondheidsgegevens. Soms ook gegevens omtrent ras/ etnische afkomst, religieuze/levensbeschouwelijke overtuigingen, biometrische gegevens en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Dit betekent dat er voor een rechtmatige verwerking van

[27] Zie voor meer informatie over gegevensverwerking in het kader van de Wvggz, Wzd en Wfz het addendum bij dit Handvat.

persoonsgegevens door de reclassering behalve een rechtmatige grondslag, ook steeds een wettelijke uitzondering op bovengenoemde verboden aangewezen moet kunnen worden. Voor de uitvoering van de reclasseringstaken zijn met name de volgende artikelen uit de UAVG relevant:

- Artikel 33 lid 1 UAVG: op grond van dit artikel mogen strafrechtelijke gegevens worden verwerkt door "*organen die krachtens de wet zijn belast met de toepassing van het strafrec*ht".
  De reclassering is krachtens haar wettelijke taken aan te merken als een orgaan dat krachtens de wet is belast met de toepassing van het strafrecht en valt derhalve onder de uitzondering van het verbod op het verwerken van strafrechtelijke gegevens;
- Artikel 30 lid 2 sub b UAVG inzake het verwerken van gezondheidsgegevens door reclasseringsinstellingen: reclasseringsinstellingen mogen op grond van deze bepaling gezondheidsgegevens verwerken, voor zover dat noodzakelijk is voor de uitvoering van de hun wettelijk opgedragen taken;
- Artikel 23 sub c UAVG: op grond van dit artikel mogen overige bijzondere persoonsgegevens worden verwerkt indien dat noodzakelijk is in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt;
- Artikel 22 lid 1 sub a en artikel 32 sub a UAVG: op grond van deze artikelen mogen bijzondere en strafrechtelijke persoonsgegevens worden verwerkt indien de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden.

Verstrekking van persoonsgegevens
De reclassering kan persoonsgegevens van haar cliënten verstrekken in de volgende situaties:
- Er is sprake van een wettelijke plicht tot gegevensverstrekking;
- Voor de uitvoering van een wettelijke reclasseringstaak aan een bevoegde instantie;
- Wanneer de belangen van anderen of de samenleving met ernstige schade worden bedreigd, een situatie van "overmacht", m.n. bij levensdelicten (artikel 6 lid sub d AVG);
- Bij een redelijke vermoeden van kindermishandeling of huiselijk geweld aan een Veilig Thuis na het doorlopen van de meldcode (artikel 5.2.6 WMO 2015);
- Wanneer dit noodzakelijk is voor de uitvoering van de taken van de RvdK (artikel 1:240 BW);
- Als de cliënt in vrijheid zijn schriftelijke toestemming voor gegevensverstrekking heeft gegeven, waarbij expliciet is aangegeven aan welke instantie of professional de gegevens mogen worden verstrekt, voor welk doel en welke gegevens.

Ad 1.
Een wettelijke plicht om gegevens te verstrekken doet zich voor in de volgende situaties:

- Als het OM of de rechter een adviesopdracht geeft voor een beslissing over de vervolging, berechting of tenuitvoerlegging van straffen of maatregelen zoals op grond van artikel 147 Wetboek van Strafvordering.
- Melding van de overtreding van de algemene of bijzondere voorwaarde bij een toezicht aan het OM o.a. op grond van artikel 14d lid 2 Wetboek van Strafrecht;
- Bij een vordering verstrekking gegevens van het OM op grond van artikel 126nd Wetboek van Strafvordering in het kader van een opsporingsonderzoek;
- Aan een gezinsvoogd, als die erom vraagt wanneer een minderjarige onder toezicht is gesteld (de civiele maatregel OTS: artikel 7.3.11 lid 4 Jw).

Ad 2.
De wettelijke taken staan hierboven vermeld. Onder bevoegde instanties worden de volgende instanties bedoeld waaraan voor de uitvoering van een wettelijke reclasseringstaak gegevens kunnen worden verstrekt:

- Justitiële organisaties zoals OM, rechterlijke macht, politie, DJI, NIFP, de jeugdreclassering, RvdK en andere erkende reclasseringsorganisaties;
- Zorg- en hulpverleners - GGD en hulpverleners in sociale wijkteams inbegrepen - voor zover zij deze gegevens nodig hebben voor een goede zorgverlening van betrokkene;
- Burgemeester of gemachtigde gemeenteambtenaar voor zover sprake is van een specifieke wettelijk geregelde taak op het gebied van de handhaving van de openbare orde en veiligheid, die verwerking van strafrechtelijke gegevens noodzakelijk maakt. Bijvoorbeeld als de burgemeester bij een persoon die voor overlast zorgt, overweegt om een bestuurlijk gebiedsverbod op te leggen. Het kan dan nodig zijn om het gebiedsverbod op het toezichtplan af te stemmen en daarvoor enige gegevens te verstrekken, maar dat betekent niet dat adviesrapportages of NIFP rapporten met de burgemeester/de gemeenteambtenaar mogen worden gedeeld.

Op grond van artikel 9 Wjsg juncto artikel 17 Bjsg is Minister van Justitie en Veiligheid bevoegd om aan de Reclassering justitiële gegevens te verstrekken voor de uitvoering van haar (wettelijke) taken. Op grond van artikel 42 lid 4 Wjsg is de Minister van JenV bevoegd om afschriften van NIFP-rapporten te verstrekken "*ten behoeve van het voorbereiden van enig rapport of het uitoefenen van enig toezich*t". Als deze gegevens worden verstrekt aan de Reclassering vallen ze onder het regime van de AVG en worden het vervolgens strafrechtelijke persoonsgegevens. De grondslag voor verwerking is gelegen in de eerder opgesomde wettelijke taken en grondslagen voor gegevensverwerking van de Reclassering. De geheimhoudingsplicht van artikel 52 Wjsg blijft echter rusten op de gegevens en verplicht de reclassering tot geheimhouding *"behoudens voor zover een bij of krachtens deze wet gegeven voorschrift mededelingen toelaat, dan wel de uitvoering van de taak met het oog waarop de gegevens zijn verstrekt tot het ter kennis brengen daarvan noodzaakt".* Dat laatste is alleen aan de orde in uitzonderingsgevallen.

Geheimhoudingsplicht en beroepsgeheim
In artikel 37 Reclasseringsregeling 1995 is geregeld dat voor álle reclasseringsmedewerkers een geheimhoudingsplicht geldt. Deze geheimhoudingsplicht is

niet absoluut. Er zijn gevallen denkbaar waarin de geheimhoudingsplicht doorbroken dient te worden. Zie verder hoofdstuk 2.7 over het beroepsgeheim.

Ook is voor reclasseringswerkers in de rechtspraak bepaald dat zij op grond van de aard van hun functie in beginsel een geheimhoudingsplicht en het daaraan gekoppelde verschoningsrecht hebben. Zie het arrest van de Hoge Raad uit 1968 (HR 20 juni 1968, NJ 1968, 332).

3.9.4 Belang van samenwerking in een samenwerkingsverband
Zowel de reclassering als de samenwerkingsverbanden in het zorg- en veiligheidsdomein streven naar een veiliger samenleving, minder crimineel gedrag en het voorkomen van recidive.

Een goede voorbereiding op een bestaan zonder criminaliteit, dat is het doel van de reclassering. Om alle taken goed uit te kunnen voeren, worden goede contacten onderhouden met de partners in de zorg- en strafrechtketen. Zoals gemeenten, politie, justitie, Veilig Thuis, gevangeniswezen en forensische zorg.
De reclassering is als enige organisatie vanaf het moment van aanhouding tot en met zijn terugkeer in de maatschappij betrokken bij een dader of verdachte. De reclassering voert het toezicht uit en ziet toe op de naleving van de bijzondere voorwaarden. Elke veroordeelde krijgt dus een eigen aanpak van toezicht - toezicht houden is maatwerk. De intensiteit van het toezicht is afhankelijk van de kans op recidive, het gedrag en de motivatie van de dader.
De reclassering controleert of de veroordeelde zich aan de bijzondere voorwaarden en gemaakte afspraken houdt. De reclassering motiveert de verdachte of dader om te leven zonder criminaliteit. De reclassering ondersteunt hem of haar bijvoorbeeld bij een zinvolle dagbesteding, huisvesting en het oplossen van schulden. Daarvoor wordt samengewerkt met onze partners in het sociaal domein zoals de gemeente of GGZ.

Daarnaast zijn specifieke aanpakken ontwikkeld voor jongvolwassenen of adolescenten in of op het randje van de criminaliteit en voor terrorismeverdachten en mensen die geradicaliseerd zijn. Ook de aanpak van huiselijk geweld en kindermishandeling staat hoog op de agenda.

3.10 Slachtofferhulp

3.10.1 Doelstelling en taken
Stichting Slachtofferhulp Nederland (hierna: SHN) biedt praktische hulp, juridisch advies en emotionele steun aan:
- slachtoffers (waartoe ook nabestaanden en familie worden gerekend) van strafbare feiten;
- slachtoffers van niet strafbare feiten als verkeersongelukken, calamiteiten en vermissingen of veroorzakers van verkeersongelukken (niet zijnde misdrijven);
- getuigen van (strafbare) feiten zoals bijvoorbeeld suïcide en bekenden van slachtoffers van (strafbare) feiten.

SHN werkt met betaalde en onbetaalde medewerkers. Het doel is het slachtoffer te ondersteunen bij het verwerken van de gebeurtenis en het, waar mogelijk, herstellen dan wel verlichten van de materiële en immateriële schade. De zelfredzaamheid en weerbaarheid van het slachtoffer zijn daarbij het uitgangspunt. Daarnaast spant SHN zich in voor de verbetering van de positie van slachtoffers in het algemeen en stimuleert zij de kennisontwikkeling op dit gebied.
SHN richt zich in dit handvat tot de slachtoffers (waartoe ook nabestaanden en familie worden gerekend) van strafbare feiten, waarbij geldt dat van een strafbaar feit sprake is wanneer het betreffende feit strafbaar is gesteld op grond van de wet[28].

SHN verzamelt en verwerkt persoonsgegevens ten behoeve van de volgende doelstelling: de hulpverlening en dienstverlening aan slachtoffers van strafbare feiten.
De taken bestaan uit het bieden van:

- advies over financiële en praktische kwesties naar aanleiding van het strafbare feit;
- informatie over of rechtstreekse doorverwijzing naar relevante bestaande gespecialiseerde hulporganisaties;
- emotionele ondersteuning;
- juridisch informatie, advies en ondersteuning die relevant is voor de rechten van het slachtoffer van strafbare feiten, onder meer inzake toegang tot procedures voor vergoeding van schade zoals het schade verhalen via het (straf)proces, maar ook het spreekrecht, schriftelijke slachtofferverklaring en over de rol van het slachtoffer in het strafproces onder meer ter voorbereiding op het bijwonen van de terechtzitting;
- advies aan slachtoffers van strafbare feiten over het risico en het voorkomen van secundaire en herhaalde victimisatie, van intimidatie en van vergelding, tenzij anderszins verstrekt door andere openbare of particuliere organisaties.

SHN verwerkt gegevens over de fysieke, sociale en maatschappelijke gevolgen van slachtoffers van strafbare feiten, gegevens over de ondersteuning van het slachtoffer, de financiële gevolgen voor het slachtoffer en de wensen van het slachtoffer. Naast “gewone” persoonsgegevens betreft dit ook bijzondere en strafrechtelijke gegevens van een kwetsbare groep.
SHN hecht uiteraard veel waarde aan de privacy van slachtoffers en, daar nauw mee verbonden, de bescherming van hun persoonsgegevens. De bescherming van persoonsgegevens is voor SHN zowel een kwestie van integriteit als van kwaliteit. Misbruik maken van bevoegdheden, meer persoonsgegevens verwerken dan nodig of onzorgvuldig omgaan met persoonlijke gegevens schaadt de vertrouwensrelatie tussen SHN en daarmee de integriteit en reputatie van SHN als maatschappelijke dienstverlener.

3.10.2 Toepasselijke regelgeving

- artikelen 6 en 7 Wjs;
- artikel 1 Regeling Aanwijzing Slachtofferhulp;
- artikel 51aa Sv;
- artikel 3 Besluit slachtoffers van strafbare feiten

[28] artikel 1 WvSr

3.10.3 Wettelijk kader gegevensverwerking en verstrekken van persoonsgegevens

De verwerking van persoonsgegevens van slachtoffers van strafbare feiten door SHN kan worden gebaseerd op de grondslag dat deze verwerking noodzakelijk is voor de vervulling van een taak in algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (art. 6 lid 1 onder e AVG).

Voor het verstrekken van persoonsgegevens aan de Veiligheidshuizen zal echter toestemming aan het slachtoffer worden gevraagd.

In de art. 6 en 7 Wjs is bepaald wat onder slachtofferhulp moet worden verstaan en dat de Minister van Justitie en Veiligheid een rechtspersoon aanwijst die belast is met de taken die onder slachtofferhulp moeten worden verstaan. Onder slachtofferhulp wordt verstaan:

- De opvang en ondersteuning van slachtoffers en nabestaanden van vermoedelijke strafbare feiten, bestaande uit:
  1°. juridische ondersteuning;
  2°. praktische ondersteuning;
  3°. kortdurende emotionele ondersteuning;
  4°. doorverwijzing naar niet in het bijzonder voor slachtoffers bedoelde hulpverleningsinstellingen.
- Activiteiten ter verbetering van de positie van het slachtoffer."

In de parlementaire geschiedenis bij de Wjs is het volgende opgenomen:

- "*Vanuit het oogpunt van borging van het publiek belang is betrokkenheid van de Minister van Justitie, bij de Stichting Slachtofferhulp Nederland gewenst."*[29]
- *"Deze subsidie-relatie tussen het Ministerie van Justitie en Slachtofferhulp Nederland heeft slechts betrekking op slachtoffers van strafbare feiten, waaronder ook de verkeersmisdrijven."*[30]

In art. 1 van de Regeling Aanwijzing Slachtofferhulp wordt SHN aangewezen als rechtspersoon die is belast met de uitvoering van de taken behorend bij slachtofferhulp. Met name art. 3 van het Besluit slachtoffers van strafbare feiten is van belang in verband met de taakstelling van SHN.

Bijzondere en strafrechtelijke persoonsgegevens

SHN mag 'bijzondere persoonsgegevens' (gezondheidsgegevens en strafrechtelijke gegevens) op basis van de volgende grondslagen verwerken:

Gezondheidsgegevens

- artikel 30 lid 3 sub a UAVG;
- artikel 23 onder c UAVG.

Strafrechtelijke gegevens:

---

29 *Kamerstukken II*, 2007-08, 31 257, nr. 3, p. 2 en 3.

30 *Kamerstukken II*, 2007-08, 31 257, nr. 3, p. 3

- artikel 33 lid 1 sub a UAVG;
- artikel 33 lid 1 sub c UAVG.

Toelichting artikel 33 lid sub a UAV: op grond van 39f lid 1 van de Wjsg en de aanwijzing Wet Justitiële en Strafvorderlijke gegevens III 3f.1 II mag SHN gegevens ontvangen van het OM omdat zij deel uitmaakt van de strafrechtketen. Op basis van art. 39f lid 1 Wjsg kunnen voor de aldaar genoemde doelen in ieder geval aan de volgende personen en instanties strafvorderlijke gegevens worden verstrekt.

Daarnaast kunnen op grond van artikel 18 Wpg bij of krachtens algemene maatregel van bestuur personen en instanties worden aangewezen aan wie of waaraan, met het oog op een zwaarwegend algemeen belang, politiegegevens worden verstrekt ter uitvoering van de bij of krachtens die algemene maatregel van bestuur aan te geven taak.

Op grond van artikel 4.2 1b. Besluit Politiegegevens kunnen politiegegevens voor zover zij deze behoeven voor een goede uitvoering van hun taak worden verstrekt aan SHN ten behoeve van het behartigen van belangen van slachtoffers van strafbare feiten of verkeersongevallen.

Verstrekking van persoonsgegevens

De samenwerking van de betrokken partijen in een samenwerkingsverband in het zorg- en veiligheidsdomein is gericht op een ketenoverstijgende aanpak van complexe problematiek rond personen en/of gezinnen teneinde een bijdrage te leveren aan het verminderen van recidive, (ernstige) overlast, criminaliteit en maatschappelijke uitval door een combinatie van repressie bestuurlijke interventie en zorg. Hierbij ligt de focus niet alleen op bestaande overtreders van de wet, maar ook op individuen of groepen met een groot risico op afglijden richting crimineel en ernstig overlastgevend gedrag. De samenwerking is onder meer gericht op (i) casusoverleggen waarin de betrokken partijen complexe casuïstiek bespreken en plannen van aanpak opstellen en (ii) het (strategisch) adviseren van lokale bestuurders en sleutelpartners over lokale gebiedsgebonden problematiek c.q. het vervullen van een adviserende en beleidsondersteunende rol.
Dit doel stemt niet overeen met de hierboven wettelijk omschreven werkzaamheden van SHN in het kader van slachtofferhulpverlening. De verwerking en verstrekking van persoonsgegevens door SHN aan betrokkenen bij samenwerkingsverband zal dan ook niet kunnen worden gebaseerd op haar taak in het algemeen belang zoals hiervoor omschreven. SHN zal voor de verwerking en verstrekking van persoonsgegevens in het kader van een samenwerkingsverband de uitdrukkelijke toestemming als bedoeld in art. 6 lid 1 onder a AVG moeten vragen aan betrokkenen. Voorts dient deze toestemming aantoonbaar te zijn.

3.10.4 Belang van samenwerking in een samenwerkingsverband

SHN heeft een beperkt aantal convenanten ondertekend en is geen sleutelpartner bij bijvoorbeeld de Veiligheidshuizen. SHN zal alleen aanschuiven bij casusoverleg in een samenwerkingsverband indien de betreffende casus daartoe aanleiding geeft. Het kan echter van belang zijn om de belangen van het slachtoffer, zoals een straat of contactverbod onder de aandacht te brengen en wellicht algemene ervaringsgegevens van SHN met een bepaalde soort casus te delen.

3.11 Stichting Halt

3.11.1 Doelstelling en taken

Stichting Halt voert op grond van art. 77e van het WvSr, art. 48g van de Wet Justitiesubsidies en de Regeling Halt 2019 - onder meer - de volgende Halt-werkzaamheden uit:

- Landelijke coördinatie en uitvoering van Halt-afdoeningen;
- In het kader van afdoeningstrajecten voor jeugdigen, de advisering door Halt aan de ketenpartners in de strafrechtketen omtrent een (eventuele) Halt-afdoening;
- Het verrichten van nazorg waardoor een warme overdracht van de jeugdige plaatsvindt naar het lokale veld en/of de jeugdstrafrechtketen.

Naast deze justitiële/wettelijke opgave voert Halt ook werkzaamheden uit in opdracht van lokale partners en/of andere opdrachtgevers. Hieronder vallen:

1. gedragsinterventies op grond van het Tuchtrecht van de KNVB;
2. gedragsinterventies (in opdracht van gemeenten en scholen);
3. voorlichtingen op primair- en voortgezet onderwijs, voor zowel gewoon als speciaal onderwijs;
4. ouderbijeenkomsten;
5. advies- en netwerkuren.

3.11.2 Toepasselijke wet- en regelgeving

- Wetboek van Strafrecht (art 77e);
- Wet justitiesubsidies (art. 48g);
- Regeling Halt 2019;
- Besluit aanwijzing Halt-feiten;
- OM-Richtlijn en kader voor strafvordering jeugd en adolescenten, inclusief strafmaten Halt (1 juni 2018);
- Beroepscode voor de jeugdzorgwerker (art. J.);
- Methodische aanpak schoolverzuim (MAS);
- Sportakkoord 2018;
- Diverse lokale convenanten en samenwerkingsafspraken met verwijzers/ gemeenten.

3.11.3 Wettelijk kader gegevensverwerking en verstrekking van persoonsgegevens

Verwerking van persoonsgegevens

Halt mag persoonsgegevens verwerken op basis van de navolgende grondslagen :

- een wettelijke verplichting (art. 6 AVG, lid 1 sub c);
- een taak van algemeen belang (art. 6 AVG, lid 1 sub e).

Bijzondere en strafrechtelijke persoonsgegevens

Halt mag bijzondere en strafrechtelijke gegevens verwerken op basis van:

- Wetboek van Strafrecht art. 77 e;
- Regeling Halt 2019;
- Art. 6 lid 1 sub c AVG;
- Art. 6 lid 1 sub e AVG;

- Art. 9 lid 2 sub h jo. art. 30 lid 3 sub a UAVG;
- Art. 9 lid 2 sub a AVG;
- Art. 10 AVG jo. art. 33 lid 1 sub a UAVG;
- Art. 10 AVG jo. art. 33 lid 1 sub b UAVG.

Op grond van artikel 5 lid 1 van de Regeling Halt 2019 is een Halt-bureau desgevraagd verplicht om informatie over de werkzaamheden aan de Minister te verstrekken. Ook kan de Minister op grond van artikel 5 lid 2 inzage vorderen van andere gegevens en bescheiden voor zover dat voor de uitoefening van zijn taak redelijkerwijs nodig is. Indien de Minister dergelijke inzage vordert zal Halt hieraan moeten voldoen.

Geheimhoudingsplicht en beroepsgeheim
Een Halt-medewerker heeft geen beroepsgeheim/verschoningsrecht. Voor de gegevens die Halt van de politie en/of OM krijgt over cliënten bestaat o.g.v. art. 7 WPG en art. 52 Wjsg een geheimhoudingsplicht. Ook de Beroepscode Jeugdzorgwerker omvat een artikel over vertrouwelijkheid van informatie (art. J). Gegevens worden niet gedeeld tenzij er een grondslag bestaat voor doorbreking van de geheimhoudingsplicht.

3.11.4 Belang van samenwerking in een samenwerkingsverband
Nabijheid, aanwezigheid en zichtbaarheid van ketenpartners helpt in de afstemming tussen partners en het beter benutten van elkaars expertise. Meer kennis bij ketenpartners van wat Halt doet, helpt Halt in het bereiken van de juiste jongeren.

Daar waar binnen het samenwerkingsverband (complexe) jongeren worden besproken, kan Halt een bijdrage leveren door vanuit kennis en expertise mee te denken. De bij Halt aanwezige contextinformatie over eerdere contacten met jongeren, kan worden benut voor een optimale inschatting van de aard en omvang van problematiek en gewenste aanpak. Halt kan alleen informatie op casusniveau verstrekken als er sprake is van een wettelijke grondslag. Omdat Halt werkzaam is op zowel het gebied van preventie (lokaal netwerk scholen, wijk/jeugdteams, CJG's) en repressie (strafrechtsketen) kan vanuit beide domeinen/vlakken worden meegedacht.

3.12 Veilig Thuis (AMHK)
Het Advies en Meldpunt Kindermishandeling en de Steunpunten Huiselijk Geweld zijn per 1 januari 2015 samengevoegd tot het Advies en Meldpunt Huiselijk Geweld en Kindermishandeling (hierna: AMHK). In de WMO wordt gesproken van AMHK. Omdat in Nederland alle AMHK's zichzelf Veilig Thuis noemen, wordt er in het vervolg gesproken over Veilig Thuis. De gemeente is verantwoordelijk voor de instelling van een Veilig Thuis. De organisatie en positionering van het Veilig Thuis kan per gemeente/regio verschillen.

3.12.1 Doelstelling en taken
Veilig Thuis heeft twee hoofdtaken: het afhandelen van meldingen over huiselijk geweld en/of kindermishandeling en het geven van advies bij een vermoeden van huiselijk geweld of kindermishandeling.

De wettelijke taken van Veilig Thuis ten aanzien van meldingen zijn:

- fungeren als herkenbaar en toegankelijk meldpunt voor alle gevallen of vermoedens van huiselijk geweld en/of kindermishandeling;
- het naar aanleiding van een melding van huiselijk geweld of kindermishandeling of een vermoeden daarvan, onderzoeken of daarvan daadwerkelijk sprake is;
- het beoordelen van de vraag of en zo ja tot welke stappen de melding van huiselijk geweld of kindermishandeling of een vermoeden daarvan aanleiding geeft;
- het in kennis stellen van een instantie die passende professionele hulp kan verlenen bij huiselijk geweld of kindermishandeling, van een melding van huiselijk geweld of kindermishandeling of een vermoeden daarvan, indien het belang van de betrokkene dan wel de ernst van de situatie waarop de melding betrekking heeft daartoe aanleiding geeft;
- het in kennis stellen van de politie of de raad voor de kinderbescherming van een melding van huiselijk geweld of kindermishandeling of een vermoeden daarvan, indien het belang van de betrokkene dan wel de ernst van de situatie waarop de melding betrekking heeft, daartoe aanleiding geeft;
- indien Veilig Thuis een verzoek tot onderzoek bij de RvdK doet, het in kennis stellen daarvan van het college B&W;
- het op de hoogte stellen van degene die een melding heeft gedaan, van de stappen die naar aanleiding van de melding zijn ondernomen.

De taak van Veilig Thuis ten aanzien van het verstrekken van advies is:
- het verstrekken van advies aan degene die een vermoeden van huiselijk geweld of kindermishandeling heeft.

De gemeente en Veilig Thuis kunnen overeenkomen dat Veilig Thuis naast de wettelijke taken nog andere taken uitvoert op het gebied van huiselijk geweld en kindermishandeling, bijvoorbeeld de uitvoering van een huisverbod op grond van de Wet Tijdelijk huisverbod. Van belang hierbij is dat veel wettelijke bepalingen die betrekking hebben op Veilig Thuis, betrekking hebben op de wettelijke taken zoals hierboven genoemd. Exclusieve bevoegdheden die Veilig Thuis heeft zoals het verwerken van persoonsgegevens zonder toestemming van de betrokkenen en het doen van onderzoek zonder de betrokkenen daarover te informeren (zie ook hierna), heeft Veilig Thuis alleen bij het uitvoeren van een wettelijke taak.

3.12.2 Toepasselijke wet- regelgeving

In relatie tot de samenwerkingsverbanden in het zorg- en veiligheidsdomein is voor Veilig Thuis de volgende wet- en regelgeving van toepassing:
- Wet Maatschappelijke Ondersteuning (hierna: WMO);
- Jeugdwet;
- Handelingsprotocol Veilig Thuis 2019.

3.12.3 Wettelijk kader gegevensverwerking en verstrekken van gegevens

Verwerking van persoonsgegevens

Op grond van artikel 5.1.6 lid 1 WMO is Veilig Thuis bevoegd om voor de uitvoering van de wettelijke taken persoonsgegevens te verwerken.

Verwerking van persoonsgegevens bij meldingen
Voor het afhandelen van meldingen mag Veilig Thuis, op grond van artikel 5.1.6. lid 2 Wmo, persoonsgegevens betreffende de gezondheid, huiselijk geweld of kindermishandeling, verwerken van personen die betrokken zijn bij huiselijk geweld of kindermishandeling. Dit mag, indien uit een melding redelijkerwijs een vermoeden van huiselijk geweld of kindermishandeling kan worden afgeleid en de verwerking noodzakelijk is te achten voor de uitoefening van de wettelijke taken.

In artikel 5.2.9 WMO is bepaald dat Veilig Thuis het BSN nummer dient te gebruiken om te waarborgen dat de te verwerken persoonsgegevens betrekking op die persoon hebben.

Op grond van artikel 5.2.6.Wmo is Veilig Thuis bevoegd om in de onderzoeksfase, informatie te verkrijgen van ketenpartners en andere partijen. Als het gaat om informatie, waarmee Veilig Thuis een situatie van huiselijk geweld of kindermishandeling kan beëindigen, dan mogen de partijen – eventueel zonder toestemming van betrokkenen en/of met doorbreking van hun beroepsgeheim – deze informatie delen met Veilig Thuis.

In het Handelingsprotocol Veilig Thuis 2019 is aangegeven dat Veilig Thuis, indien zij dat voor een betere beoordeling van de melding relevant acht, bij de start van de triage de gegevens uit de melding kan aanvullen met informatie uit uitsluitend de volgende bronnen:
- de eigen systemen van Veilig Thuis of andere Veilig Thuis organisaties;
- de Gemeentelijke Basisregistratie Personen (BRP);
- het Centraal Gezagsregister;
- de Raad voor de Kinderbescherming;
- de Verwijsindex Risicojongeren;
- de politie en/of OM;
- de direct betrokkenen zelf, voogd of curator, over de vraag of zij open staan voor hulp en ondersteuning.

Verwerking van persoonsgegevens bij advies
Bij het uitvoeren van de adviserende taak kan Veilig Thuis persoonsgegevens verwerken, maar uitsluitend voor zover degene op wie die gegevens betrekking hebben daar toestemming voor heeft verleend. Aangezien er bij de adviestaak alleen contact is met de adviesvrager, kan hoogstens sprake zijn van toestemming van de adviesvrager en kunnen dus alleen zijn of haar eigen persoonsgegevens worden verwerken. De gegevens van de persoon over wie advies wordt gevraagd zijn anoniem.

De verwerking van persoonsgegevens over een adviesvraag moet op grond van artikel 5 AVG voldoen aan de basisbeginselen van de AVG, zoals doelbinding, dataminimalisatie en opslagbeperking (zie paragraaf 2.2.1 van dit Handvat). In het Handelingsprotocol Veilig Thuis 2019 is dit voor de specifieke situatie van Veilig Thuis nader toegelicht (zie hoofdstuk 4 van het Handelingsprotocol).

Verstrekking van persoonsgegevens
Veilig Thuis verwerkt persoonsgegevens ter uitvoering van de wettelijke taken. De derdenverstrekking moet derhalve plaatsvinden in het kader van dit doel. Daarnaast is van belang dat alleen relevante gegevens worden verstrekt. Het moet dus gaan om gegevens die noodzakelijkerwijs dienen te worden uitgewisseld in het kader van de hulpverlening aan de betrokkene. In de regel zal het voor het doel niet noodzakelijk zijn om bijvoorbeeld het complete dossier van de betrokken jeugdige te verstrekken aan een jeugdhulpaanbieder.

In artikel 4.1.8 Uitvoeringsbesluit WMO is bepaald dat Veilig Thuis geen inlichtingen verstrekt over de herkomst van persoonsgegevens die het naar aanleiding van een melding heeft verkregen indien een persoon die in een beroepsmatige, hulpverlenende of pedagogische relatie tot het slachtoffer of het vermoedelijke slachtoffer of zijn huiselijke kring staat, de persoonsgegevens naar aanleiding van een melding heeft verstrekt en het verstrekken van die inlichtingen:

- een bedreiging vormt of kan vormen voor het slachtoffer of het vermoedelijke slachtoffer of zijn huiselijke kring;
- een bedreiging vormt of kan vormen voor de persoon, bedoeld onder a, of medewerkers van die persoon;
- leidt of kan leiden tot een ernstige verstoring van de vertrouwensrelatie met de huiselijke kring waartoe het slachtoffer of het vermoedelijke slachtoffer behoort; b.het andere personen betreft dan die bedoeld onder a, behoudens voor zover zij daarvoor toestemming hebben gegeven.

Gegevensverstrekking aan Politie en OM
In het Handelingsprotocol Veilig Thuis 2019 is op drie momenten sprake van informatie-uitwisseling over meldingen tussen Veilig Thuis en de politie en/of het OM:

- In het kader van afstemming en samenwerking (paragraaf 2.4);
- De triagefase (paragraaf 7.4.1);
- De onderzoeksfase (paragraaf 10.6).

(Zie het protocol voor een verdere toelichting hierop).

De wijze waarop Veilig Thuis, de politie en het OM invulling geven aan de samenwerking is uitgewerkt in het model voor de samenwerkingsafspraken tussen Veilig Thuis, politie en OM.

Huisverbod
De burgemeester is op basis van artikel 2 lid 8 Wet tijdelijk huisverbod (Wth) bevoegd gegevens te ontvangen om te oordelen om wel/niet iemand uit huis te plaatsen. Hij kan op zijn beurt ook gegevens delen met Veilig Thuis (artikel 2 lid 8 juncto lid 3 Wth).

Geheimhoudingsplicht
Medewerkers van Veilig Thuis hebben op grond van artikel 5.3.3 lid 1 WMO een geheimhoudingsplicht: zonder toestemming van de betrokkene mogen zij geen gegevens over hen aan derden verstrekken. Voor de uitzonderingen op het beroepsgeheim wordt verwezen naar hoofdstuk 5.1.

3.13 Woningcorporaties

3.13.1 Doelstelling en taken

Woningcorporaties zorgen voor kwalitatief goede, energiezuinige en betaalbare woningen voor mensen die zich om wat voor reden dan ook niet zelfstandig kunnen redden op de woningmarkt. Ze bouwen, verhuren en onderhouden huurwoningen en maatschappelijke vastgoed. Ze helpen wijken leefbaar te houden en grijpen in bij ernstige overlast, huurschulden en woonfraude. Woningcorporaties werken daarbij samen met gemeenten, huurders, zorg- en welzijnsorganisaties, politie en andere partners. De overheid bepaalt (vooral via de Woningwet) wat woningcorporaties wel en niet mogen doen. Woningcorporaties (voor de wet 'toegelaten instellingen') zijn private instellingen zonder winstoogmerk en hebben, anders dan andere verhuurders, een publieke taak die in de Grondwet en de Woningwet is vastgelegd[31]. Woningcorporaties maken jaarlijks prestatieafspraken met gemeenten en huurdersorganisaties over hun activiteiten.

De belangrijkste taken van woningcorporaties, ofwel de diensten van algemeen economisch belang (DAEB):

- Het bouwen, verhuren en beheren van sociale huurwoningen. Sociale huurwoningen zijn in eerste instantie bestemd voor huishoudens met een laag inkomen (de inkomensgrens wordt vastgesteld door de overheid). Corporaties verhuren, soms met voorrang, al dan niet via een zorginstelling en/of op verzoek van de gemeente, woningen aan kwetsbare doelgroepen zoals ouderen, statushouders, mensen in crisissituaties (bijvoorbeeld vanwege een scheiding of vanwege huiselijk geweld), ex-gedetineerden, zwerfjongeren en mensen uit een GGZ-instelling, maatschappelijke opvang of beschermd wonen. Ze streven door middel van hun voorraadbeleid en toewijzingsbeleid naar gemengde wijken en gespreide en verantwoorde plaatsing van kwetsbare huishoudens.
- Het bouwen en beheren van maatschappelijk vastgoed. Daaronder vallen bijvoorbeeld buurthuizen, opvang voor dak- en thuislozen, wijkbibliotheken, woonzorggebouwen, hospices, blijf-van-mijn-lijfhuizen, veiligheidshuizen en ruimten voor op buurt of wijk gericht maatschappelijk werk en activiteiten op het gebied van welzijnswerk door stichtingen of verenigingen.
- Investeren in de leefbaarheid van wijken en buurten Corporaties zijn een belangrijke partner in de aanpak van kwetsbare wijken (fysieke en sociale herstructurering). Woningcorporaties ondersteunen initiatieven van bewoners om wijken prettig en leefbaar te houden. Woningcorporaties mogen investeren in kleinschalige infrastructuur in de directe nabijheid van woongelegenheden, en bijdragen aan de uitvoering van plannen ter bevordering van een schone woonomgeving, ter voorkoming van overlast en ter bevordering van de veiligheid (toegestaan mits dit ten goede komt aan eigen huurders en eventueel bewoners van verkochte voormalige corporatiewoningen).
- Zij kunnen daarnaast bijdragen aan woonmaatschappelijk werk (met inbegrip van het leveren van een bijdrage aan uitvoering van achter-de-voordeur-programma's

[31] Woonruimte is een primaire levensbehoefte van de mens. Daarom moet de overheid ervoor zorgen dat er voldoende woonruimte is. De wetgever heeft dat uitgewerkt in de Woningwet en de Huisvestingswet. Voor de concrete voorziening in de woningbehoefte maakt de overheid gebruik van in de Woningwet gereglementeerde woningcorporaties (toegelaten instellingen). Het gaat overigens niet alleen om het aantal woningen, maar ook om de kwaliteit van de woningen.

voor bijvoorbeeld welzijn, gezondheid of hygiëne, onder verantwoordelijkheid van andere maatschappelijke organisaties), mits het eigen huurders betreft.
- Woningcorporaties zetten naast het voorkomen en aanpakken van overlast ook in op het voorkomen van huurachterstanden en de aanpak van woonfraude (zoals hennepteelt en illegale onderverhuur). Woningcorporaties hebben buurtbeheerders en huismeesters in dienst. Zij zijn de ogen en oren van de corporatie in een wijk en werken samen met gemeente, politie, zorg en welzijn. Als verhuurder heeft een woningcorporatie de wettelijke verplichting om in te grijpen als een huurder ernstige overlast veroorzaakt.

3.13.2 Toepasselijke regelgeving

Woningcorporaties vervullen een publieke taak met een grondslag in de grondwet en de Woningwet. De volgende wetgeving is relevant:
- de Woningwet, het Besluit Toegelaten Instellingen Volkshuisvesting (BTIV) en de Regeling Toegelaten Instellingen Volkshuisvesting (RTIV) (als het gaat om taken op het gebied van leefbaarheid met name relevant artikel 45 van de Woningwet en artikel 51 van het BTIV);
- de Huisvestingswet;
- het Burgerlijk Wetboek (in dit kader met name relevant artikel 7:204 BW en 7:206 BW (gebrekenregeling) , artikel 7:213 en 7:214 BW (goed huurderschap) en art 7:271 lid1 (tijdelijke verhuur));
- de Wet bijzondere maatregelen grootstedelijke problematiek (Wbmgp);
- de Wet aanpak woonoverlast (gemeentelijke gedragsaanwijzing);
- de Wet Victoria (Gemeentewet artikel 17a), Wet Victor (Woningwet artikel 13b), Wet Damocles (Opiumwet artikel 13b), die de burgemeester bevoegdheid geeft een woning te sluiten.

3.13.3 Wettelijk kader gegevensverwerking en verstrekken van persoonsgegevens

Woningcorporaties mogen persoonsgegevens verwerken ten behoeve van de uitoefening van hun taken. Of het verstrekken van persoonsgegevens in specifieke gevallen toegestaan is, hangt af van de situatie. Per casus moet bekeken worden voor welk doel de gegevens verwerkt worden. De meest gebruikte grondslagen bij corporaties zullen zijn:
- uitvoering van de overeenkomst;
- wettelijke plicht;
- gerechtvaardigd belang;
- toestemming van de betrokkene.

Er is geen specifieke wetgeving voor woningcorporaties voor het verwerken van bijzondere of strafrechtelijke persoonsgegevens[32]. Dit kan in uitzonderlijke gevallen wel noodzakelijk zijn voor taken zoals de huisvesting van kwetsbare doelgroepen in combinatie met zorg en de aanpak van woonoverlast en woonfraude. In dat geval moet

[32] In dit kader is de algemene uitzondering in de UAVG van het aanleggen van zwarte lijsten van belang. Woningcorporaties mogen strafrechtelijke gegevens verwerken voor de aanleg van een 'zwarte lijst' – daar komt een betrokkene alleen op in geval van zeer ernstige huurschulden of woonfraude. Deze zwarte lijsten worden op veel plaatsen gedeeld binnen het regionale samenwerkingsverband voor woningtoewijzing. Voor het delen van een zwarte lijst is een vergunning van de AP nodig.

de woningcorporatie kijken naar de bepalingen in de AVG zoals beschreven in paragraaf 2.3 en 2.5 van dit handvat.

3.13.4 Belang van samenwerking in een samenwerkingsverband

Woningcorporaties willen huisuitzettingen vanwege bijvoorbeeld schulden of overlast zoveel mogelijk voorkomen – ook omdat dit meestal een verplaatsing van het probleem inhoudt – en hebben tegelijkertijd een verantwoordelijkheid voor het woongenot van omwonenden en de leefbaarheid in een wijk. In hun werk in de wijk komen woningcorporaties partijen binnen het zorg- en veiligheidsdomein tegen. Vaak spelen er bij complexe casussen en in kwetsbare wijken problemen in de sfeer van schulden en huurachterstanden, verwaarlozing, vervuiling en schade in en om de woning, problematische overlast en/of criminaliteit vanuit de woning (drugs, prostitutie, illegale onderhuur, mensenhandel). In sommige gevallen is een huurder een gevaar voor zichzelf en/of omwonenden (ontploffingsgevaar, brandstichting of intimidatie van buurtbewoners).

Samenwerken maakt het mogelijk om preventief op te treden en adequaat en gelijkgericht in te grijpen bij bovenstaande problemen. Woningcorporaties, met woonconsulenten en buurtbeheerders in dienst, hebben een belangrijke signaleringsfunctie en horen samen met de politie vaak als eerste als er woonoverlast ontstaat. Zij hebben informatie over woon- of betalingsgedrag of over overlastgevend, crimineel of potentieel gevaarlijk gedrag. Daarnaast kan de woningcorporatie (al dan niet samen met gemeente en politie) specifieke maatregelen inzetten (selectieve woningtoewijzing, directe bemiddeling voor huisvesting, opleggen van een gedragsaanwijzing, vordering tot huisuitzetting, tweede-kans-contracten of randvoorwaarden aan een huurcontract). Andersom kan de juiste begeleiding vanuit de zorg of ingrijpen op een ander leefgebied huisuitzetting voorkomen.

Omdat de woningcorporatie vanuit verschillende taken en doelen aan betrokken kan zijn bij een casus, is het van belang steeds goed voor ogen te hebben vanuit welke taak en met welk doel de corporatie aan tafel zit.

4 Toepassing van het handvat in de praktijk

4.1 Algemeen

Voor de aanpak van complexe casuïstiek in het zorg- en veiligheidsdomein is samenwerking noodzakelijk tussen verschillende partijen. Partijen die veelvuldig met elkaar samenwerken richten in de praktijk meestal een samenwerkingsverband op middels een convenant. De praktijk laat een veelheid aan convenanten zien rond verschillende thema's, o.a. Zorg- en veiligheidshuizen voor de aanpak van complexe casuïstiek volgens het landelijk kader zorg- en veiligheidshuizen, aanpak radicalisering volgens het landelijk radicaliseringsconvenant, aanpak personen verward gedrag, samenwerkingsconvenanten voor sociale wijkteams, en voor de aanpak van jeugdgroepen.

In een convenant maken partijen afspraken over het onderwerp en doel van de samenwerking, de organisatie en de financiering. Echter, zoals in de inleiding van dit handvat vermeld: een convenant betekent niet dat partijen daarmee ook een nieuwe wettelijke grondslag krijgen om gegevens uit te wisselen. De rechtmatigheid van de gegevensverwerking en uitwisseling moet altijd getoetst worden aan de bestaande wettelijke kaders.

Die toetsing kan voor een belangrijk deel vóóraf plaats vinden bij de inrichting van het samenwerkingsverband, de werkprocessen en het daarvoor noodzakelijke gebruik van gegevens. Het resultaat daarvan wordt vastgelegd in het privacy-protocol. Het protocol schetst de juridische basis voor de verwerking en uitwisseling van gegevens tijdens de uitvoering van de werkzaamheden, de beperkingen en randvoorwaarden die daarbij in acht genomen moeten worden, de afspraken die nodig zijn om een zorgvuldige omgang met gegevens te waarborgen, en de wijze waarop invulling gegeven wordt aan bijvoorbeeld de rechten van betrokkene en de informatieplicht richting de betrokkene uit de AVG.

Dit handvat biedt een overzicht van die wettelijke kaders. In dit hoofdstuk gaan we in op de consequenties van dit handvat voor de praktijk.

Daarbij besteden we aandacht aan:

- aandachtspunten bij de juridische inrichting van de gegevensverwerking in het kader van een samenwerkingsverband;
- aandachtspunten voor het toetsen van de rechtmatigheid van gegevensverwerking bij het behandelen van een (complexe) casus in de praktijk;
- aandachtspunten bij de ontwikkeling van het werkproces en afspraken over zorgvuldigheid;
- de zorgvuldigheidseisen die professionals in het oog moeten houden bij het behandelen van een (complex) casussen;
- eisen aan het gebruik van ICT-systemen bij samenwerking.

In bijlage 2 is een voorbeeld opgenomen over de wijze waarop de Zorg- en Veiligheidshuizen de uitgangspunten van dit handvat hebben toegepast op hun

werkproces en de daarbij noodzakelijke gegevensverwerking. Zij maken daarbij gebruik van een vier-fasemodel voor procesregie bij de behandeling van complexe casuïstiek. Deze fasen zijn: aanmelding en intake, triage en voorbereiden casusoverleg, casusoverleg en afschaling. Het fasemodel en de wijze waarop de uitgangspunten uit dit handvat worden toegepast zijn in grote lijnen toepasbaar op elke situatie waarbij een vorm van procesregie en casusoverleg noodzakelijk zijn om de samenwerking tussen partijen uit meerdere domeinen rond een specifieke casus te organiseren.

4.1.1 Zorgvuldig, bewust en met respect: succesfactoren voor samenwerking
Samenwerking in het zorg- en veiligheidsdomein wordt veelal als complex ervaren. Die complexiteit hangt in belangrijke mate samen met de verschillende logica's die in de verschillende domeinen dominant zijn.

In het veiligheidsdomein is het delen van informatie en gegevens ten behoeve van het opsporen, bestrijden en sanctioneren van overlast, criminaliteit en gevaarlijke situaties een belangrijk uitgangspunt. Wetgeving faciliteert de gegevensuitwisseling binnen de keten voor deze doelen, vanuit het maatschappelijk belang om de samenleving te beschermen tegen gevaarlijk en ongewenst gedrag.

In het zorg- en sociaal domein staat de cliënt centraal. Gemeenten zijn daarbij belast met toeleiding. Zorg- en hulpverleners met de levering van hulp. In de regelgeving ten aanzien van gegevensverwerking door zorg- en hulpverleners ligt de nadruk op de bescherming van de persoonlijke levenssfeer van het individu. Dit komt tot uitdrukking in het wettelijke verankerde medisch beroepsgeheim en de geheimhoudingsverplichting op het dossier van de jeugdhulpverlener. Hier staat het maatschappelijk belang voorop dat mensen met problemen op het gebied van gezondheid, en/of welzijn altijd hulp durven te zoeken, zonder angst voor vervolging bijvoorbeeld. Beroepscodes geven professionals houvast als het gaat om het maken van afwegingen om hun geheimhouding te doorbreken. En het tuchtrecht toetst of -in geval van een klacht- de professional zich heeft gehouden aan de professionele standaarden. Het tuchtrecht rust op de individuele professional. Indien een klacht wordt gehonoreerd kunnen de sancties voor de betreffende professional variëren van een berisping tot een verbod om nog binnen het vakgebied werkzaam te zijn.

Deze verschillen in logica en wettelijk kader geven in belangrijke mate richting aan de houding van professionals ten aanzien het uitwisselen van gegevens. In de praktijk geeft dat soms wrijving: de justitie of OOV-ambtenaar die in de ogen van de zorgverlener teveel wil weten; en de zorgverlener die in de ogen van de justitie of OOV-ambtenaar niks wil vertellen. Samenwerking in het zorg- en veiligheidsdomein vraagt van professionals de bereidheid om voorbij dit soort beelden te komen, zich in te leven in elkaars positie en vanuit respect voor elkaars juridische kaders en dilemma's, op zoek te gaan naar mogelijkheden om tot oplossingen te komen die in het belang zijn van de betrokkenen en de omgeving.

De ‘manifestpartners In goed vertrouwen; de privacy van de jeugd geborgd[33]’ hebben in ten behoeve van samenwerking in het jeugddomein een aantal vuistregels opgesteld die ook behulpzaam kunnen zijn in het zorg- en veiligheidsdomein:

1. Wij vertrouwen elkaar in onze deskundigheid en professionaliteit;
2. Wij vragen nooit méér persoonsgegevens dan strikt noodzakelijk;
3. Wij zijn altijd transparant over met welk doel wij persoonsgegevens vragen;
4. Wij respecteren de positie en eigen verantwoordelijkheid van de professional aan wie wij persoonsgegevens vragen;
5. Wij maken altijd een zorgvuldige afweging of het mogelijk is om gegevens te verstrekken in het belang van de betrokkene;
6. Wij hebben vertrouwen in de andere professional, dat deze de afweging om wel of geen gegevens te vragen of te verstrekken zorgvuldig heeft gemaakt;
7. Wij voelen ons verantwoordelijk om waar mogelijk bij te dragen aan oplossingen voor de probleemsituatie van een jeugdige, zijn ouders of verzorgers, ook als bepaalde gegevensuitwisseling niet mogelijk is.

4.2 Aandachtspunten bij de juridische inrichting van de gegevensverwerking bij samenwerking rond complexe casuïstiek

4.2.1 De juridische positie van het samenwerkingsverband met betrekking tot gegevensverwerking

De samenwerkingsverbanden in het zorg- en veiligheidsdomein hebben geen eigenstandige wettelijke taak en dus ook geen eigen wettelijke basis om persoonsgegevens te verwerken.
Bij de samenwerking rond een specifieke casus behouden de deelnemende partijen hun eigen inhoudelijke bevoegdheden en verantwoordelijkheden voor de eigen taken.

De consequentie hiervan is dat ‘het samenwerkingsverband’ nooit op eigen titel gegevens verwerkt, maar de gegevens verwerkt ten behoeve van een of meerdere van de partijen. Juridisch gezien vindt er dus geen gegevensuitwisseling plaats tussen een organisatie en het samenwerkingsverband, maar tussen de betrokken organisaties onderling. In deze gevallen is er steeds sprake van een bilaterale verstrekking die ook simultaan kan plaatsvinden. In dat laatste geval wordt door een partij tegelijkertijd aan meerdere partijen persoonsgegevens verstrekt. Alleen de Wpg maakt het mogelijk om naast bilaterale verstrekkingen aan partijen, ook politiegegevens te verstrekken aan een samenwerkingsverband zelf (artikel 20 Wpg).

Vaak heeft het samenwerkingsverband een eigen organisatie met medewerkers die activiteiten uitvoeren en gegevens verwerken ten behoeve van de partijen bij specifieke casussen. Dan treedt zij op als faciliterende organisatie ten behoeve van de partijen. In dat geval moet bij de inrichting van het samenwerkingsverband aandacht besteed worden aan de juiste bevoegdheidsverlening aan de medewerkers van het samenwerkingsverband.

[33] De manifestpartners In goed vertrouwen; de privacy van de jeugd geborgd, is een coalitie van ruim 20 branche- en beroepsorganisaties in de jeugdhulp en jeugdbescherming waaronder VNG, GGZ Nederland, NIP, KNMG, ACTIZ, BPSW, Sociaal Werk Nederland en VGN. Meer informatie zie: www.privacyborgingjeugd.nl. Hier vindt u ook de volledige versie van de vuistregels.

4.2.2 Regie

In het zorg- en veiligheidsdomein werken partijen samen aan complexe oplossingen voor complexe problemen. Samenwerking is noodzakelijk om tot gecoördineerde actie te komen, omdat het vraagstuk niet kan worden opgelost als partijen onafhankelijk van elkaar en zonder afstemming hun interventies richting betrokkene(n) uitvoeren. In vrijwel alle gevallen is ook de effectiviteit van de interventies gericht op de eigen doelen gebaat bij gecoördineerde actie.

In dit verband wordt vaak gebruik gemaakt van de term regie en worden de volgende vormen van regie onderscheiden:

- Strategische regie
- Procesregie
- Casusregie

Er zijn veel verschillende definities voor deze begrippen. In dit handvat maken we gebruik van de definities zoals deze gehanteerd worden bij de zorg- en veiligheidshuizen.

Met *strategische regie* wordt bedoeld: de werkzaamheden gericht op het organiseren het samenwerkingsverband zoals het maken van afspraken over de doelen, organisatiestructuur en financiering van de samenwerking, en het opstellen van een convenant en privacy-protocol.

Bij *procesregie* gaat het om het uitvoeren van werkzaamheden gericht op de totstandkoming van samenwerking tussen partijen bij het behandelen van één specifieke casus en de ondersteuning van de casusregisseur bij de uitvoering van het plan van aanpak. Bij de zorg- en veiligheidshuizen worden deze werkzaamheden uitgevoerd door een *procesregisseur*.

Bij *casusregie* gaat het om het uitvoeren van werkzaamheden gericht op het bewaren van de onderlinge samenhang bij het uitvoeren van het plan van aanpak bij het behandelen van één specifieke casus. De verantwoordelijkheid hiervoor ligt bij een *casusregisseur*. Dit is altijd een medewerker van een van de partijen, meestal de partner met de meeste inhoudelijke expertise voor de betreffende casus. Deze kan zich laten ondersteunen door de *procesregisseur*.

<u>Juridische status van proces- en casusregie</u>

Regie is een veel gehanteerd begrip in beleidsstukken, memories van toelichting en om de coördinerende werkzaamheden in de uitvoering aan te duiden. Echter het is geen begrip dat in wetgeving in het zorg- en veiligheidsdomein expliciet is gedefinieerd. Dit betekent dat de juridische basis om persoonsgegevens te verwerken of uit te wisselen ten behoeve van proces- of casusregie altijd gevonden moet worden in de verschillende taken van de partijen die samenwerken rond een casus.

De juridische basis voor het ter beschikking stellen van gegevens ten behoeve van procesregie is dan gelegen in de noodzaak tot een beter begrip van de casus door de te betrekken partijen. Met als doel, beoordelen of afstemming en samenwerking tussen

partijen noodzakelijk is met het oog op de effectiviteit van lopende interventies, en in beeld te brengen of aanvullende voorzieningen ingezet moeten worden.

De juridische basis voor het ter beschikking stellen van gegevens ten behoeve van casusregie is dan gelegen in de noodzaak voor de betrokken partijen om in het kader van de eigen taakuitoefening en de gezamenlijke opgave, inzicht te krijgen in de ontwikkelingen in de casus, de effectiviteit van afgesproken interventies, en indien nodig te komen tot aanpassing van afgesproken interventies en beschikkingen.

4.2.3 Verantwoordelijkheid voor de gegevensverwerking in de zin van de AVG

Bij de inrichting van de samenwerking is het ook belangrijk om aandacht te besteden aan de verantwoordelijkheden ten aanzien van de gegevensverwerking. Zowel in de formeel juridische zin (wie zijn verantwoordelijk in de zin van de AVG voor de gegevensverwerking die plaats vindt in het samenwerkingsverband) als in materiële zin: hoe wordt in de praktijk vorm gegeven aan die verantwoordelijkheid en de inhoudelijke zeggenschap over de gegevens.

Op grond van artikel 26 AVG zijn twee of meer verwerkingsverantwoordelijken gezamenlijk verwerkingsverantwoordelijken wanneer zij gezamenlijk de doeleinden en middelen van de verwerking van de persoonsgegevens bepalen.

De gezamenlijke verwerkingsverantwoordelijken stellen op transparante wijze hun onderlinge verantwoordelijkheden voor de naleving van de AVG vast, met name met betrekking tot de inhoudelijke zeggenschap over de gegevens, informatiebeveiliging, en de rechten van betrokkenen. Zo is het belangrijk dat de betrokkene weet waar hij terecht kan om zijn of haar rechten uit te oefenen. De Zorg- en veiligheidshuizen hebben dit uitgewerkt in een samenwerkingsconvenant en bijbehorend privacy-protocol. Deze zijn opgenomen in bijlage 3 en 4 van dit handvat.

Ongeacht de afspraken tussen de gezamenlijke verwerkingsverantwoordelijken blijven zij hoofdelijk aansprakelijk voor de naleving van de AVG.

4.3 Aandachtspunten voor het toetsen van de rechtmatigheid bij de inrichting van de samenwerking

Het feit dat de samenwerkingsverbanden in het zorg- en veiligheidsdomein geen eigenstandige wettelijke taak hebben, samenwerkingen zijn van rechtspersonen zonder eigen juridische entiteit, en het feit dat het begrip regie niet als taak in wetgeving is vastgelegd, maakt de beoordeling van de rechtmatigheid van de gegevensverwerking in het kader van samenwerking rond specifieke casussen complex. Daarbij spelen steeds de volgende vragen een rol:

- Is er een grondslag voor het verstrekken van gegevens ten behoeve van het behandelen van een casus?
- Hebben de andere partijen die deelnemen aan de behandeling een grondslag voor het ontvangen van de gegevens in het kader van het behandelen van een casus?
- Welke gegevens zijn noodzakelijk om te verstrekken gegeven het specifieke doel van de verstrekking in een bepaalde fase van het werkproces?

– Mogen partijen bijzondere en/of strafrechtelijke persoonsgegevens verwerken?
– Voor welke partijen speelt een geheimhoudingsplicht of beroepsgeheim een rol bij de vraag of gegevens verstrekt kunnen worden en onder welke voorwaarden?
– Welke waarborgen bouwen wij in om onnodige verspreiding van gegevens tegen te gaan en te voorkomen dat gegevens gebruikt worden voor andere doelen dan afgesproken?

Daarnaast dient de gegevensverwerking te voldoen aan de materiële eisen uit de AVG zoals informatiebeveiliging, en de rechten en plichten van de betrokkene(n).

De juridische basis voor het ontvangen en verstrekken van gegevens kan soms gelegen zijn in specifieke wettelijke bepalingen die een wettelijke verplichting of een wettelijke bevoegdheid inhouden voor partijen om gegevens aan een andere partij te verstrekken voor de specifieke taken van een partij[34]. Deze staan meestal in een van toepassing zijnde materiewet.
Voorbeelden van wettelijke bepalingen die een verplichting of bevoegdheid inhouden om gegevens aan een bepaalde partij te verstrekken zijn:

- De verplichting voor iedere hulpverlener om, voor zover noodzakelijk, informatie te verstrekken aan een gezinsvoogd als er sprake is van een ondertoezichtstelling (zie artikel 7.3.11 lid 4 Jeugdwet).
- De bevoegdheid van het AMHK (Veilig Thuis) om de politie in kennis te stellen van een melding van huiselijk geweld of kindermishandeling, of een vermoeden daarvan indien de melding daar aanleiding toe geeft (WMO artikel 4.1.1 tweede lid onder, e).

[34] De AVG zegt dat er sprake is van een wettelijke verplichting 'die op de verwerkingsverantwoordelijke rust'. De AVG geeft in de artikelen en overwegingen geen scherp uitsluitsel of het alleen gaat om een wettelijke verplichting als een bestuursorgaan of private partij zelf specifiek door de wetgever is verplicht om persoonsgegevens te vergaren en verwerken óf dat het ook gaat om een wettelijke verplichting wanneer er moet worden verstrekt aan een andere partij. Het begrip 'verwerken' is een containerbegrip voor zowel vragen als verstrekken, voor zowel ongevraagd (dus vrijwillig) verstrekken als voor desgevraagd verstrekken en ook voor gedwongen verstrekken. In de onderliggende materiewetgeving wordt steeds precies uitgewerkt welke situatie aan de orde is.

- De verplichting van partijen om gegevens (persoonsgegevens en andere gegevens) te verstrekken aan opsporingsdiensten en Openbaar Ministerie zodra er ten behoeve van een opsporingsonderzoek gegevens worden gevorderd op grond van art. 126 nc of nd Sv.
- De bevoegdheid voor een (bij voorkeur niet-behandelend) psychiater of arts in het kader van de uitvoering van de Wet verplichte ggz, om aan de burgemeester specifieke gegevens te verstrekken over betrokkene ten behoeve van een crisismaatregel van betrokkene. De arts heeft daarmee de mogelijkheid om in dat specifieke geval zijn medische beroepsgeheim zoals neergelegd in de Wet verplichte ggz te doorbreken zonder dat er sprake hoeft te zijn van een conflict van plichten.

Indien er geen specifieke wettelijke bepalingen zijn op grond waarvan partijen gegevens kunnen of moeten verstrekken, kan de juridische basis gelegen zijn in de goede taakuitoefening van de taak van de ontvanger. De vragende partij moet dan onderbouwen om welke (wettelijke) taak[35] het gaat en waarom verstrekking noodzakelijk is. De afweging om te verstrekken ligt altijd bij de verstrekkende partij. Deze zal overtuigd moeten zijn van zowel de taak als de noodzaak van de gevraagde gegevens. Een bestuursorgaan moet als zij verzoekt om persoonsgegevens altijd een wettelijke taak hebben. Het mag geen persoonsgegevens vragen voor doelen waarvoor het geen wettelijke taak heeft of die onverenigbaar zijn met de bestaande eigen wettelijke taken: zo mogen bijvoorbeeld gemeenten geen persoonsgegevens van slachtoffers aan SHN vragen om zo de aangiftebereidheid van burgers te verhogen. Daar hebben zij geen wettelijke taak in en dus is dat onrechtmatig. Maar zij mogen bijvoorbeeld wel op grond van de Jeugdwet in overleg treden met een school voor zover dit noodzakelijk is voor het treffen van een individuele voorziening van de Jeugdwet (art. 2.7 eerste lid Jeugdwet).

Ook is het mogelijk dat een partij op eigen initiatief gegevens wil verstrekken omdat dit noodzakelijk is voor de goede uitvoering van de eigen (wettelijke) taak[36]. In dergelijke situaties moet er altijd een noodzaak zijn voor de verstrekking, én de ontvangende partij moet uiteraard wel iets met de gegevens kunnen doen. Dat betekent dat hij een eigen grondslag moet hebben op basis waarvan hij de gegevens mag verwerken. Deze zal veelal gelegen zijn in de eigen taak in relatie tot de betrokkene.

Bij de behandeling van complexe casussen in het zorg- en veiligheidsdomein doet bovenstaande situatie zich veelvuldig voor in een bijzondere variant. Partijen hebben vanuit de eigen taak een belang om tot afstemming van activiteiten te komen met het oog op een grotere effectiviteit van de eigen activiteiten, of willen door afstemming juist voorkomen dat afzonderlijke interventies elkaar doorkruisen. Zij zullen in eerste instantie moeten ‘onderzoeken’ of het noodzakelijk is om tot afstemming te komen, of dat het noodzakelijk is om elkaar gegevens te verstrekken. Dit ‘zoekproces’ is vaak kenmerkend voor de eerste fase in een casusoverleg. Partijen brengen dan vanuit het belang van de eigen taakuitoefening gegevens in met als eerste doel om tot een gezamenlijk beeld te komen of afstemming noodzakelijk is, of dat er wellicht aanvullende interventies nodig

[35] Met taak wordt hier ook bedoeld de activiteiten die een private partij zoals maatschappelijk werk uitvoert ten behoeve van betrokkene.
[36] Idem, zie voetnoot 31

zijn. Pas in tweede instantie kunnen ze bepalen of ze gegevens ook aan een bepaalde partij willen verstrekken ten behoeve van de taken van die partij.

Wanneer de grondslag voor de gegevensverwerking is gelegen in de uitoefening van de eigen taak en de taak van de ontvanger, dan moet er rekening mee worden gehouden dat specifieke wettelijke geheimhoudingsverplichtingen een rol kunnen spelen. Dit is het geval bij partijen die gehouden zijn aan het medisch beroepsgeheim, en bij de jeugdhulpverlener voor zover het gegevens betreft uit het behandeldossier. Zij kunnen in de regel alleen verstrekken met uitdrukkelijke toestemming van de betrokkene, tenzij er sprake is van een uitzonderingssituatie bij een conflict van plichten. De afweging of er sprake is van een uitzonderingssituatie zal per geval gemaakt moeten worden. Zie hiervoor ook paragraaf 2.7 van dit Handvat. Medisch professionals kunnen daarbij gebruik maken van het stappenplan dat is opgesteld door hun beroepsorganisaties.

Indien er geen wettelijke verplichting is, en ook geen grondslag in de eigen taak of die van de ontvanger, dan kunnen er geen gegevens verstrekt worden.

In hoofdstuk 2 van dit handvat wordt uitgebreid ingegaan op de vraag wanneer welke AVG-grondslagen voor verschillende partijen in het zorg- en veiligheidsdomein aan de orde kunnen zijn, bijzondere persoonsgegevens en de uitzonderingsgronden van artikel 23 AVG. In hoofdstuk 3 wordt uitgebreid ingegaan op de (wettelijke) taken die spelen voor de verschillende partijen. Bijlage 4 bevat het model privacy-protocol voor de zorg- en veiligheidshuizen. Daarin zijn de wettelijke taken en grondslagen uitgewerkt voor de partijen die samen werken in de zorg- en veiligheidshuizen.

4.3.1 Het privacy-protocol

Bij het *inrichten* van samenwerking rond complexe casuïstiek zullen deelnemende partijen zich *vooraf* rekenschap moeten geven van bovenstaande vragen. Met andere woorden: zij zullen in kaart moeten brengen op welke grondslagen partijen gegevens kunnen verstrekken en ontvangen bij de behandeling van complexe casuïstiek, de randvoorwaarden waaronder dat mogelijk is, voor welke partijen er beperkingen zijn bij het verwerken van bijzondere en strafrechtelijke gegevens, en voor welke partijen er sprake is van een beroepsgeheim en de consequenties daarvan. En zij zullen afspraken moeten maken om te waarborgen dat gegevens niet onnodig in verspreid raken, en niet gebruikt worden voor andere doelen dan afgesproken.

Door hier bij de inrichting van de samenwerking zo nauwkeurig mogelijk antwoord op te geven kan professionals duidelijkheid gegeven worden waar zij op moeten letten als zij bij het behandelen van een specifieke casus te maken hebben met een specifieke constellatie van partners.

Het resultaat van deze analyse en afspraken wordt vastgelegd in het privacy-protocol voor de gegevensverwerking.

Indien een samenwerkingsverband meerdere taken uitvoert dient voor elke taak de analyse opnieuw gemaakt te worden en zo nodig een apart protocol opgesteld te worden.

Bijvoorbeeld: als in het samenwerkingsverband zowel de radicaliseringstafel wordt uitgevoerd, als complexe casuïstiek volgens het landelijk kader veiligheidshuizen, dienen voor beide taken bovengenoemde punten in kaart gebracht te worden. In dit voorbeeld is het te adviseren om voor de radicaliseringszaken het landelijk convenant radicalisering als uitgangspunt te nemen (dit bevat tevens de zaken die in een protocol geregeld moeten worden) en voor de complexe casuïstiek volgens het landelijk kader, het model privacy-protocol voor de Zorg- en Veiligheidshuizen.

4.4 Aandachtspunten bij de ontwikkeling van het werkproces en afspraken over zorgvuldigheid

4.4.1 De aard van het proces bij complexe casuïstiek en de consequenties voor gegevensverwerking

Het proces van het behandelen van complexe casussen op het snijvlak van zorg- en veiligheid kenmerkt zich in hoge mate door zoeken naar wat er aan de hand is: overzicht en inzicht creëren (beeldvorming), met behulp van de verschillende expertises van deelnemers komen tot een set van zinvolle interventies gegeven de problematiek en specifieke situatie (oordelen), afstemmen van lopende trajecten met als doel dat deze elkaar niet in de weg zitten maar zo mogelijk elkaar versterken, en komen tot een gezamenlijke aanpak (besluiten).

In privacywetgeving staan – naast de juridische grondslag – het doel en de noodzakelijkheid van gegevensverwerking en uitwisseling voorop. Er mogen pas gegevens gedeeld worden als er een wettelijke grondslag voor is, als het doel ervan duidelijk is, en als het delen van gegevens noodzakelijk is voor dat doel. Bovendien moet de partij die de persoons gegevens ontvangt op grond van de AVG gerechtigd zijn om de (bijzondere) persoonsgegevens te verwerken. Voor zorgverleners geldt dat het beroepsgeheim en het belang van de cliënt zich er niet tegen mogen verzetten tenzij er sprake is van een conflict van plichten.

Het zoekproces dat inherent is aan (de beginfase van) het behandelen van complexe casuïstiek maakt dat de doelen voor gegevensverwerking gedurende het proces kunnen veranderen. Het hoofddoel is het oplossen van de probleemsituatie, maar de doelen voor de gegevensverstrekking kunnen variëren van in beeld brengen wat er aan de hand is, tot afstemming, tot het mogelijk maken van specifieke interventies door een partner. Dat laatste wordt meestal pas duidelijk aan het eind van een casusoverleg. Dit maakt het voor deelnemers moeilijk om bij de start van een casus in te kunnen schatten of de gegevens die zij dan inbrengen ook gebruikt mogen worden voor de doelen die er aan het eind van een casusoverleg uit rollen.

Meest voorkomende doelen voor gegevensverwerking bij het behandelen van complexe casuïstiek

- Bepalen of een casus voldoet aan de criteria om in het kader van het samenwerkingsverband op te pakken;
- Inzicht krijgen welke partijen reeds betrokken zijn of betrokken moeten worden en op welke wijze;
- Bepalen van het doel en thema's van een eventueel casusoverleg;
- Bepalen gemeenschappelijk 'beeld' met de te betrekken partijen om te komen tot afstemming en of plan van aanpak, afspraken over uitvoering en gegevensgebruik;
- Afbouwen van de betrokkenheid van het samenwerkingsverband en - indien er gegevens opgeslagen zijn - opschonen en op termijn vernietigen van het dossier.

Deelnemers die gegevens hebben ingebracht moeten aan het eind van het proces dan eigenlijk een nieuwe afweging maken: kan ik de gegevens die ik gedeeld heb ten behoeve van een gezamenlijke beeldvorming ook verstrekken ten behoeve van de vervolgacties in het plan van aanpak. Bijvoorbeeld: een zorgverlener zal wellicht niet willen dat informatie om tot een goede inschatting te komen van zinvolle interventies, ook gebruikt wordt voor een eventuele strafrechtelijke interventie. Of omgekeerd, politie en OM willen niet dat een hulpverlener bepaalde informatie die noodzakelijk was om zicht te krijgen op mogelijke handelingsperspectieven, gebruikt en kenbaar maakt in het contact met een cliënt.

Een voorbeeld: zo hoort het niet

Een psychiater deelt in een casusoverleg informatie t.b.v. de beeldvorming van een cliënt die voor onveilige situaties zorgt en verward gedrag vertoont. Er worden afspraken gemaakt over de vervolgacties. Er wordt de afspraak gemaakt dat niemand inhoudelijke informatie van de psychiater vastlegt voor eigen gebruik. Er wordt alleen een handelingsadvies opgesteld hoe om te gaan met de cliënt bij problemen. Dat was ook de basis waarop de psychiater toestemming had gekregen van de cliënt om deel te nemen. Enige maanden later duikt inhoudelijke informatie die de psychiater heeft ingebracht op in een procedure die een van de partners heeft aangespannen tegen de cliënt. Dit was niet besproken in het overleg. Was dat wel het geval geweest, dan had de psychiater nooit akkoord willen gaan met het gebruik van zijn informatie voor dat doel. Het resultaat is dat de psychiater voortaan geen informatie meer deelt in overleggen waar de betreffende partner bij is.

Het is aan de organisaties die afspreken met elkaar samen te willen werken om afspraken te maken hoe zij willen dat hun professionals in de praktijk dienen om te gaan met dit dilemma, en hoe wordt bewaakt dat deze afspraken worden nageleefd. Die afspraken behoren onderdeel te zijn van het privacy-protocol. In de volgende paragraaf wordt hier nader op ingegaan.

4.4.2 Uitgangspunten (afspraken) voor zorgvuldige gegevensverwerking bij het behandelen van complexe casussen

Het dilemma waarvoor deelnemers komen te staan laat zich alleen oplossen door een duidelijke fasering aan te brengen in het werkproces voor de behandeling van de complexe casuïstiek, en de doelen voor gegevensverwerking voor elke fase te concretiseren. Omdat de doelen per fase kunnen verschillen, is het belangrijk dat de partij die gegevens inbrengt gedurende het proces de zeggenschap houdt over het gebruik van gegevens door andere deelnemers aan het behandelen van de casus. Met andere woorden: op alle informatie die tijdens het proces op tafel komt rust een strikte geheimhoudingsplicht voor alle deelnemers. En niemand mag gegevens 'meenemen' en vastleggen voor eigen gebruik tenzij dit is afgesproken en de partij die de gegevens heeft ingebracht daarmee akkoord is. Iedere deelnemer moet er van op aan kunnen dat verstrekte gegevens niet gebruikt worden voor andere activiteiten en doelen dan afgesproken.

Dat vraagt om discipline van deelnemers, en een zorgvuldige bewaking van de omgang met gegevens gedurende het proces van de behandeling van een casus.

De aard van het proces van het behandelen van complexe casuïstiek vraagt om de volgende uitgangspunten:

1. Er is sprake van een duidelijke fasering van het werkproces met concretisering van doelen voor gegevensverwerking per fase;
2. Er is sprake van een strikte doelbinding bij gebruik van gegevens bij de verschillende fasen van het behandelen van casussen. Alleen de voor het doel van die fase noodzakelijke gegevens worden verwerkt;
3. Als het doel wijzigt wordt als eerste opnieuw beoordeeld of de eerder verwerkte gegevens ook daarvoor (het andere doel) noodzakelijk zijn en vervolgens of de gegevens daarvoor ook (verder) gebruikt mogen worden. Zo nodig wordt degene die de gegevens heeft ingebracht gevraagd of hergebruik akkoord is;
4. Indien noodzakelijk, wordt voor de samenwerking rond een specifieke casus een afzonderlijk en afgeschermd tijdelijk 'dossier' ingericht. Dit staat los van de 'zaakdossiers' van de deelnemende partijen. En er worden in het protocol afspraken gemaakt op welke termijn na afsluiten van de casus binnen het samenwerkingsverband dit dossier wordt vernietigd;
5. Indien er sprake is van een casusoverleg nemen uitsluitend partijen deel die noodzakelijk zijn om te komen tot een goede beoordeling van de situatie, bepalen van de aanpak en de uitvoering daarvan;
6. Een partij die in een bepaalde fase gegevens verstrekt behoudt de zeggenschap over het verdere gebruik van die gegevens voor een andere fase en voor andere doelen;
7. Partijen die bij de behandeling van een casus kennis nemen van gegevens afkomstig van een andere partij mogen deze gegevens niet 'automatisch' opnemen in het eigen dossier en gebruiken voor de eigen taken en werkzaamheden;
8. Betrokkenen bij het behandelen van de casus kunnen inzage hebben in dit 'dossier' ten behoeve van de specifieke doelen van de fase van behandeling van de casus,

maar mogen geen gegevens overnemen uit dit dossier zonder toestemming van degen die de gegevens heeft ingebracht;

9. Partijen die bij de behandeling van een casus kennis nemen van gegevens afkomstig van een andere partij mogen deze enkel opnemen in het eigen dossier en verder gebruiken voor de eigen taken als de verstrekkende partij dit afzonderlijk accordeert en uitsluitend voor de doelen die daarbij zijn afgesproken. Vuistregel is dat enkel partijen die een interventie (gaan) doen of een taak hebben in de uitvoeringsfase van de casus gegevens 'mee naar huis nemen' voor het uitvoeren van die interventie of taak;
10. Het streven blijft dat daar waar mogelijk de burger betrokken wordt bij en/of instemt met de activiteiten die bij het behandelen van casussen plaatsvinden;
11. Betrokkene wordt zo spoedig geïnformeerd dat hij of zij is aangemeld voor behandeling van de casus in het samenwerkingsverband, wat dit betekent, en op welke wijze deze zijn rechten kan uitoefenen. Deze informatieverplichting conform de AVG rust op de partij die de casus aanmeldt. Uitstel van het informeren van betrokkene(n) is slechts mogelijk als daar een inhoudelijke reden voor is, en een expliciete afweging aan ten grondslag ligt.

4.4.3 Bewaken van de rechtmatigheid en zorgvuldigheid van de gegevensverwerking tijdens het proces

Het bewaken van de rechtmatigheid van de gegevensverwerking en uitwisseling kent dus twee niveaus:

1. Invulling geven aan de zorgvuldigheidsafspraken die noodzakelijk zijn gegeven de aard van het werkproces;
2. Toetsen aan de hand van het protocol en het daarbij behorende werkproces of er specifieke beperkingen of randvoorwaarden zijn aan het uitwisselen van gegevens tussen de beoogde partners aan de specifieke casus op basis van de bestaande juridische kaders.

Dit bewaken vergt kennis en kunde die niet van alle deelnemers bij het behandelen van een casus verwacht kan worden. Daarom verdient het aanbeveling om ervoor te zorgen dat binnen een samenwerkingsverband mensen beschikbaar zijn die getraind en bevoegd zijn om het proces van samenwerking rond specifieke casussen vorm te geven en dat proces ook op deze punten te bewaken. Bij de zorg- en veiligheidshuizen wordt deze rol bijvoorbeeld vervuld door de procesregisseurs.

In bijlage 2 is bij wijze van voorbeeld het vier-fasemodel (werkproces) voor de behandeling van complexe casuïstiek van de zorg- en veiligheidshuizen opgenomen en de daarbij behorende uitwerking voor gegevensverwerking. In bijlage 3 en 4 zijn het modelconvenant en het modelprotocol voor de zorg- en veiligheidshuizen opgenomen.

4.5 Eisen aan het gebruik van ICT-systemen bij samenwerking

Ten behoeve van de samenwerking bij casuïstiek zullen partijen gebruik willen maken van een ICT-systeem. Dit kan of een systeem zijn van het samenwerkingsverband, of van een van de partijen. Op deze systemen zijn de algemene normen uit de AVG van

toepassing. Persoonsgegevens mogen dus alleen worden geregistreerd voor een duidelijk doel en op basis van een wettelijke grondslag. De registratie moet noodzakelijk zijn voor het bereiken van dat gezamenlijke doel. De gegevens moeten juist, actueel en niet bovenmatig zijn. De gegevens moeten worden beveiligd tegen verlies en onrechtmatig gebruik.

Voor de inrichting van deze systemen moeten de samenwerkingspartners een aantal uitgangspunten in acht nemen:

1. Indien gebruik wordt gemaakt van een ICT-systeem van een van de partners moet de informatiehuishouding voor ten behoeve van de samenwerking strikt gescheiden zijn van de informatiehuishouding voor andere taken van de organisatie;
2. Indien gebruik wordt gemaakt van een ICT-systeem van het samenwerkingsverband zelf en dit systeem wordt gebruikt voor verschillende taken van het samenwerkingsverband, moet er sprake zijn van een strikte scheiding tussen de informatiehuishoudingen voor de verschillende taken;
3. Registratie van inhoudelijke persoonsgegevens in het ICT-systeem blijft beperkt tot hetgeen noodzakelijk is voor de coördinatie of regie (procesregiedossier). Gegevens ten behoeve van de uitvoering van eigen taken registreren partijen in het eigen dossier, en worden niet opgeslagen in het ICT-systeem ten behoeve van de samenwerking;
4. Er dient sprake te zijn van een autorisatiebeleid waarin tevens duidelijk is wie daarop aanspreekbaar is, en het ICT-systeem moet autorisaties tot op het individuele medewerker niveau mogelijk maken;
5. Uitsluitend medewerkers die betrokken zijn bij een casus kunnen geautoriseerd worden om inzage te hebben in de persoonsgegevens van de casus en indien noodzakelijk deze te verwerken;
6. Medewerkers die betrokken zijn bij de casus mogen uitsluitend persoonsgegevens uit het gezamenlijke dossier overnemen in het eigen dossier indien de partij die de gegevens heeft ingebracht hiervoor toestemming heeft gegeven;
7. De afzonderlijke *casusdeelnemers* zijn ieder zelf verantwoordelijk voor de persoonsgegevens die zij inbrengen ten behoeve van een specifieke casus;
8. De beheerders van de ICT-voorzieningen hebben als zodanig de juridische positie van verwerker. De AVG vereist dat er de eisen, inclusief die ten aanzien van informatiebeveiliging die aan de verwerker worden gesteld in een contract of verwerkersovereenkomst zijn vastgelegd.

Bijlage 1:
Kernbegrippen uit de AVG

Betrokkene
De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is de man, de vrouw of de jeugdige van wie gegevens worden verwerkt. Zijn er meerdere namen opgenomen in één dossier, dan zijn er dus meerdere betrokkenen.

Persoonsgegevens
Persoonsgegevens zijn gegevens die een natuurlijk persoon identificeren of aan de hand waarvan een natuurlijke persoon geïdentificeerd kan worden (artikel 4 lid 1 AVG). Het gaat niet alleen om vertrouwelijke gegevens, maar om ieder gegeven dat is te herleiden tot een bepaald persoon.

Bijzondere persoonsgegevens
dit zijn persoonsgegevens die extra privacygevoelig zijn. Deze gegevens mogen alleen worden verwerkt als een wet dit uitdrukkelijk toestaat. Bijzondere persoonsgegevens zijn onder andere gegevens over de (geestelijke of lichamelijke) gezondheid, de seksuele geaardheid, de godsdienst of levensovertuiging, ras of etniciteit, politieke voorkeur en het lidmaatschap van een vakbond.

Strafrechtelijke persoonsgegevens
Dit zijn persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen en persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.

Verwerking
een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Beperken van de verwerking
het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken.

Verwerkingsverantwoordelijke
een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in Europese of nationale wetgeving worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Verwerker
een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Ontvanger
een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt.

Toestemming van de betrokkene
elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de hem of haar betreffende verwerking van persoonsgegevens aanvaardt;

Verantwoordingsplicht
de verantwoordingsplicht houdt in dat met documenten aangetoond moet worden dat juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van artikel 6 lid 1 AVG en kan dit ook aantonen. In artikel 6 lid 1 is bepaald dat persoonsgegevens verwerkt moeten worden op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (“rechtmatigheid, behoorlijkheid en transparantie”).

BIJLAGE 2:

VERTALING HANDVAT NAAR DE PRAKTIJK – EEN VOORBEELD

Verwerking van persoonsgegevens bij complexe casuïstiek in de zorg- en veiligheidshuizen

Deze bijlage bevat de geactualiseerde versie van het door de landelijke stuurgroep Zorg en Veiligheid vastgestelde document 'van juridisch kader naar operationeel proces; vertaling van handvat naar praktijk'.

Bij het lezen van deze bijlage is het van belang Hoofdstuk vier van dit handvat in het achterhoofd te houden. Hetgeen daar is beschreven met betrekking tot o.a. de juridische positie van samenwerkingsverbanden, de toetsing van de rechtmatigheid van de gegevensverwerking van de gegevensverwerking, de aard van het werkproces bij het behandelen van complexe casuïstiek en de uitgangspunten voor een zorgvuldige omgang met gegevens zijn vormen de basis voor hetgeen in deze bijlage is beschreven.

B2.1 Wettelijk kader, organisatie en doelstelling Zorg- en Veiligheidshuizen

Er is geen specifieke *wetgeving* waarin de organisatie, werkwijze en bevoegdheden van Veiligheidshuizen (ZVH) zijn vastgelegd. Een Zorg- en Veiligheidshuis is een (netwerk)samenwerkingsverband van *publiekrechtelijke* partijen zoals de politie, reclassering en gemeenten en *private* partijen zoals GGZ-instellingen voor de aanpak van keten-overstijgende problematiek. Dit betekent dat de deelnemende partijen hun eigen (wettelijke) verantwoordelijkheden en bevoegdheden behouden. Bij de overgang van de verantwoordelijkheid voor de coördinatie op de Zorg- en Veiligheidshuizen van de Rijksoverheid naar gemeenten per 1 januari 2013 is wel een beleidsdocument, het *Landelijk kader Veiligheidshuizen*[37] opgesteld (hierna: Landelijk kader, zie ook paragraaf 1.2). Het Landelijk kader is gemaakt dóór en vóór alle landelijke partners die deel uitmaken van het netwerksamenwerkingsverband 'Zorg- en Veiligheidshuis'.

Doelstelling
De doelstelling van de Zorg- en Veiligheidshuizen zoals geformuleerd in het Landelijk kader luidt:
'De doelstelling van de samenwerking in (Zorg- en) Veiligheidshuizen is het bijdragen aan veiligheid(sbeleving) als onderdeel van het integrale veiligheidsbeleid: het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en maatschappelijke uitval bij complexe problemen, door een combinatie van repressie, bestuurlijke interventie en zorg.'

[37] Voorheen werd er gesproken van Veiligheidshuizen. Tegenwoordig wordt de naam Zorg- en Veiligheidshuizen gebruikt om te benadrukken dat het gaat om casuïstiek waarbij de samenwerking tussen ketens van zorg, veiligheid en sociaal domein noodzakelijk is om tot goede oplossingen te komen.

Het Zorg- en Veiligheidshuis richt zich op:

- mensen die te maken hebben met meerdere problemen (multiproblem) die op meer dan één leefgebied spelen en (naar verwachting) leiden tot crimineel en/of overlast gevend gedrag of verder afglijden; ***en:***
- Samenwerking tussen meerdere ketens (minimaal dwang en drang) is nodig om tot een effectieve aanpak te komen; het is in de reguliere samenwerking tussen partners binnen één keten niet mogelijk om deze problematiek effectief aan te pakken; ***en:***
- De problematiek wordt beïnvloed door en heeft impact op het (gezins)systeem en/of de directe sociale leefomgeving (of wordt verwacht dat te gaan hebben); ***of:***
- Er is sprake van ernstige lokale of gebiedsgebonden veiligheidsproblematiek, die vraagt om een ketenoverstijgende aanpak. [38]

Daarnaast komt het voor dat ketenpartners gezamenlijke overleggen over "thematische" doelgroepen hebben ondergebracht bij het Veiligheidshuis zoals voor Veelplegers, Radicalisering, (risico)Jeugd, de Aanpak van Verwarde Personen, de Persoonsgerichte aanpak (PGA), het Justitieel Casus Overleg (JCO) en de Top-X-aanpak. Deze casussen voldoen niet per definitie aan de criteria van het Landelijk Kader voor complexe casuïstiek. In deze bijlage blijven deze overleggen buiten beschouwing. Zorg- en Veiligheidshuizen die dergelijke overleggen organiseren moeten bij de inrichting en uitvoering van die overleggen opnieuw kijken naar de juridische positionering van deze overleggen en hoe zij een rechtmatige en zorgvuldige gegevensverwerking voor deze overleggen organiseren. Dit handvat kan daarbij een leidraad zijn.

Juridische positie van het Zorg- en Veiligheidshuis

Zoals beschreven in paragraaf 4.2.1 van dit handvat heeft ook het Zorg- en Veiligheidshuis geen eigen wettelijke taak heeft en dus ook geen eigen wettelijke basis om persoonsgegevens te verwerken. Bij de samenwerking rond een specifieke casus behouden de deelnemende partijen hun eigen inhoudelijke bevoegdheden en verantwoordelijkheden voor de eigen taken. De consequentie hiervan is dat het Zorg- en Veiligheidshuis nooit op eigen titel gegevens verwerkt, maar de gegevens verwerkt ten behoeve van een of meerdere van de partijen in het samenwerkingsverband. Het faciliteert de deelnemende partijen bij de uitvoering van hun taken.

Procesregie en procesregisseur

De ondersteuning die het Zorg- en Veiligheidshuis biedt is die van *procesregie*. Zij organiseert namens een van de partrijen het proces om tot samenwerking en afstemming te omentussen partijen die noodzakelijk zijn om tot een goede oplossing van de casus te komen. De werkzaamheden ten behoeve van die procesregie worden uitgevoerd door de *procesregisseur* die daarbij ondersteund kan worden door administratief personeel.

Juridisch gezien handelt de procesregisseur dan namens de partij die de casus heeft aangemeld, of namens de partij die in de loop van het proces de casusregie op zich heeft

[38] Landelijk kader Veiligheidshuizen, p. 17

genomen. Kortheidshalve duiden we de partij namens wie de procesregisseur handelt aan met ‘de leidende partij’.

B2.2 Vier fasenmodel Zorg- en veiligheidshuizen

Binnen het werkproces van de Zorg en Veiligheidshuizen worden vier fasen onderscheiden, met ieder hun eigen doel:

- Aanmelden en intake: bepalen of een casus hier past of niet;
- Triage en voorbereiding casusoverleg: bepalen van een eerste toestandsbeeld, inzicht krijgen in reeds betrokken partijen, bepalen van het doel van een casusoverleg en te betrekken partijen;
- Casusoverleg: bepalen gemeenschappelijk ‘toestandsbeeld’ met de deelnemers om te komen tot plan van aanpak, afspraken over uitvoering en gegevensgebruik;
- Afschaling: afbouwen betrokkenheid en opschonen procesregiedossier bij het Zorg- en Veiligheidshuis.

B2.2.1 Fase 1 – aanmelding en intake

Aanmelding bij het Zorg- en Veiligheidshuis (ZVH) kan alleen door een partij die ook convenantpartner is en waarvoor de bevoegdheidsverlening aan de procesregisseurs in het ZVH om namens hen werkzaamheden uit te voeren op de juiste wijze is geregeld.

Tussen wie speelt de gegevensverwerking in deze fase zich af?
Deze fase speelt zich af tussen aanmeldende partijen en procesregisseur van het ZVH. Er vinden in deze fase nog geen verstrekkingen plaats aan andere partijen in het ZVH. De gegevensverwerking is de verantwoordelijkheid van de aanmeldende partij.

Taak en grondslag voor gegevensverwerking in deze fase
De procesregisseur ondersteunt de aanmeldende partij bij de goede uitvoering van diens (publiekrechtelijke) taak en handelt onder verantwoordelijkheid van de aanmeldende partij.
De procesregisseur is de facto uitvoerder voor de aanmeldende partner.

In het privacy-protocol is daartoe geregeld dat de procesregisseur handelt onder het gezag van de betreffende partijen.

Doel van gegevensverwerking in deze fase
Het doel van de gegevensverwerking door de procesregisseur in deze fase is:
T.b.v. de aanmelder bepalen of een casus thuis hoort in het ZVH. Of meer specifiek:
T.b.v. de aanmelder bepalen of een casus voldoet aan de criteria die in het samenwerkingsconvenant conform het landelijk kader veiligheidshuizen zijn afgesproken voor samenwerking in het zorg- en veiligheidshuis.

Activiteiten/werkzaamheden in deze stap
Voor de beoordeling wordt gekeken naar twee aspecten:

- Globale beoordeling op de formele criteria uit het landelijk kader:

- Er is sprake van meerdere problemen (multiproblem) die op meer dan één leefgebied spelen en (naar verwachting) leiden tot crimineel en/of overlastgevend gedrag of verder afglijden; en:
- Samenwerking tussen meerdere ketens (minimaal dwang en drang) is nodig om tot een effectieve aanpak te komen; het is in de reguliere samenwerking tussen partners binnen één keten niet mogelijk om deze problematiek effectief aan te pakken; en:
- De problematiek wordt beïnvloed door en heeft impact op het (gezins)systeem en/of de directe sociale leefomgeving (of wordt verwacht dat te gaan hebben); of:
- Er is sprake van ernstige lokale of gebiedsgebonden veiligheidsproblematiek, die vraagt om een keten-overstijgende aanpak

- Een inhoudelijke afweging op basis van de specifieke casusinformatie en inschatting van de aanmeldende partij, en van de procesregisseur over de mogelijke bijdrage van andere partners en organisaties aan het oplossen van de problematiek waarbij procesregisseur en aanmeldende partij hun deskundigheid en kennis van lokale situatie inzetten.
  Het is daarbij goed voorstelbaar dat een casus die op het eerste gezicht niet aan de formele criteria voldoet, bij nadere beschouwing toch thuis blijkt te horen in het ZVH, en vice versa.

De mogelijke uitkomsten van deze stap zijn:
- De casus wordt niet in behandeling genomen voor verdere procesregie. De procesregisseur verstrekt eventueel een advies aan de aanmelder. De aanmeldende partij handelt de casus zelf verder af, zoekt zelf bilateraal contact met een partner of organisatie, of meldt bijvoorbeeld aan bij een ander samenwerkingsverband of overlegtafel.
- Het is duidelijk een zaak voor het ZVH. De casus wordt in behandeling genomen voor de volgende processtap ‘Triage en voorbereiding casusoverleg’.
- Er is informatie nodig van andere partners of organisaties om te kunnen bepalen of de casus thuis hoort in het ZVH: de casus gaat door naar de volgende fase ‘Triage’ met als eerste doel door gerichte uitvraag bepalen of de casus in het ZVH thuis hoort.

Noodzakelijkheid van gegevens en gegevensdeling in de fase van aanmelding
De aanmeldende partij geeft de procesregisseur inzicht in de gegevens die noodzakelijk zijn om de beoordeling te maken. De principes van dataminimalisatie zijn van toepassing. Dat betekent dat de aanmelder niet zo maar alle informatie die hij heeft op tafel legt. Maar nadenkt over wat noodzakelijk is. Er is echter geen noodzaak voor anonimisering. Juist weten om wie het gaat en de context waarin het zich afspeelt kunnen van belang zijn voor de procesregisseur om de aanmeldende partij te helpen een goede afweging te maken.

Indien noodzakelijk voor een goede afweging kan de procesregisseur in deze fase ook checken of iemand al bij het eigen ZVH ‘in behandeling’ is. Echter uitsluitend de actieve

casussen en uitsluitend op ‘dat-gegevens’: is die in behandeling bij ons ja/nee, en zo ja wie is de procesregisseur.
Juridische basis in de fase van aanmelding

Grondslag conform AVG, Wpg WSJG en andere wetten
De grondslag voor gegevensverwerking door de procesregisseur in het zorg- en veiligheidshuis is dezelfde als de grondslag die geldt voor de aanmeldende partner. Die kan per partner verschillen. Bijvoorbeeld:

- Aanmelder Burgemeester, of College van B&W: Artikel 6 sub e, AVG
  Als de afdeling OOV namens de burgemeester, of als een andere gemeentelijke afdeling namens het College van B&W een casus aanbrengt is de grondslag voor gegevensverwerking door de procesregisseur artikel 6 sub e van de AVG: noodzakelijk voor de goede uitvoering van een taak van algemeen belang of de uitoefening van openbaar gezag, zoals opgenomen in die in de Gemeentewet, de WMO of andere wet expliciet is opgenomen. Welke publiekrechtelijke taak van toepassing is in een specifieke casus, is ter bepaling aan de gemeente. Bij de aanmelding moet duidelijk zijn in het kader van welke taak aanmelding plaats vindt.

In bijlage 4 is het model privacy-protocol voor Zorg- en veiligheidshuizen opgenomen. Artikel 5 van dat protocol gaat in op de grondslagen voor gegevensverwerking en uitwisseling die van toepassing zijn in de verschillende fasen van het werkproces van een ZVH. Artikel 6 van het protocol geeft een overzicht van de (wettelijke) taken die aan de orde kunnen zijn voor de elke partner indien zij betrokken zijn bij het behandelen van een casus in het ZVH. Ook geeft het protocol inzicht in de voorwaarden en beperkingen die van toepassing kunnen zijn bij de verwerking of uitwisseling van persoonsgegevens tussen partners, en de zorgvuldigheidsafspraken die tijdens het behandelen van casussen in acht moeten worden genomen. Het model privacy-protocol is gebaseerd op dit handvat en vastgesteld door de landelijke stuurgroep Zorg en Veiligheid. In deze stuurgroep zijn alle landelijke ketenpartners vertegenwoordigd.

Voor niet convenantpartners geldt dat zij niet kunnen fungeren als aanmeldende partij van een casus. Het ZVH kan namens hen geen gegevens verwerken t.b.v. procesregie omdat er geen bevoegdheidsverlening is geregeld. Een niet convenantpartner kan in specifieke casussen deelnemer zijn aan een casusoverleg, mits dit noodzakelijk is, en mits deze zich conformeert aan de afspraken in het privacy-protocol. Er zal in dat geval echter apart getoetst moeten worden op basis van welke taak en grondslag deze partij deelneemt, en of er beperkingen zijn aan de gegevens die deze partij kan verstrekken of ontvangen.

Bijzondere persoonsgegevens
In de praktijk van het ZVH is er veelal sprake van de verwerking van bijzondere persoonsgegevens in de zin van de AVG, ook in deze fase. Alle landelijke ketenpartners die genoemd zijn in het model privacy-protocol voor de ZVH zijn bevoegd om bijzondere persoonsgegevens te verwerken t.b.v. de eigen taak. Omdat in deze fase de procesregisseur handelt t.b.v. de taak, en onder de verantwoordelijkheid van de aanmelder van de casus, is dit geen belemmering zolang de aanmeldende partij een van

de landelijke ketenpartners is. Bij andere partners zal specifiek gekeken moeten worden of zij bijzondere en strafrechtelijke gegevens mogen verwerken.

Wettelijke persoonsgebonden nummers/BSN

Gebruik van wettelijke persoonsgebonden nummers als het BSN is aan strikte regels gebonden door de wetgever en mogen alleen gebruikt worden als dit expliciet in de wet is vermeld.

In het ZVH wordt het BSN vaak gebruikt om te borgen dat de gegevens die verschillende partners in brengen in fase 2 op dezelfde persoon betrekking hebben. Dit is toegestaan, mits de aanmeldende partner het BSN mag gebruiken. Dit zal meestal het geval zijn.

Geheimhoudingsplicht

De procesregisseur kan gezien worden als onderdeel van het team van de aanmeldende partner. In hoeverre de procesregisseur in deze fase inzicht mag hebben in gegevens van de aanmelder waar een geheimhouding op rust wordt bepaald door de interne regelgeving van de aanmelder.

Zorgvuldigheidsvereisten en rechten van de burger: registratie, bewaren en vernietigen, informatieplicht.

Informeren betrokkene

De betrokkene wordt bij voorkeur vooraf geïnformeerd dat een casus wordt aangemeld bij het ZVH, maar in ieder geval moet de betrokkene worden geïnformeerd zodra is vastgesteld dat de casus doorgaat naar fase 2 ‘Triage en voorbereiding casusoverleg’. Het informeren van de betrokkene is de verantwoordelijkheid van de aanmeldende partner. Hij informeert de burger over de stappen die in deze fase ondernomen worden, welke informatie bij wie wordt opgevraagd en waarom en welke rechten betrokkene heeft ten aanzien van gegevensverwerking. Waar nodig vraagt de aanmeldende partner toestemming voor het uitvragen van gegevens in de volgende fase. Afhankelijk van de werkafspraken kan dit ook gebeuren door de partner die de toestemming nodig heeft.

Als er inhoudelijke redenen zijn om dit op een later tijdstip te doen, dan is dit wel mogelijk. Leg dan de reden hiervan vast en geef aan op welk moment de betrokkene geïnformeerd gaat worden.

In sommige Zorg- en Veiligheidshuizen informeert het ZVH de betrokkene. Echter in die gevallen moet het steeds duidelijk zijn namens welke partij het ZVH betrokkene informeert.

Toegang tot gegevens in het systeem van het ZVH

In deze fase hebben uitsluitend de aanmeldende partner, de procesregisseur en eventueel de betrokken ondersteunende medewerker van het ZVH toegang tot de casusinformatie in het systeem ten behoeve van het zorg- en veiligheidshuis.

Gegevensgebruik en registratie afhankelijk van vervolg

Er kunnen zich meerdere situaties voordoen met verschillende gevolgen voor de verdere omgang met gegevens:

- Casus hoort niet thuis in ZVH
  Als de uitkomst van de deze fase is dat een casus niet thuishoort in het ZVH, vindt er ook geen registratie plaats in het systeem van het ZVH. De aanmeldende partij registreert de afhandeling in het eigen dossier. Als er al wel registratie in het ZVH systeem heeft plaats gevonden wordt deze weer vernietigd.

- Casus hoort wel thuis in ZVH: casus gaat door naar de fase van triage
  Als de uitkomst is dat de casus verder het proces van de samenwerking ingaat kunnen gegevens geregistreerd worden in het systeem van het ZVH t.b.v. de procesregie.
  De betrokkene wordt hierover geïnformeerd, alsmede over de volgende stappen en zijn haar rechten. Dit gebeurt door de aanmeldende partij of door de procesregisseur namens de aanmeldende partij.

- Informatie van andere partners of organisaties noodzakelijk om het goed te kunnen beoordelen
  Soms is het beeld niet helemaal duidelijk. Informatie van andere of organisaties kan dan nodig zijn om te kunnen beoordelen of een casus thuis hoort in het zorg- en veiligheidshuis of niet: casus gaat door naar de fase van triage om op basis van een gerichte uitvraag bij partners of andere organisaties om een betere afweging te kunnen maken.

B2.2.2 Fase 2 – Triage en voorbereiding casusoverleg

In deze stap handelt de procesregisseur nog steeds namens de aanmeldende partij. Op basis van de beschikbare informatie bereidt de procesregisseur het casusoverleg voor. Onderdeel van die voorbereiding is veelal het bevragen van partijen met de vraag of zij bekend zijn met de betrokkene, en of zij over informatie beschikken die relevant is voor de casus en die zij willen delen t.b.v. een integrale aanpak van de casus.

Wie verstrekt aan wie in deze fase?
Belangrijk uitgangspunt: formeel worden de partijen bevraagd namens de aanmeldende partij van de casus. Er is in deze fase dus formeel sprake van bilaterale uitwisseling van gegevens tussen aanmeldende partij en de betreffende partner ten behoeve van de triage en voorbereiding van een casusoverleg.

Conform de uitgangspunten van paragraaf 4.4.2 van dit handvat ‘Gegevensuitwisseling bij samenwerking rond casuïstiek in het zorg- en veiligheidsdomein’ rust er een strikte doelbinding op de gegevens die deelnemers in deze fase verstrekken. Dit betekent dat de procesregisseur de gegevens ontvangt namens de aanmelder ten behoeve van triage en het voorbereiden van het casusoverleg. Met andere woorden: om te komen tot een goede inschatting van de situatie en te bepalen welke partijen betrokken moeten worden bij een casusoverleg. Dit kan betekenen dat een deelnemer sommige informatie in deze fase wel wil delen met de aanmeldende partner ten behoeve van die specifieke doelen, maar pas later zal beslissen welke informatie ook met anderen gedeeld kan worden in

het casusoverleg en welke informatie gebruikt mag worden voor bijvoorbeeld het uitvoeren van een specifieke interventie.

Deze gegevens die in deze fase worden verstrekt, blijven dan ook binnen het ZVH en worden **niet** vastgelegd in het systeem van de aanmeldende partner.

Taak

- De taak die wordt uitgevoerd is de taak van de aanmelder.
- De procesregisseur ondersteunt de aanmelder bij de goede uitvoering van diens (publiekrechtelijke) taak en handelt onder verantwoordelijkheid van de aanmeldende partij.

In het privacy-protocol is daartoe geregeld dat de procesregisseur handelt onder het gezag van de betreffende partijen.

Doel van gegevensverwerking in deze fase
Het doel van de gegevensverwerking door de procesregisseur in deze fase is:

1. Triage – bepalen toestandsbeeld en verrijken van de informatie uit fase 1 met:

- In beeld brengen welke partijen al betrokken zijn of waarschijnlijk betrokken moeten worden bij het tot een oplossing komen voor de casus;
- In beeld brengen van de mogelijke bijdrage die deelnemers kunnen/willen leveren om tot een plan van aanpak te komen (casus-informatie, expertise, betrokkenheid uitvoering);
- In beeld brengen van de mogelijke bijdrage die deelnemers kunnen/willen leveren aan de uitvoering van een plan van aanpak (zorg, maatregelen, etc);
- In beeld brengen over welke relevante informatie deelnemers beschikken en de mogelijkheid/bereidheid die in te brengen in een casusoverleg.

2. Voorbereiden casusoverleg

- Bepalen van een zo concreet mogelijk doel voor het casusoverleg en bijvoorbeeld type beslissingen dat op basis van casusoverleg genomen moet worden;
- Bepalen van de relevante gespreksthema's voor het casusoverleg;
- Bepalen van de relevante deelnemers aan het casusoverleg, hun rol (expertise/adviseur, informant, beoogde uitvoerder interventies) en de van hen gevraagde inhoudelijke bijdrage;
- Bepalen of en zo ja welke informatie vóóraf ter inzage gegeven kan worden aan de deelnemers t.b.v. voorbereiding van het casusoverleg (let op het gaat om inzage geven. Casusbeschrijvingen mogen niet rondgestuurd worden omdat dan alsnog allerlei informatie in systemen van partijen terecht komt zonder dat duidelijk is of daar een noodzaak toe is);
- Bepalen op welke manier de burger betrokken wordt: wordt hij/zij uitgenodigd bij het overleg, vooraf, of achteraf geïnformeerd over de uitkomsten van het overleg;
- Maken van zorgvuldigheidsafspraken met betrekking tot de informatie die in het kader van het casusoverleg wordt gedeeld (doelbinding en gebruik, bewaren en

vernietigen, niemand neemt gegevens van een ander mee tenzij met toestemming) (zie ook paragraaf 4.4 van dit handvat).

Activiteiten/werkzaamheden in deze stap

In de praktijk zien we twee hoofdvarianten qua werkwijzen in deze fase:

a. De procesregisseur en aanmeldende partij voeren deze stap zelfstandig uit. De informatie van de deelnemers blijft vooralsnog binnen het Zorg- en Veiligheidshuis, en is uitsluitend ter inzage van de procesregisseur en aanmeldende partij.
b. De triage gebeurt in een in een algemeen overleg met alle ketenpartners ('weegtafel'). Op basis daarvan wordt een focusoverleg gepland met alleen de relevante partners, waarbij dieper op de casus wordt ingegaan.

- Variant b: niet toegestaan als standaardaanpak vanuit privacywetgeving
  Bij variant b vindt er eerst een generiek casusoverleg plaats met alle partners. Er wordt dan zonder toets vooraf casusinformatie over en weer gedeeld tussen alle ketenpartners, ook met ketenpartners die niet relevant zijn. Het ontbreken van die 'filter' maakt dat er niet voldaan kan worden aan het noodzakelijkheids- en proportionaliteitsvereiste uit de AVG. De gegevensdeling is per definitie niet proportioneel en daarmee niet toegestaan.
  In het landelijk kader zorg- en veiligheidshuizen was overigens al geconstateerd dat variant a de voorkeur heeft vanuit privacyoverwegingen.

De mogelijke uitkomsten van deze fase zijn

- Op basis van de informatie die in de triage naar boven komt wordt besloten de casus niet in behandeling te nemen. De procesregisseur verstrekt eventueel een advies aan de aanmeldende partij. De aanmeldende partij handelt zelf verder af, zoekt bilateraal contact met een van de partijen, of meldt aan bij een ander samenwerkingsverband of overlegtafel.
- Casusoverleg om tot een gemeenschappelijke aanpak te komen is noodzakelijk en zinvol. De voorbereiding van het casusoverleg wordt gestart.
- Er blijft twijfel of hier een gezamenlijke aanpak zinvol is een nadere beeldvorming met betrokken deelnemers is nodig. De voorbereiding van een casusoverleg wordt gestart. Doel van het casusoverleg is in eerste instantie om te bepalen of een gezamenlijke aanpak zinvol is. Dit kan geen standaardprocedure zijn omdat voorkomen moet worden dat ook casussen die helemaal niet in het ZVH thuis horen toch in een casusoverleg worden besproken.

Noodzakelijkheid van gegevens en gegevensdeling in de fase van triage en voorbereiding casusoverleg

- Uitzetten van de vraag bij partijen in het kader van triage
  Bij variant a verstrekt de procesregisseur namens de aanmeldende partij gegevens aan andere partijen die voor hen noodzakelijk zijn om te kunnen beoordelen of zij een bijdrage aan de oplossing van de casus kunnen leveren en zo ja op welke wijze. Dit zijn bilaterale verstrekkingen.

Welke partrijen benaderd worden en welke informatie daarvoor noodzakelijk is, wordt bepaald op basis van de inschatting van aanmeldende partij en procesregisseur.
Standaard alle partijen in het samenwerkingsverband benaderen is niet toegestaan omdat daarmee niet voldaan kan worden aan het noodzakelijkheids- en proportionaliteitsvereiste uit de AVG.

De te verstrekken informatie bij de vraag mag ook NAW-, inhoudelijke en contextgegevens bevatten omdat de bevraagde deelnemer anders geen inschatting kan maken of betrokkenheid zinvol is. Welke gegevens verstrekt kunnen worden bij het uitzetten van de vraag wordt bepaald door het kader van de aanmeldende partij.

- Checken of iemand bij een ander ZVH bekend is
  Indien noodzakelijk voor een goede afweging kan de procesregisseur in deze fase ook checken of iemand al bij het eigen of een ander ZVH 'in behandeling' is. Echter uitsluitend de actieve casussen en uitsluitend op 'dat-gegevens': 'is deze persoon in behandeling bij ons of een ander ZVH ja/nee?', 'en zo ja wie is de procesregisseur bij wie ik terecht kan om te bekijken of afstemming mogelijk is?.' Juridisch gezien stelt het vragende ZVH de vraag namens de aanmeldende partij, aan de leidende partij van de casus in het andere ZVH. De procesregisseur van dit laatste ZVH zal zo nodig met de leidende partij moeten beoordelen of er antwoord gegeven kan worden op de vraag.

  De vraag of er gegevens uitgewisseld kunnen worden tussen twee betrokken Zorg- en Veiligheidshuizen t.b.v. verdere behandeling, en zo ja welke, vraagt om een zorgvuldige afweging waarin elk ZVH de deelnemers die in het eigen ZVH betrokken zijn bij de casus zal moeten betrekken. De procesregisseurs zullen daarvoor afstemming moeten zoeken met de partijen die in het eigen ZVH betrokken zijn bij de casus.

- Verstrekken van informatie door partijen aan de procesregisseur
  In deze fase is er juridisch nog steeds sprake van bilaterale verstrekkingen van de deelnemers aan de aanmeldende partij.
  - De principes van dataminimalisatie zijn van toepassing;
  - De te verstrekken informatie aan de procesregisseur mag ook NAW-, inhoudelijke en contextgegevens bevatten;
  - Welke informatie een partij verstrekt wordt bepaald door het eigen juridisch kader van de betreffende deelnemer, de inhoudelijke problematiek, en de eigen inschatting van de noodzakelijke informatie;
  - De deelnemer kan eventueel aangeven dat bepaalde informatie wel of niet gedeeld mag worden in het casusoverleg;
  - De informatie is op dit moment slechts toegankelijk voor de procesregisseur en de aanmeldende partij. Uiteraard mag een deelnemer de door hem zelf verstrekte informatie in zien, maar niet de door anderen verstrekte informatie;

- Op de verstrekkingen in deze fase rust een strikte doelbinding. Dat betekent dat deze gegevens uitsluitend gebruikt worden voor de doelen van triage, voorbereiden casusoverleg zelf in het zorg- en veiligheidshuis. Ze worden uitsluitend geregistreerd in het systeem van het zorg- en veiligheidshuis. De aanmeldende partij mag deze niet registreren in het eigen systeem en niet gebruiken voor andere doelen.

Juridische basis in de fase van triage en de voorbereiding casusoverleg

Grondslag conform AVG, Wpg WSJG en andere wetten

De grondslag voor gegevensverwerking door de procesregisseur in deze fase is dezelfde als de grondslag die geldt voor de deelnemers die gegevens hebben aangedragen t.b.v. het casusoverleg. De grondslag voor de gegevensverwerking t.b.v. monitoring wordt ontleend aan de grondslag van de partner die de casusregie voert. Zoals gesteld in paragraaf B2.2.1 kan de (wettelijke) taak waaraan die grondslag wordt ontleend per partij verschillen.

Bijlage 4 bevat het Privacy protocol Zorg- en Veiligheidshuizen met daarin de artikelen met betrekking tot de grondslagen voor gegevensverwerking en uitwisseling en de wettelijke taken van de convenantpartners, die aan de orde kunnen zijn in het kader van het Zorg- en Veiligheidshuis (artikelen 5 en 6).

Bijzondere persoonsgegevens

Er zal veelal sprake zijn van de verwerking van bijzondere persoonsgegevens in de zin van de AVG in deze fase. Alle landelijke ketenpartners in het ZVH zijn bevoegd om bijzondere persoonsgegevens te verwerken t.b.v. de eigen taak. Omdat in deze fase de procesregisseur handelt t.b.v de taak, en onder de verantwoordelijkheid van de aanmeldende partij, is dit geen belemmering zolang de aanmeldende partij een van de landelijke ketenpartners is.

Indien andere dan ketenpartners betrokken worden kan dit een rol gaan spelen en moet er vooraf getoetst worden in hoeverre dit een belemmering vormt.

Wettelijke persoonsgebonden nummers**/BSN**

Gebruik van wettelijke persoonsgebonden nummers als het BSN is aan strikte regels gebonden door de wetgever en mogen alleen gebruikt worden als dit expliciet in de wet is vermeld.

In het ZVH wordt het BSN vaak gebruikt om te borgen dat de gegevens die verschillende partners in brengen in fase 2 op dezelfde persoon betrekking hebben. Dit is toegestaan, mits de aanmeldende partner het BSN mag gebruiken. Dit zal meestal het geval zijn.

Geheimhoudingsplicht

De procesregisseur kan gezien worden als onderdeel van het team van de aanmeldende partij. In hoeverre de procesregisseur in deze fase inzicht mag hebben in gegevens van

de aanmelder waar een geheimhouding op rust wordt bepaald door de interne regelgeving van de aanmelder.

De geheimhoudingsplicht van de aanmeldende partij kan wel een rol spelen op het moment dat de procesregisseur namens de aanmeldende partij gegevens gaat delen met anderen in het kader van de uitvraag t.b.v. de triage. Dan is het zaak dat voor de procesregisseur duidelijk is welke gegevens in dat kader gedeeld mogen worden.

Daarnaast kan een geheimhoudingsverplichting in de weg staan bij een of meerdere partijen die gevraagd worden gegevens te delen t.b.v. triage. De bevraagde partij zal dan een afweging moeten maken of gegevens t.b.v. triage verstrekt kunnen worden – al dan niet met toestemming van de betrokkene. Deze afweging is altijd aan de bevraagde partij. De procesregisseur zal in de vraagstelling aan moeten geven namens wie, t.b.v. welke taak, en met welk doel hij gegevens vraagt en waarom de gevraagde gegevens noodzakelijk zijn, om de bevraagde partij in staat te stellen deze afweging goed te maken.

Zorgvuldigheidsvereisten en rechten van de burger: registratie, bewaren en vernietigen, informatieplicht

<u>Informeren betrokkene</u>
Het informeren van de betrokkene is de verantwoordelijkheid van de aanmeldende partner. Hij informeert de burger over de stappen die in deze fase ondernomen worden, welke informatie bij wie wordt opgevraagd en waarom. Waar nodig vraagt de aanmeldende partner toestemming voor het uitvragen van gegevens. Afhankelijk van de werkafspraken kan dit ook gebeuren door de deelnemer die de toestemming nodig heeft.

Als er inhoudelijke redenen zijn om dit op een later tijdstip te doen, dan is dit wel mogelijk. Leg dan de reden hiervan vast en geef aan op welk moment de betrokkene geïnformeerd gaat worden.

In sommige Zorg- en Veiligheidshuizen informeert het ZVH de betrokkene. Echter in die gevallen moet het steeds duidelijk zijn namens welke partij het ZVH betrokkene informeert.

<u>Toegang tot gegevens in het systeem van het ZVH</u>
In deze fase hebben nog steeds uitsluitend de aanmeldende partij, de procesregisseur en eventueel de betrokken ondersteunende medewerker van het Zorg- en Veiligheidshuis toegang tot de casusinformatie in het systeem van het Zorg- en Veiligheidshuis. Er vindt uitsluitend registratie plaats in het systeem van het Zorg- en Veiligheidshuis, en niet in het systeem van de aanmeldende partij.

Betrokken partijen hebben geen inzage in elkaars gegevens die t.b.v. de casus zijn verstrekt. En elke patrij behoudt de zeggenschap over de gegevens die hij heeft aangedragen t.b.v. de triage en het casusoverleg, en of hij gegevens ter inzage wil geven aan andere partijen die bij de casus betrokken zijn.

Afhankelijk van de uitkomst van deze fase zijn er verschillende gevolgen voor de verdere omgang met gegevens:

- Casus blijkt alsnog niet thuis te horen in het ZVH
  Als de uitkomst van de triage is dat een casus toch niet thuishoort in het ZVH, wordt de casusinformatie weer uit het systeem van het ZVH verwijderd. De aanmeldende partij registreert de afhandeling in het eigen dossier. Er blijft hooguit 'administratieve maar niet tot de persoon herleidbare informatie' achter in het systeem van het ZVH.

  De gegevens die deelnemers hebben aangeleverd t.b.v. de triage mag niet terecht komen in de systemen van andere deelnemers, ook niet in die van de aanmeldende partner.

- Casus gaat door naar casusoverleg met specifieke deelnemers
  Als de uitkomst van de triage is dat er een casusoverleg wordt voorbereid, wordt tevens bepaald of deelnemers beschikbare informatie mogen inzien en zo ja welke. Uitsluitend de deelnemers aan het casusoverleg hebben inzage. Daarbij is het mogelijk dat sommige deelnemers een voorbehoud maken ten aan zien van het delen van gegevens met een of meerdere deelnemers.

  De betrokkene wordt geïnformeerd over de uitkomst van de triage, alsmede over doel en gespreksthema's en de deelnemers in het casusoverleg. Betrokkene wordt ook geïnformeerd over zijn/haar rechten. Dit gebeurt door de aanmeldende partner of door de procesregisseur namens de aanmeldende partner (volgt uit verantwoordelijkheid).

- Casus hoort beter thuis op een andere overlegtafel, bijvoorbeeld ZSM
  Als de uitkomst van de triage is dat een casus beter thuishoort op een andere tafel of bij een ander samenwerkingsverband, wordt de casusinformatie weer uit het systeem van het ZVH verwijderd. Er blijft hooguit 'administratieve maar niet tot de persoon herleidbare informatie' achter in het systeem van het ZVH.
  De aanmeldende partij is verantwoordelijk voor de aanmelding bij de andere overlegtafel en registreert de afhandeling in het eigen dossier. Indien de procesregisseur van het ZVH dit doet, doet hij dat namens de aanmeldende partij, en kan dit alleen als daar in de bevoegdheidsverlening rekening mee is gehouden.

  Inbreng van gegevens uit de triagefase bij de andere overlegtafel, mag uitsluitend indien de partij die de informatie heeft ingebracht dit accordeert.

B2.2.3 Fase 3 – Casusoverleg in het ZVH

In de fase van casusoverleg gaan de professionals van de relevante partijen met elkaar in gesprek om te komen tot een gezamenlijk 'toestandsbeeld' van de casus en tot een voorstel voor een plan van aanpak. Aan het eind worden afspraken gemaakt over wie wat gaat doen en wie welke gegevens mag gebruiken om zijn taak in het plan van aanpak uit te kunnen voeren. Ook wordt afgesproken wie de casusregisseur wordt, of

een casus terug komt in een vervolgoverleg (monitoring) en met wie, of dat de casus kan worden afgeschaald.

In de praktijk gaat het meestal om meerdere casus-overleggen waarbij de casus gevolgd wordt totdat besloten wordt tot afschaling.

Pas in deze fase kunnen deelnemers aan het casusoverleg via het systeem van het Zorg- en Veiligheidshuis inzage krijgen in gegevens die andere deelnemers hebben aangedragen, voor zover die noodzakelijk zijn voor dat overleg. Deelnemers mogen deze gegevens niet overnemen in het eigen systeem. Veel Zorg- en Veiligheidshuizen kiezen er voor om deelnemers helemaal geen inzage vooraf te geven. Pas tijdens het casusoverleg bepalen deelnemers of en zo ja welke gegevens zij in willen brengen in het licht van de doelen van het casusoverleg.

Op de gegevens rust een strikte doelbinding. Dat wil zegen dat ze uitsluitend gebruikt mogen worden voor het overleg. Pas aan het eind van het overleg – als duidelijk is wie welke activiteiten gaat uitvoeren in het kader van het plan van aanpak – wordt ook afgesproken wie welke gegevens mag ‘meenemen’ voor het uitvoeren van die activiteiten. Daarbij heeft elke deelnemer nog steeds de zeggenschap over de gegevens die hij heeft aangedragen en kan bepalen aan wie hij wil verstrekken t.b.v. de uitvoering van het plan van aanpak. Dat betekent ook dat een deelnemer die geen rol heeft in de uitvoering van het plan van aanpak geen persoonsgegevens meeneemt naar zijn eigen organisatie. Ook is het in principe mogelijk dat een deelnemer persoonsgegevens ter beschikking heeft gesteld t.b.v. triage en casusoverleg, maar deze niet wil verstrekken voor bepaalde activiteiten uit het plan van aanpak.

Wie verstrekt aan wie in deze fase?
Het organiseren en faciliteren van het casusoverleg doet de procesregisseur namens de aanmeldende partij. Echter de gegevensverwerking, i.c. het inzicht geven aan de deelnemers in het casusoverleg in de daarvoor noodzakelijke gegevens gebeurt formeel namens de afzonderlijke deelnemers die gegevens hebben verstrekt t.b.v. triage en casusoverleg.

Dit zelfde geldt als de procesregisseur uitvoering geeft aan de afspraken uit het casusoverleg om deelnemers te voorzien van de voor hen noodzakelijke gegevens bij de uitvoering van het plan van aanpak.

Indien de procesregisseur ondersteuning biedt aan de partij die de casusregie heeft voor de monitoring van de casus, dan handelt hij formeel namens de casusregisseur en zijn verstrekkingen van andere deelnemers t.b.v. de casusregie formeel verstrekkingen aan de casusregisseur.

De formele werkelijkheid wordt hier complex, zonder dat die voor de praktische invulling grote gevolgen hoeft te hebben. Wel betekent het dat hier in de bevoegdheidsverlening aan de medewerkers van het Zorg- en Veiligheidshuis rekening mee gehouden moet

worden en dat de procesregisseur zich moet houden aan de aanwijzingen die deelnemers mee geven bij het verstrekken van gegevens.

Indien de conclusie van het casusoverleg is dat de casus wordt overgedragen naar een andere overlegtafel dan kan dit alleen via een van de bij de casus betrokken partijen. Indien deze partij daarbij ook gegevens wil overdragen van andere betrokken partijen, dan kan dit alleen als deze partijen daarvoor toestemming geven. Indien een medewerker van het ZVH dit namens een van de partijen doet, moet hier in de bevoegdheidsverlening rekening mee worden gehouden. Formeel is het echter een aanmelding van de betreffende partij aan een andere overlegtafel (zie ook par 4.4 van dit handvat).

Taak
Met het organiseren en faciliteren van het casusoverleg ondersteunt de procesregisseur aanmelder of casusregisseur bij de goede uitvoering van diens publiekrechtelijke of andere wettelijke taak, en handelt onder verantwoordelijkheid van de aanmelder of casusregisseur.

De gegevensverwerking zoals boven beschreven doet de procesregisseur in principe ten behoeve van de publiekrechtelijke of wettelijke taak van de partij die de gegevens ter beschikking heeft gesteld.

In het privacy-protocol is daartoe geregeld dat de procesregisseur handelt onder het gezag van de betreffende partijen.

Doel van gegevensverwerking in de fase van casusoverleg
Het doel van gegevensverwerking in deze fase is:
1. Ervoor zorgen dat de deelnemers aan het casusoverleg beschikken over de gegevens die noodzakelijk zijn om een gezamenlijk toestandsbeeld van de casus te kunnen bepalen en tot een plan van aanpak te komen;
2. Ervoor zorgen dat iedere deelnemer die een rol heeft bij de uitvoering van het plan van aanpak, kan beschikken over de voor zijn rol noodzakelijke gegevens voor zover de partij die de gegevens heeft ingebracht dit accordeert;
3. Indien de casus wordt doorverwezen naar een andere instantie die niet bij het casusoverleg betrokken is, of naar een andere overlegtafel, afspraken maken over wie de aanmelding doet en welke informatie aan deze instantie of overlegtafel kan worden over gedragen;
4. Indien het een vervolg casusoverleg betreft: zicht houden op start en de afsluiting van onderdelen van het plan van aanpak en of de doelen zijn behaald, en
5. Zicht houden op ontwikkelingen die impact hebben op de casus en op eventuele stagnaties in de uitvoering van het plan van aanpak, en
6. Indien nodig komen tot bijstelling van het plan van aanpak.

Activiteiten/werkzaamheden in deze stap
Deelnemers inzicht geven in de voor het casusoverleg noodzakelijke persoonsgegevens onder uitdrukkelijke doelbinding.

Bespreken van de casus in het casusoverleg, opstellen van plan van aanpak, afspraken maken over monitoring met ondersteuning van het Zorg- en Veiligheidshuis, afspraken maken over wie welke gegevens mag ontvangen t.b.v. de uitvoering van zijn activiteiten in het plan van aanpak of welke gegevens verstrekt mogen worden aan een andere instantie of overlegtafel t.b.v. de aanpak van de casus. De zeggenschap ligt daarbij bij de deelnemers die gegevens hebben aangedragen.

Uitvoering geven aan de uitkomst van het casusoverleg ook m.b.t. de daarin afgesproken gegevensverstrekkingen t.b.v. de uitvoering van het plan van aanpak.

Indien is afgesproken dat het zorg- en veiligheidshuis ondersteunt bij de casusregie: monitoring van uitvoering van het plan van aanpak namens de casusregisseur. Ook hier geldt dat in de bevoegdheidsverlening dit geregeld moet zijn. En indien afgesproken: voorbereiden van vervolg casusoverleggen.

Noodzakelijkheid van gegevens en gegevensdeling in de fase van casusoverleg
De noodzakelijkheidsbeoordeling ten aanzien van welke deelnemers welke gegevens mogen inzien heeft plaats gevonden in de triage fase.

De noodzakelijkheidsafweging ten aanzien van gegevensverstrekking ten behoeve van het bepalen van het toestandsbeeld en de noodzakelijkheidsafweging ten aanzien van de gegevensverstrekking aan bepaalde partijen ten behoeve van de uitvoering van hun aandeel in het plan van aanpak vindt plaats in het casusoverleg. Waarbij elke deelnemer zijn eigen verantwoordelijkheid heeft.

Belangrijk is dat op de gegevens een strikte doelbinding rust. Dat wil zegen dat ze uitsluitend gebruikt mogen worden voor het overleg. En dat niemand gegevens van andere deelnemers ‘mee neemt’ naar de eigen organisatie zonder toestemming daarvoor van de organisatie die de gegevens heeft ingebracht.

Juridische basis in de fase van casusoverleg

<u>Grondslag conform AVG, Wpg WSJG en andere wetten</u>
De grondslag voor gegevensverwerking door de procesregisseur in deze fase is dezelfde als de grondslag die geldt voor de deelnemers die gegevens hebben aangedragen t.b.v. het casusoverleg. De grondslag voor de gegevensverwerking t.b.v. monitoring wordt ontleend aan de grondslag van de partner die de casusregie voert. Zoals gesteld in paragraaf B2.2.1 kan de (wettelijke) taak waaraan die grondslag wordt ontleend per partij verschillen.
Bijlage 4 bevat het privacy protocol Zorg- en Veiligheidshuizen met daarin de artikelen met betrekking tot de grondslagen voor gegevensverwerking en uitwisseling en de wettelijke taken van de convenantpartners, die aan de orde kunnen zijn in het kader van het Zorg- en Veiligheidshuis (artikelen 5 en 6).

<u>Bijzondere persoonsgegevens</u>

Er zal veelal sprake zijn van de verwerking van bijzondere persoonsgegevens in de zin van de AVG in deze fase. Alle landelijke kernpartners in het ZVH zijn bevoegd om bijzondere persoonsgegevens te verwerken t.b.v. de eigen taak. De procesregisseur handelt t.b.v de taak, en onder de verantwoordelijkheid van de aanmeldende partij of casusregisseur, is dit geen belemmering zolang deze een van de landelijke kernpartners is.

Indien andere dan de landelijke kernpartners betrokken worden, bijvoorbeeld een woningcorporatie, kan hier een belemmering optreden. Wellicht dat deze geen bijzondere persoonsgegevens mag inzien. Dit moet in de voorbereiding van het casusoverleg getoetst worden.

Wettelijke persoonsgebonden nummers/BSN

Gebruik van wettelijke persoonsgebonden nummers als het BSN is aan strikte regels gebonden door de wetgever en mogen alleen gebruikt worden als dit expliciet in de wet is vermeld.

In het ZVH wordt het BSN vaak gebruikt om te borgen dat de gegevens die verschillende partners in brengen op dezelfde persoon betrekking hebben. Dit is toegestaan, mits de aanmeldende partner het BSN mag gebruiken. Dit zal meestal het geval zijn.

Geheimhoudingsplicht

In deze fase is het vooral aan de deelnemers om te bepalen welke gegevens zij als dan niet met toestemming van betrokkene willen inbrengen in het casusoverleg, onder de strikte doelbinding van het casusoverleg: bepalen van gezamenlijk toestandsbeeld en komen tot een plan van aanpak. Op basis van de uitkomst van het casusoverleg kan elke deelnemer opnieuw een afweging maken of, en t.b.v. wiens activiteiten in het kader van het plan van aanpak, de geheimhouding – al dan niet met toestemming van betrokkene - kan worden doorbroken.

Zorgvuldigheidsvereisten en rechten van de burger: registratie, bewaren en vernietigen, informatieplicht

Informeren betrokkene

Het informeren van de betrokkene is de verantwoordelijkheid van de aanmeldende partij, dan wel de partij die de casusregie voert. Hij informeert de burger over de uitkomsten van het overleg, en aan wie welke gegevens verstrekt zullen worden en waarom.

Als er inhoudelijke redenen zijn om dit op een later tijdstip te doen, dan is dit wel mogelijk. Leg dan de reden hiervan vast en geef aan op welk moment de betrokkene geïnformeerd gaat worden.

In sommige Zorg- en Veiligheidshuizen informeert het ZVH de betrokkene. Echter in die gevallen moet het steeds duidelijk zijn namens welke partij het ZVH betrokkene informeert.

Toegang tot gegevens

In deze fase kunnen voor het eerst meerdere deelnemers inzage in de gegevens in het systeem van het zorg- en veiligheidshuis krijgen. Uitsluitend de deelnemers aan het casusoverleg krijgen inzage voor zover noodzakelijk voor het casusoverleg. Er rust een strikte doelbinding op de gegevens. Dat wil zeggen dat ze uitsluitend gebruikt mogen worden voor het overleg. Pas aan het eind van het overleg – als duidelijk is wie welke activiteiten gaat uitvoeren in het kader van het plan van aanpak – wordt ook afgesproken wie welke gegevens mag 'meenemen' voor het uitvoeren van het eigen aandeel in het plan van aanpak. Daarbij heeft elke deelnemer nog steeds de zeggenschap over de gegevens die hij heeft aangedragen t.b.v. de triage en het casusoverleg en aan wie hij wil verstrekken t.b.v. de uitvoering van het plan van aanpak.

Dat betekent dat een deelnemer die geen rol heeft in de uitvoering van het plan van aanpak geen persoonsgegevens meeneemt naar zijn eigen organisatie. Ook is het in principe mogelijk dat een deelnemer persoonsgegevens ter beschikking heeft gesteld t.b.v. triage en casusoverleg, maar deze niet wil verstrekken voor bepaalde activiteiten uit het plan van aanpak.

Er kunnen zich meerdere situaties voordoen met verschillende gevolgen voor de verdere omgang met gegevens:

- Casus blijkt alsnog niet thuis te horen in het ZVH
  Als de uitkomst van het casusoverleg is dat een casus alsnog niet thuishoort in het ZVH, wordt de casusinformatie weer uit het systeem van het ZVH verwijderd. De aanmeldende partij registreert de afhandeling in het eigen dossier. Er blijft hooguit 'administratieve maar niet tot de persoon herleidbare informatie' achter in het systeem van het ZVH.

  De gegevens die deelnemers hebben aangeleverd t.b.v. de triage mag niet terecht komen in de systemen van andere deelnemers, ook niet in die van de aanmeldende partij.

  De betrokkene wordt geïnformeerd dat de gegevens worden verwijderd uit het systeem van het zorg- en veiligheidshuis.

- Er wordt een aanpak vastgesteld en een casusregisseur aangewezen, monitoring via casusoverleg ondersteund door het ZVH
  Indien er een plan van aanpak wordt vastgesteld en een casusregisseur wordt aangewezen, worden ook afspraken gemaakt welke deelnemers welke gegevens mee mogen nemen t.b.v. de uitvoering van hun aandeel in het plan van aanpak. Het doel van het monitoren wordt geëxpliciteerd, en er worden afspraken gemaakt welke gegevens nog in het systeem van het zorg- en veiligheidshuis blijven t.b.v. de monitoring. Deelnemers die geen rol bij de uitvoering hebben 'nemen geen gegevens mee' naar de eigen organisatie.

- Casus hoort beter thuis op een andere overlegtafel, bijvoorbeeld ZSM

Als de uitkomst van het casusoverleg is dat een casus beter thuishoort op een andere tafel wordt de casusinformatie weer uit het systeem van het ZVH verwijderd. Er blijft hooguit 'administratieve maar niet tot de persoon herleidbare informatie' achter in het systeem van het ZVH. De aanmeldende partij van de casus registreert de afhandeling in zijn eigen systeem.

In het casusoverleg wordt bepaald welke partij verantwoordelijk is voor de aanmelding bij de andere overlegtafel. Vaak zal dit de oorspronkelijke aanmeldende partij van de casus zijn. Indien de procesregisseur van het ZVH dit doet, doet hij dat namens de betreffende partij, en kan dit alleen als daar in de bevoegdheidsverlening rekening mee is gehouden.

De gegevens die deelnemers hebben ingebracht in de verschillende fasen van het proces mogen niet terecht komen in de systemen van andere deelnemers, ook niet die van de aanmeldende partij.

Inbreng van gegevens bij de andere overlegtafel, mag uitsluitend met toestemming van de deelnemer die de informatie heeft ingebracht.

- Er wordt besloten tot afschaling bij het zorg- en veiligheidshuis
  Bijvoorbeeld omdat de aanpak en inbreng van betrokken deelnemers voldoende is uitgekristalliseerd, en de betrokkenheid van het zorg- en veiligheidshuis niet langer nodig wordt geacht. De casus gaat door naar fase 4: afschaling.

B2.2.4 Fase 4 – Afschaling

In deze fase wordt de betrokkenheid van het zorg- en veiligheidshuis afgebouwd, bijvoorbeeld omdat de aanpak en inbreng van betrokken deelnemers voldoende is uitgekristalliseerd, en de betrokkenheid van het zorg- en veiligheidshuis niet langer nodig wordt geacht. In deze fase schoont de procesregisseur het dossier dat in het systeem van het zorg- en veiligheidshuis is aangelegd ten behoeve van de procesregie, van alle niet langer noodzakelijke informatie. Er blijft na verloop van tijd uitsluitend administratieve informatie achter in het systeem van het zorg- en veiligheidshuis.

Het kan van belang zijn om in de eerste fase na besluit tot afschaling het dossier nog beschikbaar te hebben, voor het geval er terugval optreedt. Het is echter juridisch niet houdbaar, dat dossiers nog heel lang na afschaling in de systemen van het ZVH bewaard blijven. Daarom is afschaling in stappen nodig:

Stap 1: 0-6 maanden na besluit tot afschaling. Dossier blijft actief in het systeem van het ZVH voor het geval dat er terugval optreedt en er een nieuw casusoverleg nodig is.

Stap 2: 6-12 maanden na besluit tot afschaling. Het dossier wordt gearchiveerd. Nog wel is vindbaar dát een persoon behandeld is in het ZVH, maar het dossier zelf is niet meer toegankelijk. Indien noodzakelijk kan dit wel weer toegankelijk gemaakt worden. In de

regel neemt de manager van het Zorg- en Veiligheidshuis de beslissing of een dossier weer actief gemaakt wordt.

Stap 3: 1 jaar na besluit tot afschaling. Het dossier wordt geheel uit het systeem van het Zorg- en Veiligheidshuis verwijderd. Uitsluitend 'niet tot personen herleidbare gegevens' blijven achter.

In uitzonderingsgevallen kan tot andere termijnen worden besloten, mits de motivatie wordt vastgelegd en er een termijn wordt vastgesteld voor herbeoordeling. Die termijn voor herbeoordeling is maximaal 6 maanden.

De procesregisseur handelt namens de partij die op het moment van afschaling de regie heeft over de casus. Dat kan de aanmeldende partij zijn, het kan ook een andere partij zijn die in fase 3 de regie heeft overgenomen. Deze partij is ook verantwoordelijk voor het besluit om af te wijken van de termijnen in de afschalingsfase en de herbeoordeling.

Bewaartermijnen volgens de AVG
De wet geeft geen duidelijke bewaartermijnen voor het bewaren en vernietigen van het dossier dat ontstaat ten behoeve van dit type samenwerking. De AVG stelt dan dat het niet langer dan noodzakelijk mag worden bewaard. De keuzen die in dit geval voor de Zorg- en Veiligheidshuizen zijn gemaakt zijn gebaseerd op een inschatting van de bruikbaarheid van informatie na verloop van tijd. Vandaar echter ook de mogelijkheid om hier in sommige gevallen gemotiveerd van af te wijken.

Wie verstrekt aan wie in deze fase?
In principe is er in deze fase nauwelijks sprake meer van verstrekkingen of het delen van gegevens. Het gaat om het opschonen van het dossier in het zorg- en veiligheidshuis. Deelnemers die betrokken zijn hebben de voor hen noodzakelijke gegevens al in fase 3 gekregen en zullen deze bewaren volgens de voor hen geldende bewaartermijnen.

Taak
De procesregisseur ondersteunt de aanmelder/casusregisseur bij de goede uitvoering van diens publiekrechtelijke of andere wettelijke taak, en handelt onder verantwoordelijkheid van de aanmelder of casusregisseur.

In het privacy-protocol is daartoe geregeld dat de procesregisseur handelt onder het gezag van de betreffende partij.

Doel van gegevensverwerking in deze fase
Het algemene doel van gegevensverwerking in deze fase is:
1. Ervoor zorgen dat de casus in de systemen van het zorg- en veiligheidshuis wordt afgesloten en alle niet noodzakelijke gegevens van de casus worden vernietigd.
2. Voor zover dat nog niet is gebeurd, gegevens die noodzakelijk zijn voor de uitvoering van hun werkzaamheden in het vervolg van de casus overdragen aan de betreffende deelnemers eventueel met toestemming van de deelnemer die de gegevens heeft ingebracht.

3. Subdoelen per stap van afschaling:
   Stap 1en 2: In geval van terugval binnen een jaar de samenwerking weer snel op kunnen starten;
   Stap 2: Het beschermen van de persoonlijke levenssfeer van de betrokkene door de toegankelijkheid tot het dossier te beperken.
   Stap 3: Het beschermen van de persoonlijke levenssfeer van de betrokkene door het dossier te vernietigen.

Activiteiten/werkzaamheden in deze stap
De procesregisseur zorgt dat de gefaseerde afschaling plaats vindt.
De procesregisseur informeert de betrokken deelnemers dat het dossier is opgeschoond, en afhankelijk van de stap in het afschalingsproces, welke gegevens in het systeem van het zorg- en veiligheidshuis bewaard blijven en voor hoe lang.
De partij die op het moment van het besluit van afschaling de casusregie heeft informeert de betrokkene dat het dossier in het ZVH is vernietigd en waar hij terecht kan als hij alsnog gebruik wil maken van zijn rechten.

Noodzakelijkheid van gegevens en gegevensdeling in de fase van afschaling
De gegevens die noodzakelijk zijn om te bewaren verschillen per afschalingsstap.
Stap 1: procesregiedossier
Stap 2: een beperkte set administratieve gegevens blijft zichtbaar:
- Casusnummer
- Identificerende gegevens
- Naam aanmelder en organisatie
- Naam casusregisseur ten tijde van afschaling en organisatie
  Het procesregiedossier is niet meer toegankelijk voor medewerkers.

Stap 3: Alleen niet tot personen herleidbare gegevens voor managementdoeleinden.

Juridische basis in de afschalingsfase

<u>Grondslag conform AVG, Wpg WSJG en andere wetten</u>
De grondslag voor gegevensverwerking door de procesregisseur in deze fase is dezelfde als de grondslag die geldt voor de deelnemers die gegevens hebben aangedragen t.b.v. het casusoverleg. De grondslag voor de gegevensverwerking t.b.v. monitoring wordt ontleend aan de grondslag van de partner die de casusregie voert. Zoals gesteld in paragraaf B2.2.1 kan de (wettelijke) taak waaraan die grondslag wordt ontleend per partij verschillen.

Bijlage 4 bevat het Privacy protocol van de Zorg- en Veiligheidshuizen met daarin de artikelen met betrekking tot de grondslagen voor gegevensverwerking en uitwisseling en de wettelijke taken van de convenantpartners, die aan de orde kunnen zijn in het kader van het Zorg- en Veiligheidshuis (artikelen 5 en 6).

<u>Bijzondere persoonsgegevens, persoonsgebonden nummers en BSN</u>
Of bijzondere persoonsgegevens en of het BSN in het dossier gebruikt verwerkt mogen

worden is reeds in de eerdere fasen van het werkproces bepaald. Die vraag speelt hier dus niet meer. Het gaat hier immers om het verwijderen van gegevens.

Geheimhoudingsplicht

Er blijven aan het eind van de afschaling geen gegevens achter in het dossier die onder een geheimhoudingsverplichting vallen van een van de deelnemers.

Zorgvuldigheidsvereisten en rechten van de burger: registratie, bewaren en vernietigen, informatieplicht

Informeren betrokkene

Het informeren van de betrokkene is de verantwoordelijkheid van de partner die de casusregie heeft. De casusregisseur informeert de burger over de afschaling, de opschoning van het dossier, de gegevens die in het dossier achter blijven en hoe lang deze bewaard blijven. Daarnaast informeren zij betrokkene over zijn/haar rechten en bij wie betrokkene na vernietiging van het dossier in het ZVH terecht kan voor de uitoefening van zijn rechten.

B2.6 Doelen per fase

Fase aanmelding en intake:

- Bepalen of een casus in het ZVH thuis hoort of niet;
- T.b.v. de aanmelder bepalen of een casus voldoet aan de criteria die in het samenwerkingsconvenant conform het landelijk kader veiligheidshuizen zijn afgesproken voor samenwerking in het zorg- en veiligheidshuis;
- Adviseren van de aanmelder over aanpak.

Fase 2 triage en voorbereiding casusoverleg:

2a. Triage – bepalen toestandsbeeld en verrijken van de informatie uit fase 1 met:

- In beeld brengen welke partijen al betrokken zijn of waarschijnlijk betrokken moeten worden bij het tot een oplossing komen voor de casus;
- In beeld brengen van de mogelijke bijdrage die deelnemers kunnen/willen leveren om tot een plan van aanpak te komen (casus-informatie, expertise, betrokkenheid uitvoering);
- In beeld brengen van de mogelijke bijdrage die deelnemers kunnen/willen leveren aan de uitvoering van een plan van aanpak (zorg, maatregelen, etc);
- In beeld brengen over welke relevante informatie deelnemers beschikken en de mogelijkheid/bereidheid die in te brengen in een casusoverleg.

2b. Voorbereiden casusoverleg

- Bepalen van een zo concreet mogelijk doel voor het casusoverleg en bijvoorbeeld type beslissingen dat op basis van casusoverleg genomen moet worden;
- Bepalen van de relevante gespreksthema's voor het casusoverleg;

- Bepalen van de relevante deelnemers aan het casusoverleg, hun rol (expertise/adviseur, informant, beoogde uitvoerder interventies) en de van hen gevraagde inhoudelijke bijdrage;
- Bepalen of en zo ja welke informatie vóóraf ter inzage gegeven kan worden aan de deelnemers t.b.v. voorbereiding van het casusoverleg;
- Bepalen op welke manier de burger betrokken wordt: wordt hij/zij uitgenodigd bij het overleg, vooraf, of achteraf geïnformeerd over de uitkomsten van het overleg;
- Maken van zorgvuldigheidsafspraken met betrekking tot de informatie die in het kader van het casusoverleg wordt gedeeld (doelbinding en gebruik, bewaren en vernietigen, niemand neemt gegevens van een ander mee tenzij met toestemming) (zie ook paragraaf 4.4 van dit handvat);
- Adviseren van de aanmelder.

<u>Fase casusoverleg in ZVH:</u>

- Ervoor zorgen dat de deelnemers aan het casusoverleg beschikken over de gegevens die noodzakelijk zijn om een gezamenlijk toestandsbeeld van de casus te kunnen bepalen en tot een plan van aanpak te komen;
- Ervoor zorgen dat iedere deelnemer die een rol heeft bij de uitvoering van het plan van aanpak, kan beschikken over de voor zijn rol noodzakelijke gegevens voor zover de partij die de gegevens heeft ingebracht dit accordeert;
- Indien de casus wordt doorverwezen naar een andere instantie die niet bij het casusoverleg betrokken is, of naar een andere overlegtafel, afspraken maken over wie de aanmelding doet en welke informatie aan deze instantie of overlegtafel kan worden over gedragen;
- Indien het een vervolg casusoverleg betreft: zicht houden op start en de afsluiting van onderdelen van het plan van aanpak en of de doelen zijn behaald, en
- Zicht houden op ontwikkelingen die impact hebben op de casus en op eventuele stagnaties in de uitvoering van het plan van aanpak, en
- Indien nodig komen tot bijstelling van het plan van aanpak.

<u>Fase afschaling:</u>

Het algemene doel van gegevensverwerking in deze fase is:

1. Ervoor zorgen dat de casus in de systemen van het zorg- en veiligheidshuis wordt afgesloten en alle niet noodzakelijke gegevens van de casus worden vernietigd.
2. Voor zover dat nog niet is gebeurd, gegevens die noodzakelijk zijn voor de uitvoering van hun werkzaamheden in het vervolg van de casus overdragen aan de betreffende deelnemers eventueel met toestemming van de deelnemer die de gegevens heeft ingebracht.
3. Subdoelen per stap van afschaling:
   Stap 1en 2: In geval van terugval binnen een jaar de samenwerking weer snel op kunnen starten;
   Stap 2: Het beschermen van de persoonlijke levenssfeer van de betrokkene door de toegankelijkheid tot het dossier te beperken.
   Stap 3: Het beschermen van de persoonlijke levenssfeer van de betrokkene door het dossier te vernietigen.

BIJLAGE 3:

TEMPLATE SAMENWERKINGSCONVENANT

Convenant Samenwerking tussen ketenpartners in zorg- en veiligheidshuis […]

Context:

Met dit Samenwerkingsconvenant worden afspraken rondom de samenwerking tussen verschillende partijen in het zorg- en veiligheidshuis geformaliseerd en vastgelegd. Uit dit Samenwerkingsconvenant dient duidelijk te blijken wie, met welk doel en met welke inzet deelneemt aan het zorg- en veiligheidshuis, alsook wie waarover, op welk niveau, regie voert en hoe besluitvorming plaatsvindt.

In dit Samenwerkingsconvenant zijn de standaard onderdelen van een (meer-partijen) overeenkomst opgenomen. De verdeling van verantwoordelijkheden, rechten en plichten is uiteindelijk aan partijen zelf in te vullen. Waar nodig is door middel van gearceerde teksten ruimte voor maatwerk of toelichting gegeven op de keuzemogelijkheden en de mogelijke gevolgen van die keuzes. Dit is echter niet uitputtend en dient door iedere partij die deelneemt aan dit Convenant zelf nader te worden onderzocht.

Formuleringen, begrippen en andere specifieke zorg- en veiligheidshuis-gerelateerde termen zijn afgeleid uit het Handvat “Gegevensuitwisseling in het zorg- en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen”, versie 1.1. 7 juli 2017 (hierna ‘Handvat’ genoemd) en het Landelijk Kader Veiligheidshuizen. Ook wordt aangesloten bij de werkwijze zoals in het Handvat beschreven. Daarnaast is geput uit een aantal reeds bestaande samenwerkingsconvenanten voor wat betreft onder meer de structuur van het zorg- en veiligheidshuis. Wanneer u in uw zorg- en veiligheidshuis een andere structuur voor de samenwerking hebt ingericht en/of wilt handhaven, dient u dit template daarop aan te passen en (schriftelijk) te onderbouwen hoe u de verantwoordelijkheden van de verschillende aangesloten ketenpartners alsnog dekkend waarborgt.

Met dit template wordt beoogd te voorzien in een zo volledig sluitend model van samenwerkingsafspraken in het zorg- en veiligheidshuis. Desalniettemin dient u het template te zien en te gebruiken in het licht van uw eigen taken, bevoegdheden en verantwoordelijkheden.

Dit template is tot stand gekomen in samenwerking tussen (privacy)adviseurs van verschillende landelijke partijen, Considerati en het Ministerie van Justitie en Veiligheid.

Convenant samenwerking tussen ketenpartners zorg- en veiligheidshuis [*naam*]

De ondergetekenden:

Toelichting:

Voor de aanwijzing van partijen die mogelijk partij bij deze samenwerkingsafspraken kunnen zijn, wordt in eerste instantie verwezen naar het Landelijk Kader Veiligheidshuizen. Het betreft in ieder geval de sleutelpartners in de aanpak van Complexe Multi-problematiek, te weten de Gemeente(n), het Openbaar Ministerie, de lokale eenheid van de Nationale Politie, het 3RO, de Raad voor de Kinderbescherming, Jeugdzorg, de GGZ, Gehandicaptenzorg en DJI. Zie voor een aanvulling hierop ook Veilig Thuis.

(in geval van één gemeente)

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente [naam gemeente].

(in geval van meerdere gemeenten)

De colleges van burgemeester en wethouders en de burgemeesters, ieder voor zover het zijn bevoegdheid betreft, van de gemeenten:

[*Gemeente A*];

[*Gemeente B*];

[*Gemeente C*];

[*Gemeente D*],

verder *afzonderlijk* aangeduid als 'Partij' of 'Gemeente' *en gezamenlijk als 'Gemeenten'*,

en

en

de Korpschef van politie [naam], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie]*

het College van procureurs-generaal, hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

[*naam partij A*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

[*naam partij B*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

[*naam partij C, GGZ*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

[*naam partij i.c. GGD*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

[*naam partij E i.c. private partij*], statutair gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

(*Indien afkorting van naam van de partij dient te worden gebruikt in het convenant, deze afkorting vermelden in de beschrijving door middel van de volgende zinsnede: (verder aangeduid als '…'))*

hierna afzonderlijk te noemen 'Partij' en gezamenlijk, inclusief Gemeente[n], te noemen 'Partijen',

de volgende overwegingen in aanmerking nemende:

Toelichting:

De overwegingen beschrijven wat de bedoelingen van partijen zijn met het aangaan van de overeenkomst. Dit is van belang voor de uitleg van de overeenkomst, met name indien niet duidelijk is wat er wordt bedoeld met een zin of zinsdeel. De overwegingen geven dus de context aan de samenwerking die niet per sé in de afspraken terugkomt, maar wel van belang is voor de partijen die aan de samenwerking deelnemen met betrekking tot het uitleggen van de afspraken. Onderstaande overwegingen zijn niet uitputtend en dienen als leidraad, maar zullen voor de meeste zorg- en

veiligheidshuizen van toepassing zijn. Partijen kunnen overwegingen weghalen of toevoegen indien die (niet) van belang zijn voor hun specifieke vorm(en) van samenwerking. Van belang bij het formuleren van overwegingen is dat deze duidelijk zijn beschreven en consequent woordgebruik en formuleringen toepassen.

Woorden met hoofdletter geschreven hebben altijd de betekenis die aan dat woord in dit Protocol is toegekend.

- Partijen in het kader van samenwerking op het gebied van integrale veiligheid en complexe casuïstiek het zorg- en veiligheidshuis [*naam zorg- en veiligheidshuis*] (hierna: 'zorg- en veiligheidshuis') hebben opgezet;
- De Rijksoverheid per 1 januari 2013 de verantwoordelijkheid voor de veiligheidshuizen van het Openbaar Ministerie naar de zetelgemeente van de Veiligheidsregio heeft overgedragen, waardoor de gemeentelijke strategische regierol verder versterkt is;
- Er bestuurlijke afspraken zijn gemaakt tussen het toenmalige Ministerie van Veiligheid en Justitie en de Vereniging Nederlandse Gemeenten, namens alle Nederlandse gemeenten, rondom de financiële bijdrage van de Rijksoverheid aan de Veiligheidshuizen, die zijn opgenomen als bijlage bij de brief van de Staatssecretaris van Veiligheid en Justitie d.d. 2 augustus 2012, kenmerk 287830;
- Van belang is dat Partijen personele bijdragen blijven leveren in de vorm van partnerbijdragen aan triage- en/of casus-overleggen en/of structurele deelname aan het zorg- en veiligheidshuis;
- Partijen hun eigen bevoegdheden houden met betrekking tot de in het zorg- en veiligheidshuis besproken casuïstiek en het zorg- en veiligheidshuis de uitoefening van deze bevoegdheden niet overneemt, maar stuurt op een integrale en gezamenlijke inzet van Partijen;
- Partijen nadrukkelijk het belang en de noodzaak onderschrijven dat alleen door domein-overstijgende en gezamenlijke inzet de complexe probleemsituaties die in het zorg- en veiligheidshuis worden voorgelegd, kunnen worden opgelost of verbeterd;
- Hiervoor enkele belangrijke voorwaarden zijn geformuleerd, waaronder de bestendiging van de goede aansluiting met en de herkenbaarheid voor alle Partijen van het zorg- en veiligheidshuis en de bestuurlijke borging van de domein-overstijgende aanpak binnen het zorgdomein, justitieel domein en gemeentelijk domein;
- Partijen te kennen hebben gegeven de huidige samenwerking bestuurlijk-juridisch, beheersmatig, organisatorisch en financieel te willen versterken;
- Partijen hebben aangegeven alle onderlinge samenwerkingsafspraken rondom Complexe Multi-Problematiek schriftelijk te willen vastleggen in een samenwerkingsconvenant;

[U dient een verwijzing te maken naar de afspraken rondom de verwerking van persoonsgegevens, daarvoor dient u een keuze te maken tussen de volgende twee opties:

- [OPTIE 1: in geval van één protocol] De afspraken rondom de verwerking van persoonsgegevens in het Privacy Protocol Integrale Veiligheid en Complexe Multi-Problematiek zijn vastgelegd, dat integraal onderdeel is van dit samenwerkingsconvenant;
- [OPTIE 2: in geval van meerdere doelen voor samenwerking en dus meerdere Privacy Protocollen] De afspraken rondom de verwerking van persoonsgegevens per doel van de samenwerking in afzonderlijke Privacy Protocollen zijn vastgelegd, die onderdeel zijn van dit samenwerkingsconvenant, te weten: [puntsgewijs overzicht van protocollen];
- In de Landelijke Stuurgroep zorg en Veiligheid vindt met landelijke vertegenwoordigers overleg plaats. In dit landelijke overleg worden de koers en landelijke prioriteiten van de zorg- en veiligheidshuizen bepaald. Het landelijke overleg biedt hierbij kaders die op regionaal niveau

nader worden ingevuld. Het landelijke niveau biedt een opschalingsmogelijkheid voor regionale ontwikkelpunten. Op landelijk niveau worden landelijke trends en ontwikkelpunten gesignaleerd en waar nodig oplossingen bedacht. Elke partner is verantwoordelijk voor afstemming en uitvoering van afspraken binnen de eigen organisatie op zowel landelijk als regionaal niveau.

- De managers van de zorg- en veiligheidshuizen zijn verenigd in de Vereniging van managers zorg- en veiligheidshuizen;
- Dit samenwerkingsconvenant verder wordt aangehaald als 'het Convenant'.

verklaren te zijn overeengekomen:

Artikel1. Definities

Toelichting:

In dit artikel volgen de definities. Definities worden gebruik om veelgebruikte termen of zinnen af te korten, waarmee in de rest van de overeenkomst niet iedere keer de gehele zin of omschrijving dient te worden gebruikt. Dit bevordert de leesbaarheid van de overeenkomst. De definities zijn afkomstig uit het Landelijk Kader Veiligheidshuizen en uit het vertaaldocument "Van handvat naar praktijk".

In dit Convenant en de daarbij behorende bijlage(n) wordt verstaan onder:

1.1. Strategische Regie: de coördinatie van regionale samenwerking in het zorg- en veiligheidshuis, verbinding van verschillende ketens en afstemming met andere lokale en regionale samenwerkingsverbanden, organisaties en overlegtafels.
1.2. Procesregie: Het uitvoeren van werkzaamheden gericht op de totstandkoming van samenwerking tussen Partijen bij het behandelen van één specifieke Casus en de ondersteuning van de Casusregisseur bij de uitvoering van het plan van aanpak;
1.3. Casusregie: het uitvoeren van werkzaamheden gericht het bewaren van de onderlinge samenhang bij het uitvoeren van het plan van aanpak bij het behandelen van één specifieke Casus;
1.4. Casus: een geval of situatie dat of die voldoet aan de criteria voor complexe casuïstiek zoals geformuleerd in Bijlage 2, en die is aangemeld bij het zorg- en veiligheidshuis ter beoordeling en eventuele bespreking in het Casusoverleg;
1.5. Betrokkene: de natuurlijke persoon op wie informatie, waaronder persoonsgegevens zoals beschreven in het Privacy Protocol, betrekking heeft;
1.6. Derde: de natuurlijk persoon of rechtspersoon, niet zijnde de betrokkene, noch één der partijen.
1.7. Aanmelding en Intake: het voordragen van een Casus door één der Partijen en het uitwisselen van informatie, waaronder Persoonsgegevens, tussen de Procesregisseur van het zorg- en zorg- en veiligheidshuis en de aanmeldende Partij ter toetsing of de Casus in aanmerking komt voor behandeling in het zorg- en veiligheidshuis.
1.8. Triage: het proces waarbij relevante Partijen worden bevraagd om te komen tot een nadere afweging ten aanzien van de routering van de casus, tot een bepaling van het doel en de thema's van een eventueel Casusoverleg, en tot een afweging welke Partijen relevant zijn om te betrekken bij een Casusoverleg.
1.9. Casusoverleg: fase waarin overleg plaats vindt door Partijen gericht op de totstandkoming van een plan van aanpak, afstemming tijdens de uitvoering daarvan, en het beoordelen of Casus kan worden afgeschaald;

1.10. Afschaling: fase die volgt op het besluit in het Casusoverleg dat de betrokkenheid van het zorg- en veiligheidshuis niet langer nodig is, waarin het dossier dat in het systeem van het zorg- en veiligheidshuis is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie, en uiteindelijk verdwijnt uit het systeem van het zorg- en veiligheidshuis;
1.11. Procesregisseur: de medewerker van het zorg- veiligheidshuis die namens een van de Partijen is belast met de werkzaamheden in artikel 12;
1.12. Casusregisseur: de medewerker van een van de Partijen die is belast met de taken in artikel 13;
1.13. Manager: de persoon die is belast met de taken zoals geformuleerd in Artikel 11;
1.14. Stuurgroep: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 4;
1.15. Partneroverleg: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 6;
1.16. Landelijk Kader: het 'Landelijk Kader Veiligheidshuizen – vóór en dóór partners', opgesteld door het Ministerie van Veiligheid en Justitie, d.d. januari 2013.
1.17. Jaarplan: het door de Stuurgroep op grond van Artikel 4.4 vastgestelde plan betreffende de operationele en inhoudelijke kaders en het financieel en inhoudelijk beleid van het zorg- en veiligheidshuis.
1.18. Werkproces: het door het Partneroverleg op grond van Artikel 6.6 [*of, indien gebruik wordt gemaakt van de optionele artikelen, Artikel 6.7 of 6.8*], onder c, vastgestelde proces voor samenwerking in het zorg- en veiligheidshuis, waaronder het proces omtrent en het delen van informatie en het op- en afschalen van een Casus.

Artikel 2. Doel en Functie zorg- en veiligheidshuis

2.1. Het zorg- en veiligheidshuis is een samenwerkingsverband waarin zorg- en strafpartners en gemeenten, onder eenduidige regie, werken aan complexe zorg- en veiligheidsproblemen. De doelstelling van de samenwerking is bijdragen aan de algemene veiligheid, het verbeteren van de persoonlijke situatie, het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en/of maatschappelijke uitval. Dit gebeurt door een combinatie van repressie, bestuurlijke interventies en zorg, hetgeen moet worden gezien als een zwaarwegend algemeen belang.

2.2. Om het onder 2.1 geformuleerde doel te bereiken heeft het zorg- en veiligheidshuis drie functies:

a) Het faciliteren en regisseren van Casusoverleggen waar complexe casuïstiek wordt besproken;
b) Het functioneren als expertisecentrum voor multidisciplinaire zorg- en veiligheidsproblematiek en vraagbaak voor ketenpartners en professionals;
c) Het signaleren van relevante trends en ontwikkelingen en (strategisch) adviseren van bestuurders en sleutelpartners;

***Toelichting**:*

Bovenstaande doelen zullen voor ieder en zorg- en veiligheidshuis gelijk zijn. Het zorg- en veiligheidshuis kan daarnaast echter ook een functie vervullen om de samenwerking op aanvullende gebieden te faciliteren, zoals op de onderwerpen re-integratie ex-gedetineerden, nazorg jeugd of radicalisering. Deze zijn niet meegenomen in dit Convenant, maar kunnen door een nieuw artikel 2.3. worden toegevoegd:

"2.3. Daarnaast heeft het zorg- en veiligheidshuis tot functie het behandelen van casuïstiek op de gebieden;
a. Nazorg jeugd
b. Nazorg ex-gedetineerden
c. Radicalisering
d. …

Let wel: Voor iedere vorm van samenwerking dient een apart Privacy Protocol te worden opgesteld, danwel het meegeleverde Privacy Protocol te worden uitgebreid. Ook dient te worden getoetst of het Werkproces zoals beschreven voor complexe casuïstiek aanpassingen behoeft voor deze nieuwe vormen van samenwerking.

Artikel 3. Structuur zorg- en veiligheidshuis

3.1. Het zorg- en veiligheidshuis kent de volgende structuur:
   a. de Stuurgroep;
   b. het Partneroverleg of een ander tactisch overleg;
   c. Het Casusoverleg;
   d. de Manager;
   e. de Procesregisseur;
   f. de Casusregisseur;
   g. ondersteunend Personeel.

***Toelichting**:*

Voor zover bekend heeft ieder zorg- en veiligheidshuis zeker één of meer ondersteunende personeelsleden. Dit zijn bijvoorbeeld administratieve medewerkers. Ook hun rol en verhouding tot Partijen dient duidelijk uit dit Convenant te volgen.

Wanneer uw eigen zorg- en veiligheidshuis een andere structuur kent of andere terminologie gebruikt voor de verschillende onderdelen van het samenwerkingsverband, benoem deze dan in dit artikel en beleg hun rollen en taken verderop in het Convenant en sluit het Privacy Protocol hierop aan.

Artikel 4. Stuurgroep

4.1. Het zorg- en veiligheidshuis heeft een Stuurgroep die fungeert als het bestuur van het zorg- en veiligheidshuis. De Stuurgroep is verantwoordelijk voor de Strategische Regie van het zorg- en veiligheidshuis;
4.2. De Stuurgroep komt ten minste iedere [*aantal*] weken bij elkaar. De vergaderingen van de Stuurgroep vinden in beginsel plaats op locatie van het zorg- en veiligheidshuis.
4.3. De Stuurgroep bestaat uit vertegenwoordigers van een aantal Partijen, te weten:
   - de burgemeester van een (beheers)gemeente [*naam gemeente*]. Deze treedt tevens op als voorzitter van de Stuurgroep;
   - één wethouder voor Jeugd, aangewezen door […];
   - één wethouder voor Maatschappelijke Zorg, aangewezen door […];
   - één (Hoofd)officier van Justitie, aangewezen door […];
   - één politiechef van de politie, eenheid […], aangewezen door […];
   - de Manager van het zorg- en veiligheidshuis;

- één secretaris, aangewezen door […].
- […]

Toelichting:
bovenstaande is een voorstel voor de invulling van de Stuurgroep. Ieder zorg- en veiligheidshuis kan zelf de samenstelling van de Stuurgroep bepalen. De aanwijzing is van belang om de mandaatverlening te verduidelijken: ieder lid van de Stuurgroep moet mandaat hebben vanuit de bevoegde persoon in de eigen organisatie om deel te nemen en bindende besluiten te nemen in de Stuurgroep)

4.4. De Stuurgroep is verantwoordelijk voor het in het kader van de Strategische Regie opstellen van operationele en beleidsmatige kaders voor de opdracht van het zorg- en veiligheidshuis in de vorm van een Jaarplan, en beslist over eventueel bijstellen/afwijken van deze kaders. Jaarlijks stelt de Stuurgroep in een Jaarplan een inhoudelijk en financieel beleid vast als opdracht voor het zorg- en veiligheidshuis. Dit Jaarplan bevat ten minste de volgende onderdelen:
   a) Langetermijnvisie;
   b) Prioriteiten voor het betreffende kalenderjaar;
   c) Begroting en jaarrekening inclusief jaarverslag.
   d) Het borgen van de kwaliteit van de samenwerking, de plannen van aanpak en de informatiebeveiliging en de evaluatie daarvan;
   e) *[…]*
   f) *[…]*

Toelichting:
Voeg hier eventuele andere onderwerpen toe die in het Jaarplan dienen te worden opgenomen.

4.5. De Stuurgroep heeft daarnaast de volgende taken en bevoegdheden:
   a. het Werkproces indien nodig op hoofdlijnen aanpassen;
   b. besluiten met betrekking tot personeel nemen die het zorg- en veiligheidshuis aangaan;
   c. besluiten omtrent toetreding van nieuwe organisaties tot dit Convenant.

Toelichting:
Denk hier ook aan de bevoegdheid tot het namens Partijen aangaan van overeenkomsten. Waar wordt deze bevoegdheid belegd? Wat als een product of dienst van een derde partij wordt ingekocht – wie mag dan namens Partijen tekenen? Dit kan bijvoorbeeld ook bij de Manager of het Partneroverleg worden belegd (zie verderop). Daarbij is van belang dat de afgevaardigden in de Stuurgroep, het Partneroverleg en de Manager tekenbevoegd moeten zijn namens alle Partijen, hiertoe moet dan ook het juiste mandaat worden verleend indien die bevoegdheid er nu nog niet is.

4.6. De Gemeente(n) en het Partneroverleg ontvangen het Jaarplan ter informatie uiterlijk [*aantal*] weken na vaststelling daarvan door de Stuurgroep.

4.7. De secretaris van de Stuurgroep is verantwoordelijk voor het organiseren van de vergaderingen, het samenstellen van de agenda op basis van inbreng vanuit het Partneroverleg en de leden van de Stuurgroep en het opstellen en verspreiden van het verslag van de betreffende vergadering.

Artikel 5. Besluitvorming Stuurgroep

5.1. De Stuurgroep neemt besluiten over de Strategische Regie in het zorg- en veiligheidshuis. Incidentele strategische besluiten komen toe aan het Partneroverleg.

5.2. Voorafgaand aan het nemen van besluiten vraagt de Stuurgroep om inbreng van Partijen.

5.3. De Stuurgroep houdt bij het nemen van besluiten rekening met de uitkomsten van de overleggen van de Landelijke Stuurgroep Zorg en Veiligheid.
5.4. Besluiten worden genomen met een meerderheid van stemmen en zijn bindend voor alle Partijen die aan dit Convenant deelnemen, voor zover niet strijdig met de wettelijke taken, bevoegdheden en beroepsnormen van Partijen. Er wordt gestreefd naar consensus.
5.5. Bij afwezigheid van een lid van de Stuurgroep wordt die Partij verzocht schriftelijk inbreng te leveren rondom de geagendeerde besluiten. Zonder schriftelijke inbreng worden besluiten die deze Partij in belangrijke mate kunnen treffen niet genomen, tot die Partij gehoord is.
5.6. Indien de Stuurgroep niet tot een besluit kan komen, wordt de aangelegenheid ter beslissing voorgelegd aan [*naam]**.* Dat geldt ook voor gevallen waarin een verhoging van de financiële of personele bijdrage van Partijen of beperking van de dienstverlening van het zorg- en veiligheidshuis aan de orde is. De Voorzitter kan besluiten de colleges van burgemeesters en wethouders en andere Partijen hiervoor te benaderen. Voor het overige wordt de Stuurgroep door de bevoegde gezagen gemandateerd om besluiten te nemen.

Toelichting *:
Hier is ruimte om een overkoepelend orgaan een rol te geven in bepaalde besluitvorming

5.7. De Stuurgroep informeert [*naam*] over de besluitvorming in de Stuurgroep. De secretaris van de Stuurgroep informeert het Partneroverleg schriftelijk over de in de Stuurgroep genomen besluiten.

***Toelichting**:*
Denk hier aan andere gremia die op de hoogte moeten zijn van besluiten in de Stuurgroep, zoals de Gemeenteraad. Een dergelijke informatievoorziening kan hier worden ingebouwd. Verder is het van belang dat het Partneroverleg op de hoogte is van besluiten in de Stuurgroep.

5.8. De vergaderingen van de Stuurgroep zijn niet openbaar.

Artikel 6. Partneroverleg

Toelichting:

Ieder zorg- en veiligheidshuis dient een overlegstructuur in te richten die op tactisch niveau sturing geeft aan het zorg- en veiligheidshuis. In dit Convenant is voor deze overlegstructuur gekozen voor de naam Partneroverleg.

6.1. Partijen in het zorg- en veiligheidshuis voeren ter uitvoering van de in artikel 2 bepaalde doeleinden onderling overleg op tactisch niveau: het 'Partneroverleg'.
6.2. Het Partneroverleg vindt iedere [*aantal*] weken plaats, of wanneer een Partij hier een verzoek toe indient.
6.3. Het Partneroverleg bestaat uit:
a) één afgevaardigde van iedere Partij of door de Procesregisseur aangewezen Partijen;
b) de Procesregisseur;
c) de Manager van het zorg- en veiligheidshuis; en
d) een secretaris.
6.4. *(OPTIONEEL)* Eénmaal per jaar vindt een overleg plaats waarvoor alle Partijen worden uitgenodigd, *daar wordt het jaarverslag en de jaarrekening vastgesteld en wordt het Jaarplan besproken.*
6.5. De secretaris is aangewezen door [*naam Partij*] en valt onder verantwoordelijkheid van [*naam Partij*].

6.6. De afgevaardigden van Partijen hebben het mandaat of de machtiging om op tactisch niveau sturing te geven aan de operationele processen van het zorg- en veiligheidshuis en besluiten te nemen met betrekking tot uitvoering van de onder Artikel 6.8 geformuleerde taken.

Toelichting:

In het Partneroverleg en de Stuurgroep wordt geen casuïstiek besproken maar beleidsaangelegenheden. Aangezien niet alle convenantpartners op stuurgroepniveau vertegenwoordigd zijn, is de suggestie om éénmaal per jaar alle partners in een jaarvergadering bijeen te roepen om daar de resultaten van het afgelopen jaar en de ontwikkelingen voor het komende jaar te bespreken. In verband met het AVG vereiste van transparantie en accountability is het voorstel dat de verwerking van persoonsgegevens als onderwerp onderdeel uitmaakt van het jaarverslag en het jaarplan.

6.7. *(OPTIONEEL in geval van meerdere gemeenten)* De Gemeenten laten zich gezamenlijk vertegenwoordigen door één gemeentelijke afgevaardigde, die door de afzonderlijke gemeenten is gemandateerd om namens hen inbreng te leveren en gemachtigd om besluiten te nemen in het Partneroverleg. Bestaande taken en verantwoordelijkheden van de vertegenwoordigde Gemeenten blijven onverlet. In navolging van de Algemene Verordening Gegevensbescherming kan de verwerkingsverantwoordelijkheid voor de verwerking van persoonsgegevens niet worden gemandateerd of gedelegeerd.

Toelichting

Zie voor een toelichting op de mogelijkheden tot mandaat-verlening Bijlage 5.

6.8. Het Partneroverleg heeft de volgende taken:
   a) Op tactisch niveau sturing geven aan de operationele processen van het zorg- en veiligheidshuis;
   b) Formuleren van voorstellen en vragen ten behoeve van of ter besluitvorming in de Stuurgroep;
   c) In samenwerking met de Manager opstellen van het operationele Werkproces. Een kopie van het door het Partneroverleg vastgestelde Werkproces wordt aan alle Partijen verstrekt;
   d) Het afstemmen van externe communicaties;
   e) [*Voeg hier eventueel aanvullende taken toe voor het Partneroverleg*];
   f) [*Voeg hier eventueel aanvullende taken toe voor het Partneroverleg*];

6.9. De secretaris van het Partneroverleg is verantwoordelijk voor het organiseren van de vergaderingen, het samenstellen van de agenda op basis van inbreng vanuit de Stuurgroep en de leden van het Partneroverleg en het opstellen en verspreiden van het verslag van de betreffende vergadering, alsook het informeren van de Stuurgroep over de in het Partneroverleg genomen relevante besluiten.

Artikel 7. Besluitvorming Partneroverleg

7.1. Besluiten in het Partneroverleg worden genomen met een meerderheid van stemmen en zijn bindend voor alle Partijen die deelnemen aan dit Convenant, voor zover niet strijdig met de wettelijke taken, bevoegdheden en beroepsnormen van Partijen. Er wordt gestreefd naar consensus.

7.2. Bij afwezigheid van een lid van het Partneroverleg wordt die Partij verzocht schriftelijk inbreng te leveren rondom de geagendeerde besluiten. Zonder schriftelijke inbreng worden besluiten die deze Partij in belangrijke mate kunnen treffen niet genomen, tot die Partij gehoord is.

7.3. Indien het Partneroverleg niet tot een besluit kan komen, wordt de aangelegenheid ter beslissing voorgelegd aan de Stuurgroep.
7.4. De secretaris van het Partneroverleg informeert de Stuurgroep schriftelijk over de in het Partneroverleg genomen relevante besluiten.
7.5. De vergaderingen van het Partneroverleg zijn niet openbaar.

Artikel 8. Het Casusoverleg

8.1. Partijen in het zorg- en veiligheidshuis voeren ter uitvoering van de in artikel 2 bepaalde doeleinden onderling overleg op operationeel niveau in het 'Casusoverleg'. Het Casusoverleg vindt plaats wanneer op basis van Triage wordt besloten een Casus in het Casusoverleg te bespreken.
8.2. Het Casusoverleg bestaat uit afgevaardigden van Partijen, aangewezen door de Procesregisseur conform Artikel 12.
8.3. De afgevaardigden van Partijen hebben het mandaat om op operationeel niveau besluiten te nemen over de behandeling van een Casus.
8.4. Het Casusoverleg heeft de volgende taken:
a. Het aanwijzen van een Casusregisseur;
b. Opstellen van een integraal plan van aanpak;
c. Komen tot inhoudelijke afspraken in onderlinge samenhang voor de behandeling van de Casus, waaronder in ieder geval het bepalen van de rol en informatiebehoefte van iedere betrokken Partij om uitvoering te kunnen geven aan het plan van aanpak;
d. Het bepalen van de criteria voor Afschaling, alsook het nemen van besluiten hieromtrent.
8.5. Partijen geven ieder met het oog op hun eigen wettelijke taken en bevoegdheden uitvoering aan de uitkomsten van het Casusoverleg, in het bijzonder voor wat betreft de uitwisseling van informatie en de uitvoering van het plan van aanpak zoals vastgesteld op grond van artikel 8.4, onder b.
8.6. De Casusregisseur stemt waar nodig af met de Procesregisseur voor wat betreft de uitvoering van de onder artikel 8.4 genoemde taken.

Artikel 9. Afspraken Casusoverleg

9.1. In het Casusoverleg worden in gezamenlijkheid afspraken gemaakt.
9.2. De vergaderingen van het Casusoverleg zijn niet openbaar. Informatieverstrekking aan derden omtrent hetgeen wordt besproken in het Casusoverleg vindt slechts plaats conform het Convenant, het Privacy Protocol [/de Privacy Protocollen], binnen de voor Partijen geldende wettelijke kaders en slechts na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke zoals bedoeld in het Privacy Protocol, die de betreffende informatie oorspronkelijk aan het samenwerkingsverband heeft verstrekt .

Artikel 10. Contactpersonen

10.1. De afgevaardigden in het Partneroverleg, de Stuurgroep en het Casusoverleg fungeren tevens als contactpersoon voor de secretarissen van de Stuurgroep c.q. het Partneroverleg, de Manager van het zorg- en veiligheidshuis, de Procesregisseur en indien van toepassing, de Casusregisseur.

Artikel 11. Manager

11.1. Het dagelijks bestuur van het zorg- en veiligheidshuis is belegd bij de Manager van het zorg- en veiligheidshuis ('de Manager').

11.2. De Manager wordt aangewezen door de Stuurgroep en valt onder de verantwoordelijkheid van [*naam Partij*].
11.3. De Manager heeft de volgende taken en bevoegdheden:
   a. Het vaststellen van de operationele werkprocessen in afstemming met het Partneroverleg;
   b. Het toezicht op de naleving en uitvoering van het Jaarplan;
   c. […]
   d. […]

Toelichting:
Vul hier aanvullende taken en bevoegdheden van de Manager in, liefst zo uitputtend mogelijk, bijv:
- opstellen jaarverslagen)
- Het informeren van de Stuurgroep omtrent de voortgang van de samenwerking in het zorg- en veiligheidshuis door Partijen met het oog op het Jaarplan door het opstellen van een [jaarlijkse] rapportage met aantallen casussen die zijn behandeld, aantallen casussen die succesvol zijn afgerond, overzicht van uitgaven en overige aandachtspunten;
- Optreden als woordvoerder voor het zorg- en veiligheidshuis in overleg met het Partneroverleg;

Denk bijvoorbeeld ook aan het inkopen van bepaalde producten/diensten (eventueel gekoppeld aan een maximumbedrag), het sluiten van daarbij behorende overeenkomsten in naam van Partijen, het aansturen van externe communicatie etc.). Het verdient aanbevelingen ook dat soort zaken in dit Convenant te regelen: wie is bijvoorbeeld bevoegd nieuwe computers te kopen voor het zorg- en veiligheidshuis? Of nieuwe personeel te selecteren en detacheringsovereenkomsten te ondertekenen? Dit kan eventueel worden gekoppeld aan een beheersovereenkomst met de gemeente waarin het zorg- en veiligheidshuis is gevestigd of een andere partij die de financiering van het zorg- en veiligheidshuis voor haar rekening neemt.

11.4. Geschillen omtrent de uitvoering van zijn taken door de Manager worden voorgelegd aan de Stuurgroep.

Artikel 12. Procesregisseur

12.1. De Procesregisseur is bevoegd en verantwoordelijk voor de Procesregie binnen het zorg- en veiligheidshuis.
12.2. De Procesregisseur is belast met de volgende taken:
   a. Het beoordelen van een Casus op geschiktheid voor behandeling in het Casusoverleg na Aanmelding/Intake. Deze beoordeling geschiedt in overleg met de Partij die de Casus bij de Procesregisseur heeft aangedragen;
   b. Het faciliteren van de triage ten behoeve van de Partij die een Casus Aanmeldt in het Veiligheidshuis;
   c. Het voorbereiden van het Casusoverleg, waaronder in ieder geval het zo concreet mogelijk bepalen van het doel van het Casusoverleg, het bepalen van het type besluiten dat in het Casusoverleg dient te worden genomen en het bepalen van de relevante gespreksthema's voor het Casusoverleg;
   d. Het op basis van de onder a. genoemde beoordeling agenderen van een Casus in het Casusoverleg;
   e. Het organiseren van de Casusoverleggen, waaronder het aanwijzen van Partijen die worden uitgenodigd deel te nemen aan een Casusoverleg en het bepalen van de van hen gevraagde inhoudelijke bijdrage aan dat Casusoverleg. Alleen die Partijen worden uitgenodigd die rechtmatig bij het overleg aanwezig mogen zijn;

f. Het beoordelen of, en zo ja welke informatie voorafgaand aan het Casusoverleg door deelnemers aan het Casusoverleg kan worden ingezien. Deze beoordeling geschiedt in overleg met de Partij die de Casus bij het Veiligheidshuis heeft Aangemeld of de Casusregie heeft, en uitsluitend als de Partij die de gegevens heeft verstrekt dat accordeert;
g. Het ondersteunen van de Casusregisseur, waaronder het toezien op de naleving van de uitvoering van het in het Casusoverleg vastgestelde plan van aanpak door Partijen;
h. Het toezien op de naleving van het vastgestelde Werkproces door Partijen tijdens het Casusoverleg;

12.3. De Procesregisseur werkt voor wat betreft de taken genoemd onder artikel 12.2 a tot en met g namens de Partij die een casus Aanmeldt of de Casusregie voert. De Procesregisseur werkt voor wat betreft de taak genoemd in artikel 12.2, onder h, onder de gezamenlijke verantwoordelijkheid van Partijen.
12.4. Geschillen omtrent de uitvoering van zijn taken door de Procesregisseur worden voorgelegd aan de Manager. De Manager kan het geschil waar nodig voorleggen aan de Stuurgroep.

Artikel 13. Casusregisseur

13.1. Conform artikel 8.4, onder a, kan in het Casusoverleg een Casusregisseur worden aangewezen. De Casusregisseur werkt onder de verantwoordelijkheid van de Partij tot wie deze behoort. De Casusregisseur is doorgaans afkomstig uit de organisatie waar het zwaartepunt van de zorgverlening aan de betreffende betrokkene ligt.
13.2. De Casusregisseur is belast met het toezicht op de naleving van de afspraken zoals die zijn vastgelegd in het plan van aanpak.
13.3. De Casusregisseur stemt af met de Procesregisseur voor wat betreft de voortgang van het Plan van Aanpak
13.4. Geschillen omtrent de uitvoering van taken door een Casusregisseur worden voorgelegd aan de Procesregisseur. Deze kan, indien noodzakelijk, het geschil ter beslechting voorleggen aan het Partneroverleg.

Artikel 14. Ondersteunend Personeel

***Toelichting**:*
Indien het zorg- en veiligheidshuis wordt bemand door ondersteunend personeel (anders dan hierboven genoemd), definieer dan in dit artikel welke bijkomende functies worden voorzien en wie deze levert, danwel onder wiens verantwoordelijkheid deze vallen.

14.1. Het zorg- en veiligheidshuis wordt ondersteund door één of meerdere administratieve medewerkers, [*denk aan: secretaresse/receptionist*]. [*Naam Partij*] draagt zorg voor voldoende personele ondersteuning in het zorg- en veiligheidshuis. Dit personeel werkt onder de verantwoordelijkheid van [*Naam Partij*].
14.2. De [Stuurgroep/Manager] kan, buiten het inzetten van personeel dat in loondienst is bij […], besluiten personeel op grond van een dienstverleningsovereenkomst in te zetten. Dit personeel werkt onder verantwoordelijkheid van […].
14.3. De dagelijkse aansturing van het personeel gebeurt door de Manager.

Artikel 15. Uitwisseling van informatie

15.1. Partijen voorzien elkaar van alle noodzakelijke informatie voor het behalen van de doelstellingen van het zorg- en veiligheidshuis zoals beschreven in artikel 2 en het uitvoeren van hun respectievelijke taken zoals beschreven in dit Convenant, voor zover wettelijk mogelijk. Partijen zijn ieder zelf verantwoordelijk voor het verstrekken van informatie in het

zorg- en veiligheidshuis. Verder gebruik van die informatie geschiedt onder gezamenlijke verantwoordelijkheid van Partijen, slechts voor zover volgens geldende wet- en regelgeving is geoorloofd en met inachtneming van artikel 16, lid 2.

15.2. Voor zover het de verwerking van persoonsgegevens, waaronder (bijzondere) persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming, de Wet justitiële en strafvorderlijke gegevens of de Wet politiegegevens betreft, handelen partijen overeenkomstig het Privacy Protocol Integrale Veiligheid en Complexe Multiproblematiek, in het bijzonder voor wat betreft de daarin vastgelegde doeleinden en grondslagen voor die verwerking.

Toelichting:

Indien meerdere doelen worden nagestreefd door het zorg- en veiligheidshuis dient voor ieder van die doeleinden naar een eigen Privacy Protocol te worden verwezen:

Voorbeeld:

15.3 Voor zover het de verwerking van gegevens, waaronder (bijzondere) persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming, de Wet justitiële en strafvorderlijke gegevens of de Wet politiegegevens betreft, handelen Partijen overeenkomstig de respectievelijke Privacy Protocollen zoals hieronder aangeduid:

- *Voor de doeleinden zoals beschreven in Artikel 3.2, onder a en b: Privacy Protocol Integrale Veiligheid en Complexe Multiproblematiek.*
- *Voor de doeleinden zoals beschreven in Artikel 3.2, onder c: Privacy Protocol [naam protocol]*
- *Voor de doeleinden zoals beschreven in Artikel 3.2, onder d: Privacy Protocol [naam protocol]*

Artikel 16. Interventie en het gebruik van informatie

16.1. Partijen behouden hun eigen bevoegdheden met betrekking tot de in het Zorg- en veiligheidshuis besproken Casussen. Afzonderlijk optreden op basis van eigen informatie blijft door samenwerking in het zorg- en veiligheidshuis onverlet. Desalniettemin streven Partijen naar een zo gezamenlijk mogelijke behandeling van een Casus waar noodzakelijk voor het bewerkstelligen van de in artikel 2 geformuleerde doeleinden.

16.2. De Partij die de informatie verstrekt bepaalt op welke wijze de informatie door de overige Partijen mag worden gebruikt, behoudens hetgeen hierover omtrent de verwerking van persoonsgegevens is bepaald in het Privacy Protocol Integrale Veiligheid en Complexe Multiproblematiek*/[de Privacy Protocollen*]. Partijen verklaren dat Privacy Protocol te onderschrijven en daarnaar in het kader van samenwerking in het zorg- en veiligheidshuis te zullen handelen.

Artikel 17. Geheimhouding en beveiliging

17.1. Partijen nemen conform de toepasselijke wettelijke bepalingen en ongeacht de duur van dit Convenant strikte geheimhouding in acht over elkaars organisatie, over informatie die ten behoeve van de uitvoering van dit Convenant bij en/of tussen Partijen bekend wordt en vertrouwelijk is, dan wel waarvan mag worden aangenomen dat deze vertrouwelijk is, dan wel persoonsgegevens die worden uitgewisseld, alsmede over al hetgeen waarvan redelijkerwijs is aan te nemen dat bekendmaking daarvan de belangen van de andere Partijen, het privacybelang van de betreffende burger(s) of het algemene maatschappelijk belang zou

schaden, voor zover deze informatie niet al openbare informatie betreft als gevolg van openbaarmaking door één of meer der Partijen, dan wel anderszins bekend is geworden bij het publiek, behoudens wettelijke verplichtingen en hetgeen is bepaald in Artikel 9.2 en Artikel 15.

17.2. Partijen staan ervoor in dat hun personeel bekend is met de in dit artikel vastgestelde verplichting en de naleving hiervan nakomen.

17.3. Partijen nemen ieder voor zich adequate technische en organisatorische maatregelen om informatie te beschermen tegen verlies of onrechtmatige verwerking, waaronder ten minste het bewaren, verstrekken, verzenden en archiveren van informatie. Voor informatiebeveiliging in het zorg- en veiligheidshuis wordt zorg gedragen door [naam Partij], conform het Informatiebeveiligingsbeleid zorg- en veiligheidshuis [naam zorg- en veiligheidshuis], meegeleverd in Bijlage 4. [*Naam Partij*] stelt de benodigde middelen ter beschikking voor de uitvoering van dat Informatiebeveiligingsbeleid door het zorg- en veiligheidshuis.

Artikel 18. Financiering en overige bijdragen

18.1. Partijen zijn ieder voor zich verantwoordelijk voor het dragen van financiële lasten voor deelname in het zorg- en veiligheidshuis in het kader van dit Convenant die niet worden gedekt door de Rijksbijdragen of bijdrage van de Gemeente(n), waaronder in ieder geval het leveren van een afgevaardigde voor het Partneroverleg, de Stuurgroep en de Casusregisseur en eventuele reis- en verblijfkosten voor die afgevaardigden.

18.2. De Manager houdt toezicht op de financiële huishouding van het zorg- en veiligheidshuis en rapporteert hierover aan de Stuurgroep.

Artikel 19. Communicatie

19.1. Partijen communiceren niet afzonderlijk naar derden over de samenwerking in het zorg- en veiligheidshuis in het kader van de uitvoering van dit Convenant, zonder voorafgaande instemming van de andere Partijen en met inachtneming van het bepaalde in Artikel 9.2 en Artikel 15.

19.2. De Manager ziet toe op het coördineren van communicatie naar derden en treedt op als woordvoerder voor het zorg- en veiligheidshuis.

Artikel 20. Toetreding

20.1. Dit Convenant staat open voor toetreding door andere organisaties die binnen de kaders van hun publieke en/of maatschappelijke taak een bijdrage kunnen leveren aan de in Artikel 2 geformuleerde doeleinden.

20.2. Een organisatie die tot dit Convenant wil toetreden kan daartoe een aanvraag doen bij één van de leden van de Stuurgroep/het Partneroverleg/de Partijen.

20.3. Partijen worden vooraf door de secretaris van de Stuurgroep op de hoogte gebracht van de voorgenomen toetreding.

20.4. De Stuurgroep beslist op het verzoek van toetreding na akkoord te hebben verkregen van alle Partijen. In geval van goedkeuring, vindt toetreding tot het Convenant plaats door middel van ondertekening van Bijlage 1 bij dit Convenant door die andere organisatie en de voorzitter van de Stuurgroep.

Artikel 21. Wijzigingen

21.1. De bepalingen in dit Convenant kunnen door de Partijen in gezamenlijk overleg worden gewijzigd. Wijzigingen in dit Convenant worden door de Stuurgroep besloten. Mondelinge mededelingen, toezeggingen of afspraken welke betrekking hebben op de inhoud van dit

Convenant, hebben geen rechtskracht, tenzij deze uitdrukkelijk schriftelijk zijn bevestigd door de Stuurgroep.

21.2. Wijziging van het Convenant vergt het opnieuw ondertekenen door Partijen van het gewijzigde Convenant.

21.3. In geval van wijzigingen, waaronder inbegrepen toetreding van een nieuwe organisatie tot het Convenant, die door een Partij onaanvaardbaar worden ervaren, kan deze Partij deelname aan het zorg- en veiligheidshuis schriftelijk opzeggen met ingang van het tijdstip waarop het gewijzigde Convenant van kracht wordt.

Artikel 22. Aansprakelijkheid

Toelichting:

Bepaal gezamenlijk hoe wordt omgegaan met aansprakelijkheid op grond van de uitvoering van dit Protocol. Wat als het delen van Persoonsgegevens in het Veiligheidshuis leidt tot een boete van de Autoriteit Persoonsgegevens of een claim van een Betrokkene op schadevergoeding? Er zijn veel scenario's denkbaar. Hieronder is een voorbeeld opgenomen waarin onderscheid is gemaakt tussen schade die het gevolg is van niet-nakoming door één der Partijen en de situatie waarin de gezamenlijke gegevensverwerking heeft geleid tot schade bij derden of tot boetes en de situatie waarin de samenwerking leidt tot schade bij een Partij.

22.1. Partijen zetten zich in voor een goede uitvoering van het bepaalde in dit Protocol en zullen zich houden aan de dienaangaande in dit Protocol gemaakte afspraken.

22.2. Partijen zijn ieder voor zich aansprakelijk voor aanspraken van derden op schadevergoeding op grond van directe of indirecte schade, administratieve boetes of andere aanspraken van derden in geval van toerekenbare tekortkoming door de aangesproken Partij in de nakoming van het bepaalde in dit Protocol en de bijbehorende Bijlagen.

22.3. Wanneer meerdere Verwerkingsverantwoordelijken of Verwerkers bij dezelfde Verwerking betrokken zijn, en verantwoordelijk zijn voor schade die door die Verwerking is veroorzaakt, wordt elke Verwerkingsverantwoordelijke of Verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk wordt vergoed.

22.4. Een Verwerker is slechts aansprakelijk voor de schade die door Verwerking is veroorzaakt wanneer bij de Verwerking niet is voldaan aan de specifiek tot Verwerkers gerichte verplichtingen van de Algemene Verordening Gegevensbescherming of buiten dan wel in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke is gehandeld.

22.5. Onverminderd het gestelde in lid 4 kan iedere Verwerkingsverantwoordelijke of Verwerker die de volledige vergoeding heeft betaald vervolgens bij de andere Verwerkingsverantwoordelijken of Verwerkers die bij dezelfde Verwerking betrokken zijn, het deel van de schadevergoeding verhalen dat overeenkomt met hun deel van de aansprakelijkheid voor de schade. Een Verwerkingsverantwoordelijke of Verwerker kan door andere Verwerkingsverantwoordelijken of Verwerkers worden vrijgesteld van onderlinge betaling van schadevergoeding indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

Artikel 23. Duur, opzegging, beëindiging

23.1. Dit Convenant treedt in werking op de dag van ondertekening door Partijen en wordt ten minste aangegaan tot [*datum*]. Verlenging van het Convenant geschiedt in onderling overleg.

OF

Dit Convenant treedt in werking op de dag van ondertekening door Partijen en wordt tenminste aangegaan voor een periode van [*aantal*] jaar, waarna het Convenant automatisch iedere keer met een periode van één jaar wordt verlengd, behoudens schriftelijke opzegging door Partijen.

23.2. De Stuurgroep kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een Partij met onmiddellijke ingang uitsluiten van de samenwerking in het zorg- en veiligheidshuis, indien de afspraken zoals neergelegd in dit Convenant niet door de desbetreffende Partij worden nagekomen.

23.3. Verplichtingen die naar hun aard zijn bestemd om ook na beëindiging of uitsluiting van het project voort te duren, blijven na beëindigingen van dit Convenant bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding.

Artikel 24. Opvolging

24.1. Dit Convenant vervangt alle eerdere door Partijen gesloten Convenanten met betrekking tot samenwerking in het zorg- en veiligheidshuis.

Artikel 25. Toepasselijk recht

25.1. Op dit Convenant is Nederlands recht van toepassing.

Aldus overeengekomen:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

[Naam Partij]
in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*
Datum en plaats:

Bijvoegsel 1 bij Samenwerkingsconvenant: Toetredingsformulier nieuwe partner tot Convenant

[naam organisatie], statutair gevestigd te […] en kantoorhoudend aan […], hierbij rechtsgeldig vertegenwoordigd door [naam, functie],

overwegende dat:

- Deelname aan het Convenant gelet op de publieke en/of maatschappelijke taak die zichzelf in het kader van integrale veiligheid en complexe casuïstiek toedicht en gelet op de verantwoordelijkheid en/of bevoegdheid van ondergetekende een bijdrage levert aan de doelstelling zoals geformuleerd in Artikel 2 van het Convenant;
- De Stuurgroep positief heeft besloten op toetreding van ondergetekende aan het Convenant;

verklaart daartoe het volgende:

- Ondergetekende onderschrijft de in het Convenant geformuleerde doelstellingen, verplicht zich de bepalingen in het Convenant te zullen naleven en verklaart zich in dit kader gerechtigheid tot het uitwisselen van informatie met Partijen.

Aldus ondertekend te […], op datum […]

Naam organisatie:

Naam bevoegde functionaris:

……..

Namens Stuurgroep:

Naam:

……

Bijvoegsel 2 bij Samenwerkingsconvenant: Criteria Complexe Casuïstiek

Volgens het Landelijk Kader Veiligheidshuizen dient samenwerking in de Veiligheidshuizen zich te richten op het oplossen van vraagstukken met een complexe, meervoudige problematiek. Veiligheidshuizen beperken zich daarom tot juist die zaken waarin de verbinding tussen de zorg-, strafrechtketen en interventies vanuit de gemeente en haar partners voorwaarde is voor een succesvolle, duurzame aanpak van (potentieel) crimineel en overlast-gevend gedrag.

Een casus voldoet aan de notie 'complexe casuïstiek' wanneer deze aan de volgende criteria voldoet:

- Er is sprake van ernstige lokale of gebieds-gebonden veiligheidsproblematiek, die vraagt om een keten-overstijgende aanpak, of;
- De problematiek wordt beïnvloed door en heeft impact op het (gezins-)systeem en/of de directe sociale leefomgeving (of wordt verwacht dat te gaan hebben);
- Samenwerking tussen meerdere ketens (minimaal dwang en drang) is nodig om tot een effectieve aanpak te komen; het is in de reguliere samenwerking tussen partners binnen één keten niet mogelijk om deze problematiek effectief aan te pakken; en;
- Er is sprake van meerdere problemen (multiproblem) die op meer dan één leefgebied spelen en (naar verwachting) leiden tot crimineel en/of overlast-gevend gedrag of verder afglijden.

Bijvoegsel 3 bij Samenwerkingsconvenant: Werkproces

Zie voor een beschrijving van het Werkproces en hoe dit binnen uw zorg- en veiligheidshuis dient te worden vastgesteld, het door de Landelijke Stuurgroep Zorg en Veiligheid vastgestelde document “Van juridisch kader naar operationeel proces, vertaling handvat naar de praktijk.”

U dient het binnen uw zorg- en veiligheidshuis vastgestelde Werkproces in deze bijlage te beschrijven volgens de daarin vastgelegde werkwijze.

Bijvoegsel 4 bij Samenwerkingsconvenant: Informatiebeveiligingsbeleid

Stel een informatiebeveiligingsbeleid op (naast het beleid voor de bescherming van persoonsgegevens). Informatiebeveiliging is breder dan de bescherming van persoonsgegevens; ook andere (gevoelige) informatie, zoals vertrouwelijke informatie over een ketenpartner, moet op een zorgvuldige en veilige manier worden behandeld.

Aansluiting kan worden gezocht bij de Baseline Informatiebeveiliging Overheid (BIO). Zie: https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio

- Het informatiebeveiligingsbeleid dient te worden vastgesteld door de Stuurgroep;
- Het informatiebeveiligingsplan dient te worden vastgesteld door de Stuurgroep;
- Incidentenmanagement dient te zijn ingericht;
- Er dienen periodieke rapportages over informatiebeveiliging, incidenten en maatregelen te worden opgesteld en overhandigd aan de Stuurgroep.

Bijvoegsel 5 bij Samenwerkingsconvenant:
Nadere toelichting op mandaat, machtiging en vertegenwoordiging

De verwerkingsverantwoordelijkheid voor de verwerking van persoonsgegevens kan niet worden gemandateerd. Andere verantwoordelijkheden kunnen onder omstandigheden worden gemandateerd.

Onder mandaat wordt verstaan de bevoegdheid om in naam van een bestuursorgaan besluiten te nemen. In geval van mandatering wordt een bevoegdheid door bijv. een College van Burgemeester en Wethouders van een gemeente toegekend aan een College van Burgemeester en Wethouder van een andere gemeente, die deze op naam van de mandaatgever uitoefent. Bij mandatering blijft de bevoegdheid bij het oorspronkelijke bestuursorgaan op grond van de Awb bestaan en blijft dat bestuursorgaan aansprakelijk voor de eventuele gevolgen van de genomen beslissingen en wordt de gemandateerde partij dus niet aansprakelijk. Een voorwaarde voor mandaat is onder meer dat het gemandateerde bestuursorgaan schriftelijke bevestigt in te stemmen met de mandatering. Zie voor de overige vereisten art. 10:1 t/m 10:12 Awb.

In het kader van het zorg- en veiligheidshuis is voor mandatering noodzakelijk dat alle gemeenten eerst toetreden tot de Stuurgroep en het Partneroverleg. Pas nadat zij zijn toegetreden kunnen zij formeel andere gemeenten mandateren om namens hen besluiten te nemen in de Stuurgroep en het Partneroverleg. De mandaatgever dient daarnaast akkoord te zijn met eventuele machtigingen aan bijvoorbeeld de Manager van een zorg- en veiligheidshuis.

In de Stuurgroep en het Partneroverleg worden niet zo zeer besluiten genomen in de zin van de Awb als wel besluiten die leiden tot privaatrechtelijke rechtshandelingen, zoals bijv. het opzeggen van een huurcontract van een pand en aangaan van een ander huurcontract etc. Er is een scala aan onderwerpen waarover besluiten moeten worden genomen enerzijds gaat het om bedrijfsvoering en anderzijds betreffen het bestuurlijke zaken en die hebben de nodige raakvlakken:

- toetreding van nieuwe partijen
- jaarverslag en de jaarrekening
- jaarplan, begroting (en het meerjarenbeleidsplan).
- vaststellen danwel wijzigen van de tekst van het convenant en privacyprotocol
- vaststellen danwel wijzigingen van de werkprocessen
- de hoogte van de financiële bijdrage van partners danwel bijdrage in natura middels het detacheren van personeel,
- uitbreiding danwel inkrimping van formatie
- functieomschrijvingen en salariëring
- beleid omtrent VOG's, screening (mits daar een wettelijke grondslag voor is)
- aannemen of ontslaan van individuele personeelsleden
    - aanstellingsovereenkomsten
    - detacheringsovereenkomsten aangaan danwel beëindiging
    - dienstverleningsovereenkomsten in geval van inhuur van zzp-ers bijv. middels model ARVODI

- huur van kantoorlocatie, aanschaf kantoorinventaris, ICT hardware en software, telefonie, e-mail e.d. t/m leasen van auto's
- afhandelen van klachtzaken (bijv. NOM)
- uitvoeren van audits en evaluaties en evt. implementatie van wijzigingen als gevolg daarvan
- consequenties van beleidswijzigingen van landelijke partners, departement en VNG of bijv. gewijzigde wet- en regelgeving

Per zorg- en veiligheidshuis dient duidelijk te worden uitgewerkt welke Partij waarvoor verantwoordelijk is: we onderscheiden achtereenvolgens de Stuurgroep, het Partneroverleg, de beheersgemeente en de Manager van het zorg- en veiligheidshuis. Daarnaast dient helder worden wat onder welke reikwijdte valt. Zo vallen bijv. besluiten over ambtenaren en personeel van ZBO's onder de Awb, terwijl het aangaan van een huurcontract van een kantoorlocatie privaatrechtelijk is. Beantwoording van inzageverzoeken en klachten over de verwerking van persoonsgegevens etc. vallen onder de Awb en daar blijven de verwerkingsverantwoordelijken altijd zelfstandig verantwoordelijk voor.

BIJLAGE 4:

TEMPLATE PRIVACY PROTOCOL

Integrale Veiligheid en Complexe Multi-Problematiek zorg- en veiligheidshuis [*naam*]

Met dit Privacy Protocol worden afspraken rondom de uitwisseling en het verder gebruik van persoonsgegevens door en tussen verschillende partijen in het zorg- en veiligheidshuis geformaliseerd en vastgelegd. Uit dit Privacy Protocol dient duidelijk te blijken met welk doel persoonsgegevens worden verwerkt, wie voor welke acties met betrekking tot persoonsgegevens verantwoordelijk is, wanneer sprake is van gezamenlijke verantwoordelijkheid en hoe invulling wordt gegeven aan de materiële vereisten uit privacy wet- en regelgeving zoals de informatieplicht, de rechten van de betrokkene, beveiliging en het bewaren en vernietigen van persoonsgegevens.

In dit Privacy Protocol zijn de standaard onderdelen van een samenwerkingsovereenkomst opgenomen, behoudens hetgeen al is geregeld in het Convenant. De precieze verdeling van verantwoordelijkheden, rechten en plichten is uiteindelijk aan partijen zelf in te vullen, tenzij de wet hier een dwingende bepaling over heeft, en dient aan te sluiten op de verdeling van rollen en bevoegdheden zoals belegd in het Convenant. Door middel van gearceerde teksten is op specifieke plekken ruimte voor maatwerk en toelichting gegeven op de keuzemogelijkheden en de mogelijke gevolgen van die keuzes. Dit is echter niet uitputtend en dient door iedere partij die deelneemt aan dit Protocol zelf nader te worden onderzocht. Wanneer u in uw zorg- en veiligheidshuis een andere structuur voor de samenwerking hebt ingericht en/of wilt handhaven, dient u dit template daarop aan te passen en (schriftelijk) te onderbouwen hoe u de verantwoordelijkheden van de verschillende aangesloten ketenpartners alsnog dekkend waarborgt.

Formuleringen, begrippen en andere specifieke zorg- en veiligheidshuis-gerelateerde termen zijn afgeleid uit het Handvat “Gegevensuitwisseling in het zorg- en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen”, versie 1.1. van juli 2017 en het Landelijk Kader Veiligheidshuizen. Ook wordt aangesloten bij de werkwijze zoals in het Handvat beschreven. Daarnaast is geput uit een aantal reeds bestaande samenwerkingsconvenanten voor wat betreft onder meer de structuur van het zorg- en veiligheidshuis.

Dit Protocol en de daarin gehanteerde terminologie is gebaseerd op Algemene Verordening gegevensbescherming, alsook de Wet politiegegevens en de Wet justitiële strafvorderlijke gegevens.

Met dit Template wordt niet beoogd te voorzien in een volledig sluitend Privacy Protocol voor

Het zorg- en veiligheidshuis. Het Template dient als leidraad en kan per zorg- en veiligheidshuis op onderdelen worden aangepast. Dit Template dient samen met het Convenant te worden gebruikt.

Dit Template is tot stand gekomen in samenwerking tussen (privacy)adviseurs van verschillende landelijke partijen, Considerati en het Ministerie van Justitie en Veiligheid.

Privacy Protocol tussen ketenpartners zorg- en veiligheidshuis [*naam*]

Toelichting:
Onderstaande deelnemers dienen gelijk te zijn aan de deelnemers die partij zijn bij het samenwerkingsconvenant. Zie voor een toelichting op mogelijke deelnemers de toelichting op dit onderdeel in het samenwerkingsconvenant.

De ondergetekenden:

(in geval van één gemeente)

Het college van burgemeester en wethouders en de burgemeester, ieder voor zover het zijn bevoegdheid betreft, van de gemeente [naam gemeente].

(in geval van meerdere gemeenten)

De colleges van burgemeester en wethouders en de burgemeesters, ieder voor zover het zijn bevoegdheid betreft, van de gemeenten:

[*Gemeente A*];

[*Gemeente B*];

[*Gemeente C*];

[*Gemeente D*],

verder *afzonderlijk* aangeduid als 'Partij' of 'Gemeente' *en gezamenlijk als 'Gemeenten'*,

en

de Korpschef van politie [naam], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie]*

het College van procureurs-generaal, hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

[*naam partij A*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*]; !

[*naam partij B*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

[*naam partij C*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

[*naam partij i.c. GGD*], gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [naam, functie];

[*naam partij E i.c. private partij*], statutair gevestigd te [*plaats*] en kantoorhoudend te [*adres*], hierbij rechtsgeldig vertegenwoordigd door [*naam, functie*];

(*Indien afkorting van naam van de partij dient te worden gebruikt in het convenant, deze afkorting vermelden in de beschrijving door middel van de volgende zinsnede: (verder aangeduid als '…'))*

hierna afzonderlijk te noemen 'Partij' en gezamenlijk, inclusief Gemeente[n], te noemen 'Partijen',

de volgende overwegingen in aanmerking nemende:

Toelichting

De overwegingen beschrijven wat de bedoelingen van partijen zijn met het aangaan van de overeenkomst. Dit is van belang voor de uitleg van de overeenkomst, met name indien niet duidelijk is wat er wordt bedoeld met een zin of zinsdeel. De overwegingen geven dus de context aan de samenwerking die niet per se in de afspraken terugkomt, maar wel van belang is voor de partijen die aan de samenwerking deelnemen met betrekking tot het uitleggen van de afspraken. Onderstaande overwegingen zijn niet uitputtend en dienen als leidraad. Partijen kunnen overwegingen weghalen of toevoegen indien die (niet) van belang zijn voor hun specifieke vorm(en) van samenwerking. Van belang bij het formuleren van overwegingen is dat deze duidelijk zijn beschreven en consequent woordgebruik en formuleringen toepassen.

- Partijen in het kader van samenwerking op het gebied van integrale veiligheid en complexe casuïstiek zoals beschreven in het Landelijke Kader het zorg- en veiligheidshuis [*naam zorg- en veiligheidshuis*] (hierna: 'het zorg- en veiligheidshuis') hebben opgezet;
- Partijen voor deze samenwerking afspraken hebben vastgelegd in het Convenant 'Samenwerking tussen ketenpartners in zorg- en veiligheidshuis [*naam zorg- en veiligheidshuis*], gesloten op [*dd-mm-jjjj*]' (verder: het Convenant), waar dit Privacy Protocol deel van uitmaakt;
- voor de samenwerking in het zorg- en veiligheidshuis de uitwisseling van gegevens, waaronder Persoonsgegevens, tussen de Partijen noodzakelijk is;
- in het door Partijen opgezette zorg- en veiligheidshuis Persoonsgegevens worden verwerkt ten dienste en onder verantwoordelijkheid van Partijen;
- Partijen slechts die Persoonsgegevens binnen het zorg- en veiligheidshuis delen die noodzakelijk zijn voor het doel van de samenwerking;
- op de samenwerking wet-en regelgeving met betrekking tot de bescherming van Persoonsgegevens van toepassing is waarbij Partijen conform deze wet- en regelgeving willen samenwerken;
- dit Privacyprotocol (verder aangeduid als: 'het Protocol') de gedragsregels omschrijft bij het verstrekken en verder Verwerken van Persoonsgegevens door Partijen in het kader van de samenwerking op het gebied van integrale veiligheid en complexe multi-problematiek, alsook de verschillende verantwoordelijkheden met het oog op de rechten en plichten uit toepasselijke privacy wet- en regelgeving, belegd;
- met dit Protocol reeds invulling wordt gegeven aan de in Artikel 26 van de Europese Algemene Verordening Gegevensbescherming neergelegde verplichting voor Partijen om op een transparante wijze hun samenwerkingsafspraken en hun verantwoordelijkheden jegens elkaar en jegens Betrokkene vast te leggen;
- dit Protocol aansluit bij het bepaalde in het 'Landelijk Kader Veiligheidshuizen' van het Ministerie van Veiligheid en Justitie, vastgesteld in januari 2013 (verder aangeduid als: 'het Landelijk Kader') en het 'Handvat Gegevensuitwisseling in het zorg en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen', versie 1.1. van juli 2017, (verder aangeduid als: 'het Handvat'), alsmede bij de in het Handvat en het Landelijk Kader gebezigde terminologie;
- dit privacy protocol verder wordt aangehaald als 'het Protocol'.

verklaren te zijn overeengekomen:

Artikel 1. Definities

***Toelichting**:*
In dit artikel volgen de definities. Definities worden gebruik om veelgebruikte termen of zinnen af te korten, waarmee in de rest van de overeenkomst niet iedere keer de gehele zin of omschrijving dient te worden gebruikt. Dit bevordert de leesbaarheid van de overeenkomst.

In dit Protocol en de daarbij behorende bijlage(n) wordt verstaan onder:

1.1. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de Betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 lid 1 AVG);
1.2. Politiegegevens: elk Persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1, sub a, Wpg);
1.3. Strafvorderlijke gegevens: Persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg verwerkt in een gegevensbestand (artikel 1 sub b Wjsg);
1.4. Justitiële gegevens: bij algemene maatregel van bestuur omschreven Persoonsgegevens of gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de strafvordering, die in een bestand worden Verwerkt (artikel 1 sub a Wjsg, respectievelijk Bjsg);
1.5. Tenuitvoerleggingsgegevens: persoonsgegevens of gegevens over een rechtspersoon inzake de tenuitvoerlegging van strafrechtelijke beslissingen, die in een dossier of een ander gegevensbestand zijn of worden verwerkt;
1.6. Bijzondere Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG);
1.7. Strafrechtelijke persoonsgegevens: Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (zoals bedoeld in artikel 10 AVG);
1.8. Verwerken: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (artikel 4 lid 2 AVG);
1.9. Betrokkene: de natuurlijke persoon op wie informatie, waaronder Persoonsgegevens, betrekking heeft (artikel 4 lid 1 AVG);
1.10. Derde: een natuurlijk persoon of rechtspersoon, niet zijnde de betrokkene, noch één der Partijen;
1.11. Verwerkingsverantwoordelijke(n): een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijke

recht is vastgesteld, kan daarin reeds zijn bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 4 lid 7 AVG);

1.12. Afzonderlijke Verwerkingsverantwoordelijken: Partijen zijn Afzonderlijke Verwerkingsverantwoordelijke voor zelfstandige Verwerkingen en wanneer verschillende Verwerkingen min of meer geïntegreerd zijn, maar geen sprake is van Gezamenlijke Verwerkingsverantwoordelijken;
1.13. Gezamenlijke Verwerkingsverantwoordelijken: Van Gezamenlijke Verwerkings-verantwoordelijkheid is sprake wanneer Verwerkingen zijn geïntegreerd, en niet één Partij als Verwerkingsverantwoordelijke kan worden aangemerkt voor de geïntegreerde Verwerkingen. In dat geval zijn de Partijen Verwerkingsverantwoordelijken voor het geheel van de Verwerking;
1.14. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt (artikel 4 lid 8 AVG);
1.15. Casusregie: het uitvoeren van werkzaamheden gericht het bewaren van de onderlinge samenhang bij het uitvoeren van het plan van aanpak bij het behandelen van één specifieke Casus;
1.16. Procesregie: het uitvoeren van werkzaamheden gericht op de totstandkoming van samenwerking tussen Partijen bij het behandelen van één specifieke Casus en de ondersteuning van de Casusregisseur bij de uitvoering van het plan van aanpak;
1.17. Casus: een geval of situatie dat of die voldoet aan de criteria voor complexe casuïstiek zoals geformuleerd in Bijlage 2 van het Convenant, en die is Aangemeld bij het zorg- en veiligheidshuis ter beoordeling en eventuele bespreking in het Casusoverleg;
1.18. Aanmelding en Intake: het voordragen van een Casus door één der Partijen en het uitwisselen van informatie, waaronder Persoonsgegevens, tussen de Procesregisseur van het zorg- en veiligheidshuis en de aanmeldende Partij ter toetsing of de Casus in aanmerking komt voor behandeling in het zorg- en veiligheidshuis;
1.19. Triage: het proces waarbij relevante Partijen worden bevraagd om te komen tot een nadere afweging ten aanzien van de routering van de casus, tot een bepaling van het doel en de thema's van een eventueel Casusoverleg, en tot een afweging welke Partijen relevant zijn om te betrekken bij een Casusoverleg;
1.20. Casusoverleg: fase waarin overleg plaats vindt door Partijen gericht op de totstandkoming van een plan van aanpak, afstemming tijdens de uitvoering daarvan, en het beoordelen of Casus kan worden afgeschaald;
1.21. Afschaling: fase die volgt op het besluit in het Casusoverleg dat de betrokkenheid van het zorg- en veiligheidshuis niet langer nodig is, waarin het dossier dat in het systeem van het zorg- en veiligheidshuis is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie, en uiteindelijk verdwijnt uit het systeem van het zorg- en veiligheidshuis;
1.22. Procesregisseur: de medewerker van het zorg- veiligheidshuis die namens een van de Partijen is belast met de werkzaamheden in artikel 12 van het Convenant;
1.23. Casusregisseur: de medewerker van een van de Partijen die is belast met de taken in artikel 13 van het Convenant;
1.24. Manager: de persoon die is belast met de taken zoals geformuleerd in Artikel 9 van het Convenant;
1.25. Stuurgroep: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 4 van het Convenant;
1.26. Partneroverleg: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 6 van het Convenant;

Toelichting:
Iedere Partij moet zijn vertegenwoordigd op het niveau van het Partneroverleg. Dit is met name het geval wanneer de betreffende Partij niet deelneemt aan de Stuurgroep. Het enkel deelnemen aan de samenwerking op het niveau van het Casusoverleg is onvoldoende voor een Partij om te kunnen waarborgen dat deze aan diens verantwoordelijkheden rondom de bescherming van persoonsgegevens in het kader van de samenwerking voldoet.

1.27. Privacyadviseur: Ieder zorg- en veiligheidshuis heeft een medewerker die belast is met privacyadvisering of kan gebruik maken van een privacyadviseur van een gemeente. Deze persoon is ook belast met beleidsontwikkeling over gegevensverwerking en helpt mee met de voorbereiding van audits;
1.28. Jaarplan: het door de Stuurgroep op grond van Artikel 4.4 van het Convenant vastgestelde plan betreffende de operationele en inhoudelijke kaders en het financieel en inhoudelijk beleid van het zorg- en veiligheidshuis;
1.29. Werkprocessen: de door het Partneroverleg op grond van Artikel 6 van het Convenant vastgestelde processen voor samenwerking in het zorg- en veiligheidshuis, waaronder het proces omtrent en het delen van informatie en het Afschalen van een Casus;
1.30. AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
1.31. Wjsg: Wet justitiële en strafvordelijke gegevens;
1.32. Bjsg: Besluit justitiële en strafvorderlijke gegevens;
1.33. Wpg: Wet politiegegevens.

Artikel 2. Afzonderlijke en Gezamenlijke Verwerkingsverantwoordelijken

2.1. Partijen in het zorg- en veiligheidshuis zijn Afzonderlijk Verwerkingsverantwoordelijke voor de Persoonsgegevens die zij verstrekken aan de Procesregisseur ten behoeve van de Aanmelding en Intake en aan Partijen in het kader van Triage, Casusoverleg, en Afschaling.
2.2. Partijen in het zorg- en veiligheidshuis zijn conform artikel 26 Algemene Verordening Gegevensbescherming Gezamenlijk Verwerkingsverantwoordelijken voor de Persoonsgegevens die zij, anders dan de verstrekking zoals bedoeld in artikel 2.1, Verwerken op locatie of in de informatiesystemen van het zorg- en veiligheidshuis in het kader van de samenwerking voor de doeleinden zoals omschreven in artikel 3.

Toelichting:
Wanneer twee of meer Verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de Verwerking bepalen, zijn ze gezamenlijk verantwoordelijk voor die Verwerking. Zie artikel 26 AVG.

2.3. Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis door personeel van het zorg- en veiligheidshuis geschiedt onder gezag van de Partij die de betreffende Persoonsgegevens heeft verstrekt. Deze Partij wordt voor die Verwerking aangeduid als Verwerkingsverantwoordelijke.

Artikel 3. Doel Verwerking Persoonsgegevens

3.1. Dit Protocol ziet op alle Verwerkingen van Persoonsgegevens door Partijen in het kader van de uitvoering van artikel 2.2 van het Convenant.
3.2. Het verwerken van Persoonsgegevens in het zorg- en veiligheidshuis vindt plaats met als doel het gezamenlijk door Partijen bijdragen aan de veiligheid als onderdeel van het integrale zorg- en veiligheidsbeleid van de Gemeente(n). De samenwerking is meer specifiek gericht op het

voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en maatschappelijke uitval bij complexe problemen, door een combinatie van repressie, bestuurlijke interventie én zorg, hetgeen gezien moet worden als een zwaarwegend algemeen belang. Meer specifiek draagt de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis bij aan:

a. het oplossen van complexe multi-problematiek, problematiek waarbij personen die het subject zijn in de casuïstiek te maken hebben met meerdere problemen die op meer dan één leefgebied spelen;

b. het voorkomen van (verder) crimineel en/of overlast-gevend gedrag of verder afglijden van die personen;

c. het oplossen van ernstige lokale of gebiedsgebonden veiligheidsproblematiek; en

d. het mogelijk maken van samenwerking met het oog op de hierboven geformuleerde doeleinden.

3.3. Om het onder artikel 3.2 geformuleerde doel te bereiken Verwerken Partijen gezamenlijk de nodige Persoonsgegevens in het kader van Aanmelding en intake, Triage, Casusoverleg, en Afschaling. Voor elk van deze fasen in het werkproces zijn specifieke doelen voor de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis van toepassing. Deze doelen zijn gespecificeerd in Bijlage 2.

3.4. Partijen Verwerken de Persoonsgegevens die zij in het kader van de samenwerking onder dit Protocol hebben verkregen niet voor andere doeleinden dan de doelen omschreven in artikel 3.2.

3.5. Bij het Verwerken van Persoonsgegevens in het zorg- en veiligheidshuis worden de volgende uitgangspunten in acht genomen:

a. Er is sprake van een strikte doelbinding per fase van de voor de te Verwerken Persoonsgegevens en alleen de voor het doel van die fase noodzakelijke persoonsgegevens worden verwerkt;

b. Als het doel van de Verwerking van Persoonsgegevens wijzigt, of, de casus gaat door naar een volgende fase, wordt als eerste opnieuw beoordeeld of de eerder verwerkte gegevens ook daarvoor noodzakelijk zijn en vervolgens of de gegevens daarvoor ook (verder) gebruikt mogen worden;

c. Een partner die in een bepaalde fase Persoonsgegevens verstrekt behoudt de zeggenschap over het verdere gebruik van die gegevens en of die voor een andere fase en/of andere doelen gebruikt mogen worden;

d. Partners die bij de behandeling van een casus kennisnemen van Persoonsgegevens afkomstig van een andere partner mogen deze gegevens enkel verder gebruiken voor hun eigen taken in het kader van de casusbehandeling, als de partner die de gegevens heeft ingebracht, dit afzonderlijk accordeert.

Artikel 4. Categorieën Persoonsgegevens

4.1. In het kader van de samenwerking worden door Partijen van de in Bijlage 4 categorieën Betrokkenen de daarin genoemde categorieën Persoonsgegevens Verwerkt:

Toelichting:
Persoonsgegevens betreft informatie die direct of indirect herleidbaar is tot een natuurlijk persoon, zoals geformuleerd in de definities. Dat kan een naam, adres of telefoonnummer zijn, maar ook gegevens over gezondheid, gewoonten, voorkeuren of (strafrechtelijke) verleden.

De kring van Betrokkenen kan breder zijn dan één specifieke natuurlijke persoon. Bij het uitwerken van Bijlage 4 dient u rekening te houden met het feit dat ieder natuurlijk persoon over wie u Persoonsgegevens verwerkt als aparte (categorie) Betrokkenen dient te worden aangeduid. U dient de categorieën Persoonsgegevens nader te toetsen met het oog op noodzakelijkheid en grondslag zoals bedoeld in artikel 4 van dit Protocol. Hiervoor is het voor publieke instellingen bijvoorbeeld van belang dat zij een publiekrechtelijke taak in wetgeving kunnen aanwijzen waarop de Verwerking wordt gebaseerd (zie voor verdere toelichting en duiding het Handvat).

4.2. Partijen Verwerken Persoonsgegevens, inclusief Bijzondere en Strafrechtelijke Persoonsgegevens, binnen de wettelijke kaders van de voor iedere Partij toepasselijke wet- en regelgeving.

4.3. Partijen Verwerken Persoonsgegevens voor de onder artikel 3.2 geformuleerde doeleinden enkel in de informatiesystemen van het zorg- en veiligheidshuis, of in de door de Stuurgroep aangewezen informatiesystemen en conform het beveiligingsbeleid zoals opgenomen in Bijlage 3 bij dit Protocol.

***Toelichting**:*
Door het Ministerie van JenV is voor onder andere overleggen in het zorg- en veiligheidshuis het systeem GCOS ontwikkeld. Indien GCOS door Partijen ook voor andere werkprocessen/ samenwerkingsverbanden dan het zorg- en veiligheidshuis beschreven, wordt gebruikt, dienen deze Partijen er rekening mee te houden dat die gegevensverwerking en de toegangs-autorisaties volstrekt gescheiden dienen te zijn van de Gegevensverwerking van het zorg- en veiligheidshuis in GCOS. Nog niet alle zorg- en veiligheidshuizen gebruiken GCOS.

Artikel 5. Verwerkingen en verstrekkingen van persoonsgegevens ten behoeve van het behandelen van een casus

5.1 Verwerking van persoonsgegevens door de procesregisseur

5.1.1 De procesregisseur verwerkt persoonsgegevens ten behoeve van de procesregie in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 slechts voor zover dit noodzakelijk is voor het bewerkstelligen van de in de desbetreffende fase aan de orde zijnde doelen voor gegevensverwerking als verwoord in artikel 3.3 en bijlage 2.

5.1.2 De procesregisseur verwerkt de in het eerste lid bedoelde persoonsgegevens ten behoeve van een goede taakuitoefening van de aanmeldende partij, dan wel de goede taakuitoefening van de partij onder wiens verantwoordelijkheid de casusregisseur zoals verwoord in artikel 13 van het convenant valt.

5.1.3 Voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1 zijn van toepassing de grondslag conform de AVG en/of andere wettelijke grondslag, en de wettelijke bepalingen op grond waarvan de aanmeldende partij, dan wel de partij onder wiens verantwoordelijkheid de casusregisseur valt, de casus heeft aangemeld respectievelijk de casusregie voert.

5.1.4 De verantwoordelijke voor de verwerking van persoonsgegevens zoals bedoeld in artikel 5.1.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.2 van dit protocol.

5.2 Verstrekken van persoonsgegevens ten behoeve van aanmelding en intake, triage en casusoverleg

5.2.1 Partijen kunnen persoonsgegevens inbrengen in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 slechts voor zover dit noodzakelijk is voor het bewerkstelligen van de in de desbetreffende fasen aan de orde zijnde doelen voor gegevensverwerking als verwoord in artikel 3.3 en bijlage 2.

5.2.2 Persoonsgegevens als bedoeld in artikel 5.2.1 worden slechts ingebracht indien dit noodzakelijk is voor de goede vervulling van de eigen taak, en/of de goede uitvoering van de taak van de partij ten behoeve waarvan de werkzaamheden in het kader van aanmelding en intake, triage of casusoverleg worden uitgevoerd.

5.2.3 De grondslag conform de AVG voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1 wordt ontleend aan de eigen taak, en/of de taak van de partij ten behoeve waarvan de werkzaamheden in het kader van aanmelding en intake, triage of casusoverleg worden uitgevoerd.

5.2.4 De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.2.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.1 van dit protocol.

5.3 Verstrekken van gegevens bij het uitvoering geven aan afspraken uit het casusoverleg

5.3.1 Onverminderd het bepaalde in artikel 6 en 7, kunnen partijen persoonsgegevens verstrekken aan een andere partij in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 voor zover deze noodzakelijk zijn voor deze partij bij:

a. het uitvoering geven aan interventies en acties die in het casusoverleg zijn afgesproken
b. het voeren van de casusregie op het plan van aanpak als dat in het casusoverleg is afgesproken
c. het toebedelen van de casus aan een specifieke partij ten behoeve van verdere afhandeling, zoals het adviseren van de aanmelder of het aanbrengen van de casus bij een andere overlegtafel.

5.3.2 De grondslag conform de AVG voor het verstrekken van persoonsgegevens als verwoord in artikel 5.3.1 wordt ontleend aan de eigen taak en/of de taak van de partij die de activiteiten onder artikel 5.3.1 a t/m c uitvoert.

5.3.3 De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.3.

Artikel 6. Grondslag voor het verwerken en verstrekken van persoonsgegevens ten behoeve van het behandelen een casus en de van toepassing zijnde taken van partijen

6.1 De grondslag voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. Voor gegevens afkomstig van het Openbaar Ministerie, is de grondslag gelegen in de artikel 8a, 39f en 51c Wet justitiële en strafvorderlijke gegevens.

6.2 De grondslag voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt, en/of de verstrekkende partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.

6.3 De grondslag voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de ontvangende partij en/of de verstrekkende partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.

6.4 De onder 6.1, 6.2 en 6.3 bedoelde grondslag kan bij casussen slechts van toepassing zijn indien dit voortvloeit uit de goede uitvoering van de taken en werkzaamheden van partijen, en de verwerking plaats vindt namens of de verstrekking plaats vindt aan een van de onder a t/m m genoemde partijen en voorwaarden:

a. het bestuursorgaan de burgemeester: de goede uitvoering van taken en de uitoefening van bevoegdheden van de burgemeester, waaronder in het bijzonder taken en bevoegdheden op het gebied van Openbare Orde en Veiligheid zoals neergelegd in de Gemeentewet artikel 172.
b. het bestuursorgaan het College van B&W: de goede uitvoering van taken van het College van B&W, waaronder in het bijzonder taken in het sociaal domein zoals bedoeld in de WMO artikel 2.3.1 t/m 2.3.5, de Jeugdwet artikel 2,3 en 2.4, de Participatiewet artikel 7.1, en de wet schuldhulpverlening artikel 3.
c. het Openbaar Ministerie: voor de strafrechtelijke handhaving van de rechtsorde alsmede andere bij de wet vastgestelde taken (artikel 124 Wet op de Rechterlijke organisatie). De grondslag voor het verstrekken van justitiële, strafvorderlijke of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
d. de politie: vervulling van taken zoals bedoeld in de Politiewet artikel 3, te weten taken op het gebied van opsporing, handhaving van de rechtsorde en hulp aan hen die dat behoeven. De grondslag voor het verstrekken van persoonsgegevens inclusief politiegegevens is gelegen in artikel 20 Wpg. Deze verstrekkingen dienen nader te zijn vastgelegd in de onlosmakelijk bij dit Privacy-protocol behorende en ondertekende Artikel

20 Wpg Beslissing, waarin staat vermeld dat er alleen artikel 8 en 13 Politiegegevens worden verstrekt. De Artikel 20 Beslissing wordt ondertekend door de gemandateerde politiechef van de Eenheid, en het gezag te weten de Burgemeesters en de Officier van Justitie. In artikel 7 zijn nadere voorwaarden benoemd die van toepassing zijn op gegevens die in het kader van deze taken worden verstrekt.

e. de Raad voor de Kinderbescherming: de goede uitvoering van de taken van de Raad voor de Kinderbescherming, waaronder in het bijzonder taken zoals bedoeld in boek 1 afdeling 3 van het Burgerlijk Wetboek, waaronder de artt. 1:240 BW en de artt. 1:255 juncto 1:257 BW, de artt. 77o en 77hh van het Wetboek van Strafrecht, de artt. 126 nd en 491 van het Wetboek van Strafvordering alsmede art. 28 van het Besluit Tenuitvoerlegging Jeugdstrafrecht 1994, de Algemene Wet Bestuursrecht, de artt. 2.4, 3.1 en 3.2 van de Jeugdwet alsmede art. 7.3.11 lid 4 van de Jeugdwet en art. 4 onder c, lid 1 van de Wet Opneming Buitenlandse Kinderen ter Adoptie(wobka). Met inachtneming van het Kwaliteitskader 2016 van de Raad voor de Kinderbescherming.
f. Veilig Thuis: de goede uitvoering van de taken van het AMHK, waaronder in het bijzonder taken zoals bedoeld in de Wmo artikel 4.1.1, met inachtneming van het Handelingsprotocol Veilig Thuis 2019.
g. een Reclasseringsinstelling: de goede uitvoering van taken van de reclasseringsinstelling, waaronder in het bijzonder taken zoals bedoeld in de Reclasseringsregeling 1995 artikel 8 lid 1.
h. een Gecertificeerde Instelling zoals bedoeld in de Jeugdwet artikel 1.1: de goede uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering zoals bedoeld in de Jeugdwet artikel 1.1.
i. een instelling voor Geestelijke Gezondheidszorg: de uitvoering van de taken bij behandeling, verpleging, verzorging en bejegening van personen met een psychische stoornis, inclusief verslaving met of zonder verblijf in het kader van de Wgbo of de Wet verplichte geestelijke gezondheidszorg.
j. een GGD: de uitvoering van de taken in het kader van de OGGZ op grond van artikel 1.2.1. sub a Wmo 2015.
k. de Dienst Justitiële Inrichtingen: de Dienst Justitiële Inrichtingen: voor de uitvoering van taken van de Minister van Justitie en Veiligheid, de selectiefunctionaris en de directeur van een justitiële inrichting op grond van de Beginselenwet justitiële jeugdinrichtingen, de Beginselenwet verpleging ter beschikking gestelden, de Penitentiaire beginselenwet en de wet Forensische zorg. De wettelijke grondslag voor de verwerking en verstrekking van persoonsgegevens is na inwerkingtreding van de wijziging van de Wet justitiële en strafvorderlijke gegevens (Wjsg) ter implementatie van de Europese richtlijn gegevensbescherming opsporing en vervolging gelegen in de Wjsg.
l. Slachtofferhulp Nederland: voor de uitvoering van de taken zoals genoemd in artikel 6 en 7 Wet Justitie subsidies jo. de Aanwijzing rechtspersoon slachtofferhulp [1], en artikel 51aa Wetboek van Strafvordering jo Besluit slachtoffers van strafbare feiten artikel 1^{e} en 3. De wettelijke grondslag voor de gegevensverwerking is mede gelegen in artikel 9 en/ of artikel 10 AVG jo art. 33 lid1a en art. 30 lid 3a en lid 4 UAVG. Met dien verstande dat gegevens aan de deelnemende partijen van het convenant alleen verstrekt kunnen worden met de uitdrukkelijke toestemming van de betrokkene.
m. Een aanbieder zoals bedoeld in de Wmo artikel 1.1.1, zorgaanbieder zoals bedoeld in de Wlz artikel 1.1.1, dan wel een jeugdhulpaanbieder zoals bedoeld in de Jeugdwet artikel 1.1: voor de verlening van voorzieningen en/of de uitvoering van zorg- dan wel hulpverleningstaken en voor zover dit noodzakelijk is in het kader van de behandeling of hulpverlening.

6.5 Op de persoonsgegevens die worden verwerkt, ingebracht, en/of verstrekt zoals bedoeld in artikel 5 zijn uitdrukkelijk de uitgangspunten van artikel 3.5 van toepassing en het bepaalde in artikel 7.

Toelichting:
Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de Gemeente §5.4 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door het Openbaar Ministerie §5.3 van het Handvat.

De Artikel 20 Wpg Beslissing wordt ondertekend door de gemandateerde politiechef van de betreffende eenheid en het bevoegd gezag, te weten de Burgemeesters en de Officier van Justitie.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de Politie §5.2 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de Reclassering §5.8 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de GGZ §5.5 van het Handvat.

Zie voor een nadere toelichting op de juridische basis voor de Verwerking van Persoonsgegevens door de GGD §5.5 van het Handvat.

Partijen dienen ieder voor zich vast te stellen op grond van welke wettelijke grondslag zij Persoonsgegevens in het kader van de samenwerking van het zorg- en veiligheidshuis Verwerken. Wanneer deze grondslag is gekoppeld aan materie-wetgeving, bijvoorbeeld omdat de betreffende Verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang, dient de betreffende materie-wetgeving waarin dit algemeen belang is beschreven, te worden benoemd. In artikel 6.4 a t/m m van dit protocol zijn voor een groot deel van de vaste partners in het zorg- en veiligheidshuis de taken die aan de orde kunnen zijn benoemd. Hoofdstuk 5 van het Handvat voorzetten voor nadere invulling hiervan.

Publieke instellingen dienen de Verwerking van Persoonsgegevens in het zorg - veiligheidshuis voor de in Artikel 3 genoemde doeleinden een grondslag in de wet te kunnen aanwijzen (artikel 6, onder e, AVG). Private partijen dienen te onderzoeken of zij (uitdrukkelijke) toestemming kunnen krijgen voor de Verwerking (artikel 6, onder a, AVG), danwel dat de Verwerking noodzakelijk is voor hun gerechtvaardigd belang en de belangen van de Betrokkene hier niet tegen opwegen (artikel 6, onder f, AVG).

Artikel 7. Doorverwerking geheimhoudingsbepalingen en toepassing toestemmingsvereiste

7.1 De geheimhoudingsbepaling van artikel 7 Wpg blijven rusten op de verstrekte gegevens. Dit geldt voor de ontvanger maar ook voor de tweede en derde ontvanger. Wanneer er over betrokkene in een eerder stadium op grond van artikel 16 lid 1b onder 2 Wpg politiegegevens zijn verstrekt aan de burgemeester óf op grond van artikel 15 Wpg politiegegevens ter beschikking zijn gesteld aan een Buitengewone Opsporingsambtenaar van een gemeente óf op grond van het Besluit politiegegevens (Bpg), voor een ander doel politiegegevens zijn verstrekt aan een van de convenantpartijen, dan worden deze gegevens door de desbetreffende ontvanger in principe niet als persoonsgegevens door verstrekt aan de procesregisseur van het Zorg- en Veiligheidshuis. Bij voorkeur worden door de politie op grond van artikel 20 Wpg opnieuw actuele politiegegevens verstrekt aan de procesregisseur van het Zorg- en Veiligheidshuis voor de doelen zoals genoemd in artikel 3.2, 3.3 en bijlage 2. De politie kan in uitzonderingsgevallen ook toestemming geven aan de ontvanger voor doorverstrekking aan de procesregisseur van het zorg- en veiligheidshuis maar legt deze toestemming vast in haar systemen.

7.2 Indien voor het inbrengen en/of verstrekken van persoonsgegevens zoals bedoeld in de artikelen 5.2 en 5.3 toestemming noodzakelijk is voor doorbreken geheimhoudingsbepalingen zoals bijvoorbeeld verwoord in de Wgbo (artikel 7:457 BW) en artikel 88 wet big, de beroepscode van de Jeugdzorgwerker artikel J, beroepscode NIP artikel 71 t/m 87 (psycholoog), of beroepscode NVO artikel 8 (pedagoog), de Reclasseringsregeling 1995 artikel 37, dan:

a. wordt deze gevraagd op het moment dat duidelijk is dat het inbrengen of verstrekken noodzakelijk is t.b.v. van de in de betreffende fase aan de orde zijnde doelen, of de uitvoering van de in 5.3.1 a t/m c genoemde activiteiten;
b. worden deze persoonsgegevens uitsluitend verstrekt voor zover hiervoor de uitdrukkelijke toestemming is verkregen van de betrokkene of diens wettelijke vertegenwoordiger;
c. legt de partij die de toestemming heeft verkrijgen deze schriftelijk vast en informeert Betrokkene dat hij zijn toestemming altijd weer kan intrekken;
d. draagt de partij die toestemming heeft verkregen bij intrekking van die toestemming er zorg voor dat er geen verdere verstrekkingen meer plaats vinden;
e. maakt de betrokken zorg- of hulpverlener een eigen afweging conform de voor hem geldende professionele standaarden, indien toestemming niet verkregen wordt en hij ervan overtuigd is dat zich hier een conflict van plichten voordoet, of goed hulpverlenerschap het verstrekken van persoonsgegevens verlangd.

Artikel 8. Documentatie individuele verstrekkingen

8.1. Indien Partijen daartoe verplicht zijn door voor hen geldende materiewetgeving, dan leggen zij de afzonderlijke verstrekkingen van Persoonsgegevens, inclusief onderbouwing van de noodzakelijkheid daarvan met het oog op de in artikel 5 en 6 vastgelegde grondslagen, vast. Dit geldt ten minste voor politie en OM. De politie documenteert iedere verstrekking conform de documentatieplicht van art 32 Wpg, het Openbaar Ministerie conform artikel 39j Wjsg.

Toelichting:

Sommige partijen zijn verplicht naast het verwerkingsregister ook afzonderlijke verstrekkingen vast te leggen. Dit geldt ten minste voor de Politie en het OM. Voor het Openbaar Ministerie geldt dat ten minste vastgelegd moet worden welke informatie verstrekt is, en wie de ontvangers (welke partijen) zijn van deze informatie. Deze informatie dient in ieder geval voor de duur van 4 jaar vastgelegd te zijn. Binnen het parket dienen goede afspraken gemaakt te worden met de privacy functionaris van het parket, zodat deze de informatie goed en makkelijk kan raadplegen. Dit is noodzakelijk om op een accurate wijze de rechten van betrokkenen te kunnen waarborgen.

De Documentatieplicht uit artikel 8 is iets anders dan het verstrekkingenregister uit de AVG zoals vermeld in artikel 24 van dit protocol.

Artikel 9. Dataminimalisatie

9.1 Partijen Verwerken niet meer Persoonsgegevens dat noodzakelijk met het oog op de in artikel 2.1 van dit Protocol geformuleerde doeleinden.

9.2 Ten behoeve van de Intake van een Casus verstrekt de Partij die de Casus bij de Procesregisseur aanmeldt enkel die Persoonsgegevens die noodzakelijk zijn voor de Procesregisseur om de Casus te toetsen aan de criteria van complexe casuïstiek zoals geformuleerd in Bijlage 2 van het Convenant. De Procesregisseur registreert enkel die Persoonsgegevens in het informatiesysteem van het zorg- en veiligheidshuis die noodzakelijk zijn voor Triage.

9.3 In het Casusoverleg Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn voor het opstellen en uitvoeren van een integraal plan van aanpak.

9.4 In het kader van Afschaling Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn om te bepalen of het plan van aanpak in het Casusoverleg tot de gewenste resultaten heeft geleid. Indien wordt besloten dat behandeling van de Casus in het zorg- en veiligheidshuis niet of niet langer noodzakelijk is, worden de betreffende Persoonsgegevens niet langer in het zorg- en veiligheidshuis Verwerkt. [*De Procesregisseur*] ziet erop toe dat Persoonsgegevens conform artikel 11 worden geanonimiseerd of vernietigd.

9.5 Wanneer de Partij die Persoonsgegevens in het zorg- en veiligheidshuis heeft verstrekt, kennis verkrijgt over de onjuistheid van die Persoonsgegevens, informeert die Partij de Casusregisseur en Procesregisseur hierover. De Procesregisseur coördineert de eventuele correctie van Persoonsgegevens in het zorg- en veiligheidshuis.

9.6 Enkel de [*Procesregisseur/Casusregisseur/Manager/administratief medewerker/afgevaardigden van Partijen in het Casusoverleg*] heeft*/hebben* toegang tot de Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het zorg- en veiligheidshuis en enkel voor zover noodzakelijk voor hun rol in een specifieke Casus.

Toelichting:

Beperkt zo veel mogelijk de toegang tot Persoonsgegevens die in en ten behoeve van het zorg- en veiligheidshuis worden Verwerkt. Enkel personen die ten behoeve van de uitvoering van de in artikel 3 omschreven doeleinden toegang tot bepaalde Persoonsgegevens nodig hebben, dienen die toegang te hebben. Handig is daarbij niet hetzelfde als noodzakelijk. De noodzakelijkheid van de gegeven autorisaties dient onderbouwd te kunnen worden indien daarom wordt gevraagd.

Artikel 10 Kwaliteit

10.1 Partijen dragen er zorg voor dat de Persoonsgegevens die zij in het kader van de onder artikel 3.2 geformuleerde doeleinden verstrekken toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn. De Partij die Persoonsgegevens in het zorg- en veiligheidshuis verstrekt blijft verantwoordelijk voor de juistheid, actualiteit en nauwkeurigheid van die Persoonsgegevens.

Artikel 11 Bewaren en Vernietigen

11.1 Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel of de doeleinden waarvoor ze worden Verwerkt zoals geformuleerd onder artikel 3 en met inachtneming van artikel 9.

11.2 Persoonsgegevens worden vernietigd zodra de Verwerking daarvan niet langer nodig is voor het doel waarvoor zij zijn Verwerkt, maar uiterlijk binnen *1 jaar* na het besluit tot Afschaling.

a. Persoonsgegevens kunnen tot zes maanden na besluit tot Afschaling worden bewaard in een vorm waarmee enkel […] toegang hebben tot de gegevens.
b. Na zes maanden na besluit tot Afschaling worden persoonsgegevens gearchiveerd en heeft enkel […] toegang tot die Persoonsgegevens.
c. Na één jaar na besluit tot Afschaling worden de Persoonsgegevens vernietigd.

11.3 Na één jaar kunnen gegevens, niet zijnde Persoonsgegevens, enkel worden bewaard voor managementdoeleinden.

Artikel 12 Beveiliging

12.1 Partijen dragen zorg voor passende technische en organisatorische beveiligingsmaatregelen om Persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige Verwerking zoals omschreven in Bijlage 3. Die maatregelen betreffen onder meer, maar niet uitsluitend, maatregelen met betrekking tot de toegang tot Persoonsgegevens, alsook het gebruik van beveiligde verbindingen voor de verstrekking van Persoonsgegevens.

12.2 Wanneer Persoonsgegevens aan andere Partijen worden verstrekt, gebeurt dit uitsluitend op een adequaat beveiligde manier, conform de geldende beveiligingsnormen voor de betreffende gegevens.

12.3 [*Naam Partij*] draagt zorg voor de adequate beveiliging van Persoonsgegevens die worden Verwerkt op locatie en in de informatiesystemen van het zorg- en veiligheidshuis en rapporteert hierover indien nodig aan de Stuurgroep.

12.4 [*De Manager/Procesregisseur*] is verantwoordelijk voor het toezien op de naleving van de beschermingsmaatregelen zoals geformuleerd in Bijlage 3 voor de Verwerking van Persoonsgegevens op locatie en in de informatiesystemen van het zorg- en veiligheidshuis en rapporteert hierover aan [*naam Partij zoals genoemd in artikel 12.3*] en is bevoegd aanwijzingen te geven aan Partijen omtrent de juiste omgang met Persoonsgegevens in dat verband.

Toelichting
Wanneer Persoonsgegevens aan andere Partijen worden verstrekt gebeurt dit met het oog op de gevoeligheid van de Persoonsgegevens en de mogelijke risico's voor Betrokkenen uitsluitend op een adequaat beveiligde manier. In het beveiligingsplan dienen hier richtlijnen voor te worden

opgenomen. De voorkeur heeft het dat de partij voor wie de gegevens zijn bedoeld deze kan inzien of op kan halen in een beveiligde omgeving en via een beveiligde verbinding. Het gebruik van email dient vermeden te worden. Indien dit bij uitzondering niet anders kan dient passende encryptie van de Persoonsgegevens plaats te vinden voor verstrekking.

Artikel 13 Geheimhouding

13.1. Een ieder die op grond van dit Protocol kennis neemt van Persoonsgegevens is verplicht tot geheimhouding daarvan, tenzij de wet tot bekendmaking verplicht. De Manager, Procesregisseur en eventueel ander ondersteunend personeel van het zorg- en veiligheidshuis worden door middel van een geheimhoudingsverklaring tot geheimhouding gebonden.

13.2. Partijen dragen er zorg voor dat iedere medewerker die in de uitvoering van het Convenant of dit Protocol in aanraking komt met Persoonsgegevens geheimhouding van die gegevens waarborgt.

13.3. Alle medewerkers van het zorg- en veiligheidshuis, inclusief medewerkers op basis van een dienstverleningsovereenkomst, deelnemers aan Casusoverleggen en overige afgevaardigden van Partijen die toegang hebben tot Persoonsgegevens die onder dit Protocol worden Verwerkt, beschikken over een positieve Verklaring Omtrent Gedrag, danwel hebben een veiligheidsonderzoek op grond van de voor de eigen organisatie geldende wet- en regelgeving doorlopen.

13.4. Wettelijke geheimhoudingsplichten zijn onverminderd van toepassing op eenieder die Strafrechtelijke persoonsgegevens of andere Bijzondere Persoonsgegevens in het kader van de samenwerking in het zorg- en veiligheidshuis ontvangt.

13.5. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van de politie en Openbaar Ministerie slechts verwerken voor het specifieke doel waarvoor deze zijn verstrekt ten behoeve van de Casus. Deze Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen indien het doel van de verdere verwerking verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de gegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.

13.6. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van andere Partijen die aan een geheimhoudingsplicht als onder meer bedoeld in de Wet Geneeskundige behandelovereenkomst (artikel 7:457 BW), Reclasseringsregeling 1995, Jeugdwet of Wet Maatschappelijke Ondersteuning zijn gebonden, slechts Verwerken voor het specifieke doel van de casus waarvoor deze zijn verstrekt. De Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen met toestemming van de verstrekkende Partij en indien het doel van de verdere verwerking verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de Persoonsgegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.

13.7. Wanneer de grond voor het verstrekken van de Persoonsgegevens als bedoeld in lid 7 gebaseerd is op toestemming van Betrokkene als bedoeld artikel 6 lid 1 onder a AVG en/of artikel 9 lid 2 onder a AVG en Betrokkene trekt deze toestemming in, laat de verstrekkende Partij dit aan de ontvangende Partij weten, waarbij ook de toestemming voor Verwerking en verdere Verwerking voor de ontvangende Partij vervalt.

Toelichting:

Het opzettelijk schenden van de geheimhoudingsplicht is strafbaar gesteld in artikel 272 Wetboek van strafrecht

Artikel 14 Datalekken

14.1. Partijen houden procedures in stand die er op gericht zijn om inbreuken in de beveiligingsmaatregelen zoals geformuleerd in Bijlage 3 met betrekking tot de bescherming van Persoonsgegevens redelijkerwijs te detecteren en daarop actie te ondernemen, daaronder begrepen maatregelen tot herstel.

14.2. [*Naam Partij*] is verantwoordelijk voor het in stand houden van procedures zoals bedoeld in artikel 14.1 voor de Verwerking van Persoonsgegevens op locatie of in de informatiesystemen van het zorg- en veiligheidshuis. [*De Manager/Procesregisseur*] ziet toe op de naleving van deze procedures in het zorg- en veiligheidshuis.

14.3. Partijen stellen [*de Manager/Procesregisseur*] onverwijld maar uiterlijk binnen […] uur na kennisneming op de hoogte van een inbreuk op persoonsgegevens in de zin van artikel 4, onder 12, AVG dan wel artikel 26g Wet justitiële en strafvorderlijke gegevens die een risico inhoudt voor de rechten en vrijheden van betrokkenen zoals bedoeld in artikel 33 AVG. Deze kennisgeving omvat in ieder geval:
   a. De aard en omvang van de inbreuk;
   b. De contactgegevens van de persoon bij wie meer informatie over de inbreuk kan worden verkregen;
   c. De maatregelen die kunnen worden genomen om de gevolgen van de inbreuk te voorkomen of beperken;
   d. De mogelijke gevolgen en risico's van de inbreuk op de bescherming van Persoonsgegevens voor de Betrokkene;
   e. De maatregelen die Partij zelf reeds heeft genomen of zal nemen om de bescherming van Persoonsgegevens te herstellen.

14.4. [De Manager/Procesregisseur] informeert Partijen middels het Partneroverleg schriftelijk over een inbreuk zoals bedoeld in artikel 14.3.

14.5. Partijen melden, indien wettelijk verplicht, een inbreuk zoals bedoeld in Artikel 14.3 bij de Autoriteit Persoonsgegevens. [*De Manager/Procesregisseur*] stuurt een afschrift van de melding aan de Autoriteit Persoonsgegevens aan het Partneroverleg en de Stuurgroep.

14.6. Wanneer een inbreuk als bedoeld in Artikel 14.3 waarschijnlijk een hoog risico voor de rechten en vrijheden van Betrokkene(n) zal inhouden als bedoeld in artikel 34 AVG, wordt deze over de inbreuk geïnformeerd. Partijen informeren de Betrokkene over de inbreuk. De beslissing tot melding aan de Betrokkene wordt in het Partneroverleg genomen. De inhoud van die melding wordt in het Partneroverleg afgestemd, danwel door het Partneroverleg aan één Partij gemandateerd.

14.7. Partijen verlenen elkaar de medewerking die redelijkerwijs van elkaar mag worden verwacht om aan de op Partijen rustende kennisgevingsverplichtingen te voldoen, mede met het oog op een eventueel onderzoek door de Autoriteit Persoonsgegevens.

14.8. Kennisgeving van de inbreuk aan de Autoriteit Persoonsgegevens door de Partijen gebeurt zonder onredelijke vertraging maar in ieder geval binnen 72 uur na ontdekking en geschiedt volgens de daartoe door de Autoriteit Persoonsgegevens ter beschikking gestelde procedure. De kennisgeving aan de Autoriteit Persoonsgegevens omvat minimaal:
   a. de aard van de inbreuk;
   b. een omschrijving van de categorieën Betrokkenen van wie Persoonsgegevens zijn betrokken bij de inbreuk;
   c. de categorieën Persoonsgegevens;
   d. of de Persoonsgegevens zijn versleuteld, geanonimiseerd, of anderszins onbegrijpelijk zijn gemaakt;

e. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
f. de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de Persoonsgegevens en de maatregelen die Partij heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

14.9. Kennisgeving van de inbreuk aan Betrokkene zoals bedoeld in Artikel 14.5 is niet vereist indien:
a. passende technische en organisatorische maatregelen zijn genomen die de bescherming van Persoonsgegevens ook na de inbreuk garanderen;
b. achteraf genomen maatregelen de waarschijnlijkheid op een hoog privacy risico hebben weggenomen, of;
c. wanneer mededeling aan Betrokkene een onevenredig inspanning zou vragen.

14.10. Voorts kan de mededeling aan betrokkene worden uitgesteld, beperkt of achterwege gelaten worden, indien de inbreuk enkel ziet op gegevens afkomstig van het Openbaar Ministerie, en indien dit noodzakelijk en evenredig is:
a. ter vermijding van belemmering van gerechtelijke onderzoeken of procedures;
b. ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
c. ter bescherming van de openbare veiligheid;
d. ter bescherming van de rechten en vrijheden van derden;
e. ter bescherming van de nationale veiligheid.

14.11. Partijen houden een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van de Persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen, alsmede de tekst van de kennisgeving aan de Betrokkene. [*De Manager/Procesregisseur*] houdt een overzicht bij van gelijksoortige inbreuken die plaatsvinden op locatie of in de informatiesystemen van het zorg- en veiligheidshuis.

Artikel 15 Privacy by Design

15.1. Voorafgaand aan een (nieuwe) Verwerkingen onder dit Protocol, of de inzet van nieuwe technologieën voor de Verwerkingen onder dit Protocol, voeren Partijen middels het Partneroverleg een Gegevensbeschermingseffectbeoordeling uit conform artikel 35 AVG. De [*Procesregisseur/Manager*] coördineert dit proces.

15.2. Bij de uitvoering van de Gegevensbeschermingseffectbeoordeling wordt het model Gegevensbeschermingseffectbeoordeling Rijksdienst gevolgd.

15.3. Bij een voornemen omtrent de inzet van nieuwe technologieën kan dit voornemen ter advies worden voorgelegd aan het Landelijk Overleg Managers Veiligheidshuizen. Het Landelijk Overleg Managers Veiligheidshuizen kan advies uitbrengen over de beoogde inzet van nieuwe technologieën.

15.4. De uitkomsten van de Gegevensbeschermingseffectbeoordeling worden ter besluitvorming voorgelegd aan de Stuurgroep. De Stuurgroep kan hiervoor advies vragen , aan het Partneroverleg over de voorgenomen nieuwe Verwerking zoals bedoeld in artikel 15.1. De Stuurgroep legt waar nodig op grond van artikel 36 AVG namens alle gezamenlijke Verwerkingsverantwoordelijken de beoogde Verwerking voor aan de Autoriteit Persoonsgegevens.

Artikel 16 Informatieverstrekking aan Betrokkenen

16.1. Vóór het verstrekken van Persoonsgegevens in het kader van de samenwerking wordt Betrokkene door de verstrekkende Partij, danwel de Partij die de Casusregie voert, geïnformeerd over het voornemen diens Persoonsgegevens verder te Verwerken in het kader van samenwerking in het zorg- en veiligheidshuis onder dit Protocol.

16.2. Deze informerende Partij maakt de het tijdstip waarop en de wijze van informeren kenbaar aan de overige bij een Casus betrokken Partijen.
16.3. [*De Manager/Procesregisseur*] draagt zorg voor het publiceren van een privacy statement op de website van het zorg- en veiligheidshuis.
16.4. Alle deelnemende partijen zorgen op hun eigen website voor vermelding van deelname aan het zorg- en veiligheidshuis en voor een verwijzing naar de website van het betreffende zorg- en veiligheidshuis/de Veiligheidshuizen waaraan zij deelnemen, alsook voor verwijzing naar het zorg- en veiligheidshuis convenant(en) en het privacyprotocol(len).
16.5. De onder artikel 16.1 bedoelde informatieverstrekking, alsook het onder artikel 16.3 genoemde privacy statement, bevatten ten minste de volgende informatie:
   a. De doeleinden voor de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis zoals beschreven in artikel 3.2.
   b. De Partijen die deelnemen aan de samenwerking in het zorg- en veiligheidshuis;
   c. De termijn waarvoor de Persoonsgegevens worden opgeslagen en bewaard zoals omschreven onder artikel 11, danwel de criteria voor het bepalen van die termijn;
   d. Dat Betrokkene verscheidene rechten heeft met betrekking tot de Verwerking van diens Persoonsgegevens zoals geformuleerd onder artikel 17 tot en met 21;
   e. Indien de Verwerking van Persoonsgegevens is gebaseerd op toestemming, dat Betrokkene het recht heeft deze te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de Verwerking van de Persoonsgegevens die heeft plaatsgevonden vóór intrekking van de toestemming;
   f. Dat Betrokkene het recht heeft een klacht in te dienen over de Verwerking van zijn of haar Persoonsgegevens onder dit Protocol bij het zorg- en veiligheidshuis en bij de Autoriteit Persoonsgegevens;
   g. Nadere uitleg indien de Persoonsgegevens moeten worden verstrekt of verder Verwerkt op grond van een wettelijke of contractuele verplichting;
   h. Nadere uitleg indien Betrokkene verplicht is de Persoonsgegevens te verstrekken;
   i. Indien sprake is van geautomatiseerde besluitvorming, met inbegrip van profilering, uitleg over de achterliggende logica, het belang van de verwerkingsactiviteiten en de verwachte gevolgen voor de Betrokkene.
   j. De contactgegevens van de [*De Manager/Procesregisseur*] bij wie de Betrokkene terecht kan voor meer informatie over de Verwerking van zijn Persoonsgegevens, dan wel waar hij zijn rechten geldend kan maken.

***Toelichting**:*
Het verdient aanbeveling de uitoefening van de rechten van de Betrokkene te centraliseren. Door een online statement te plaatsen met duidelijke contactgegevens en de Manager de uitvoering van de verplichting van Partijen te laten coördineren, is het proces rondom de wijze waarop invulling wordt gegeven aan de rechten van de Betrokkene door Partijen optimaal belegd. Wanneer de partijen van mening verschillen over de gegevens die in geval van een inzageverzoek wel of niet moeten worden verstrekt dan wordt dit besproken in het casusoverleg en zo nodig in het Partneroverleg.

16.6. De informatieverplichting zoals bedoeld in artikel 16.1 is niet van toepassing indien het achterwege laten van informeren van Betrokkene noodzakelijk is in het belang van:
   a. De veiligheid van de staat;
   b. De voorkoming, opsporing en vervolging van strafbare feiten;
   c. Gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
   d. Het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of;

e. De bescherming van de betrokkene of van de rechten en vrijheden van anderen.

16.7. Partijen leggen de motivatie voor het niet voldoen aan de informatieplicht op grond van Artikel 16.6 schriftelijk vast en leggen vast wanneer zij verwachten dat betrokkene wel geïnformeerd kan worden, alsook van welke omstandigheden dit afhankelijk is, hoe periodiek wordt getoetst of deze omstandigheden nog aanwezig zijn en hoe dan wel wanneer Betrokkene geïnformeerd zal worden.

Artikel 17 Rechten van de Betrokkenen

17.1. Betrokkenen kunnen bij Partijen een verzoek indienen om:
   a. Inzage te krijgen in de Persoonsgegevens die door Partijen over hem of haar worden Verwerkt;
   b. Correctie of verwijdering van de hem betreffende Persoonsgegevens dan wel beperking van de Verwerking;
   c. bezwaar te maken tegen de Verwerking;
   d. zijn of haar Persoonsgegevens over te dragen.

17.2. Verzoeken door Betrokkene ten aanzien van Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het zorg- en veiligheidshuis worden gecoördineerd door de [*Manager/Procesregisseur*]. [*De Manager/Procesregisseur*] wordt hierbij ondersteund door de [*Procesregisseur/administratief medewerker*]. [*De Manager/Procesregisseur*] legt het verzoek via de Procesregisseur voor aan het Casusoverleg en stemt daarin met Partijen de beantwoording van het verzoek af.

17.3. Indien het verzoek als bedoeld in Artikel 17.1 direct is gericht aan een der Partijen wordt de Manager hierover zo spoedig mogelijk door die Partij in kennis gesteld, opdat deze de beantwoording van het verzoek conform artikel 17.2 kan coördineren. Beantwoording van het verzoek door de Partij wordt in het Partneroverleg afgestemd.

17.4. Het bepaalde in artikel 17.2 en artikel 17.3 ontslaat Partijen niet van diens verantwoordelijkheid als Verwerkingsverantwoordelijke ten aanzien van een verzoek van Betrokkene.

17.5. Artikel 17.1 t/m 17.4, alsmede de artikelen 18, 19 en 20 zijn niet van toepassing op gegevens die verstrekt zijn door het College van procureurs-generaal. Op deze gegevens is de Wet justitiële en strafvorderlijke gegevens van toepassing. Verstrekkingen van gegevens door het College van procureurs-generaal worden ingevolge artikel 8 van dit Protocol en artikel 39j Wjsg schriftelijk vastgelegd en bewaard voor de duur van 4 jaar. Inzage- en rectificatieverzoeken worden beoordeeld door de privacyfunctionaris van het verstrekkende parket van het Openbaar Ministerie. Verzetschriften tegen verwerking van gegevens worden beoordeeld door de afdeling Bestuurlijke en juridische zaken van het Parket-Generaal.

17.6. Op gegevens die eerder verstrekt zijn door de politie is de geheimhoudingsplicht van de Wet politiegegevens van toepassing. Derhalve zijn artikel 18, 19 en 20 van dit Protocol niet van toepassing. Inzage- en correctieverzoeken worden beoordeeld door het Wpg loket van de verstrekkende eenheid van de politie. Verzet- en bezwaarschriften tegen verwerking van gegevens worden beoordeeld door de privacyfunctionaris en/of jurist van de verstrekkende eenheid van de politie, conform art. 29 Wpg.

Artikel 18 Recht op inzage

18.1. In het geval het verzoek ziet op inzage in de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis door Partijen zoals bedoeld in artikel 17.1 onder a, dient de beantwoording van

dat verzoek een volledig overzicht in begrijpelijke vorm met ten minste de volgende informatie te bevatten:

a) de verwerkingsdoeleinden;

b) de betrokken categorieën van Persoonsgegevens;

c) de ontvangers of categorieën van ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;

d) 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;

e) dat de Betrokkene het recht heeft de Verwerkingsverantwoordelijke(n) 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;

f) dat de Betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;

g) wanneer de Persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;

h) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4 AVG 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.

18.2. Het verzoek wordt binnen vier weken door de Manager beantwoord. Een verzoek tot inzage wordt enkel geweigerd, indien en voor zover dit noodzakelijk is met het oog op in de wet gespecificeerde weigeringsgronden.

18.3. Een eventuele (gedeeltelijke) afwijzing is schriftelijk en gemotiveerd.

18.4. Alvorens aan een verzoek als bedoeld in artikel 17.1 wordt voldaan, verifiëren Partijen de identiteit van de Betrokkene die het verzoek indient. Betrokkene dient hiervoor persoonlijk langs te komen bij het zorg- en veiligheidshuis.

18.5. Bij voldoen aan een verzoek als bedoeld in artikel 17.1, verstrekt de Manager namens de Verwerkingsverantwoordelijke aan de Betrokkene een kopie van de Persoonsgegevens die worden verwerkt.

Artikel 19 Recht op correctie en verwijdering

19.1. Indien de Betrokkene op grond van zijn verzoek om inzage een verzoek tot correctie of verwijdering van bepaalde hem of haar betreffende Persoonsgegevens zoals bedoeld in artikel 17.1 onder b doet bij het zorg- en veiligheidshuis, legt de [*Manager/Procesregisseur*] dit verzoek voor aan het Partneroverleg met het oog op de beoordeling van het verzoek.

19.2. Onjuiste Persoonsgegevens betreffende de Betrokkene worden op diens verzoek onverwijld gecorrigeerd.

19.3. Persoonsgegevens betreffende de Betrokkene worden zonder onredelijke vertraging op diens verzoek verwijderd wanneer deze:

a. voor het doel van de Verwerking onvolledig of niet ter zake dienend zijn; of
b. anderszins in strijd met een wettelijk voorschrift worden Verwerkt.

19.4. [*De Manager/Procesregisseur*] informeert de Betrokkene over de beslissing omtrent zijn verzoek tot correctie of verwijdering van hem of haar betreffende Persoonsgegevens schriftelijk en gemotiveerd zo spoedig mogelijk, maar uiterlijk binnen 4 weken na ontvangst van het verzoek.

Artikel 20 Recht op verzet

20.1. Indien de Verwerking van Persoonsgegevens door Partijen is gebaseerd op de grondslagen van artikel 6 Algemene Verordening Gegevensbescherming, kan de Betrokkene daartegen te allen tijde verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

20.2. Indien een verzoek tot verzet door Betrokkene bij één der Partijen wordt ingediend, informeert die Partij onverwijld de [*Manager/Procesregisseur*] over het ingediende verzoek.

20.3. [*De Manager/Procesregisseur*] legt het door Betrokkene ingeroepen recht tot verzet voor aan het Partneroverleg om te beoordeling of het verzoek gerechtvaardigd is en coördineert de afhandeling daarvan.

20.4. [*De Manager/Procesregisseur*] informeert de Betrokkene over de beslissing zoals bedoeld in artikel 17.3 binnen 4 weken en draagt er zorg voor dat de beslissing binnen deze 4 weken wordt uitgevoerd. Een beslissing om niet, of niet geheel, te voldoen wordt altijd gemotiveerd en kan met het oog op artikel 21 AVG enkel worden gebaseerd op dwingende gerechtvaardigde gronden.

Artikel 21 Recht op overdraagbaarheid van Persoonsgegevens

21.1. Het recht op overdraagbaarheid van Persoonsgegevens is niet van toepassing op Partijen in het zorg- en veiligheidshuis.

Toelichting:

Overdraagbaarheid van gegevens is niet van toepassing op Verwerkingsverantwoordelijken die Persoonsgegevens Verwerken het kader van de uitoefening van een wettelijke verplichting, een taak van algemeen belang of in het kader van de uitoefening van openbare taken (zie de Overwegingen 68 en 69).

Artikel 22 Verwerkers

22.1. Partijen besteden de Verwerking van Persoonsgegevens onder dit Protocol niet uit zonder dat de […] tevoren schriftelijk toestemming heeft gegeven over de beoogde verandering inzake de inzet van Verwerkers die ten behoeve van het zorg- en veiligheidshuis Persoonsgegevens Verwerken. Een overeenkomst van opdracht tussen Partijen en een door […] goedgekeurde Verwerker inzake Verwerking van Persoonsgegevens dient ten minste hetzelfde beschermingsniveau te bieden aan de belangen van Betrokkene als het onderhavige Protocol. Meer in het bijzonder moet de Bewerker voor de Verwerkingen van Persoonsgegevens in het kader van dit Protocol een vergelijkbaar niveau van beveiliging garanderen als in Bijlage 3 van dit Protocol.

22.2. Partijen leggen de afspraken tussen hen en Verwerkers(s) omtrent de omgang met Persoonsgegevens die Bewerker ten behoeve van Partijen Verwerkt, in een schriftelijke overeenkomst vast. […] is bevoegd deze overeenkomst namens Partijen aan te gaangaan.

22.3. [*De Manager/Procesregisseur*] houdt een lijst bij van de overeenkomsten die met schriftelijke toestemming van de […] zijn overeengekomen, welke lijst minimaal eenmaal per jaar wordt bijgewerkt. Deze lijst zal beschikbaar worden gehouden ten behoeve van Partijen en de toezichthouder.

Artikel 23. Verstrekking aan derden

23.1. Persoonsgegevens die in het kader van dit Protocol worden Verwerkt, worden niet verstrekt aan anderen dan deelnemers aan het Casusoverleg, behoudens het bepaalde in Artikel 19 en tenzij Partijen hiertoe wettelijk verplicht zijn. Deze verstrekking wordt schriftelijk vastgelegd door [*De Manager/Procesregisseur*].

23.2. Indien een verstrekking van Persoonsgegevens aan derden plaatsvindt, is dat een individuele afweging van elke Partij op grond van zijn eigen wet- en regelgeving.

Artikel 24. Verwerkingsregister en Functionaris Gegevensbescherming

24.1. Partijen registeren hun Verwerkingen van Persoonsgegevens onder dit Protocol in een eigen register van verwerkingsactiviteiten.

24.2. Aanvullend neemt [de Manager/Procesregisseur] de Verwerkingen van Persoonsgegevens op locatie en in de informatiesystemen van het zorg- en veiligheidshuis op in een gezamenlijk register van verwerkingsactiviteiten onder dit Protocol ten behoeve van Partijen.

24.3. Het register van verwerkingsactiviteiten bevat minimaal de volgende informatie:

a. De naam en contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken (of diens vertegenwoordiger);
b. De verwerkingsdoeleinden;
c. Een beschrijving van de categorieën Persoonsgegevens die worden Verwerkt;
d. Een beschrijven van de categorieën Betrokkenen;
e. De categorieën van ontvangers aan wie de Persoonsgegevens worden (of zullen worden) verstrekt;
f. Indien van toepassing, doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.

24.4. De Functionarissen Gegevensbescherming van de afzonderlijke Partijen hebben, zonder aankondiging van bezoek vooraf, recht op toegang tot de gebouwen en overlegruimtes van het zorg- en veiligheidshuis en tot de Verwerkingen en register van Verwerkingen, alsook toegang tot enige andere informatie, voor zover dit noodzakelijk is voor diens toezichthoudende werkzaamheden.

24.5. De Privacy Adviseur van het zorg- en veiligheidshuis dient als eerste aanspreekpunt voor de betrokken Functionarissen Gegevensbescherming.

24.6. De Functionarissen Gegevensbescherming van de Verwerkingsverantwoordelijken houden toezicht op de naleving van de verplichtingen in dit Protocol en zijn bevoegd aanwijzingen te geven aan de Manager en Procesregisseur.

Artikel 25. Aansprakelijkheid

Toelichting:

Bepaal gezamenlijk hoe wordt omgegaan met aansprakelijkheid op grond van de uitvoering van dit Protocol. Wat als het delen van Persoonsgegevens in het zorg- en veiligheidshuis leidt tot een boete van de Autoriteit Persoonsgegevens of een claim van een Betrokkene op schadevergoeding? Er zijn veel scenario's denkbaar. Hieronder is een voorbeeld opgenomen waarin onderscheid is gemaakt tussen schade die het gevolg is van niet-nakoming door één der Partijen en de situatie waarin de gezamenlijke gegevensverwerking heeft geleid tot schade bij derden of tot boetes en de situatie waarin de samenwerking leidt tot schade bij een Partij.

25.1. Partijen zetten zich in voor een goede uitvoering van het bepaalde in dit Protocol en zullen zich houden aan de dienaangaande in dit Protocol gemaakte afspraken.
25.2. Partijen zijn ieder voor zich aansprakelijk voor aanspraken van Betrokkenen, of Derden op schadevergoeding op grond van directe of indirecte schade, administratieve boetes of andere aanspraken van derden in geval van toerekenbare tekortkoming door de aangesproken Partij in de nakoming van het bepaalde in dit Protocol en de bijbehorende Bijlagen.
25.3. Wanneer meerdere Verwerkingsverantwoordelijken of Verwerkers bij dezelfde Verwerking betrokken zijn, en verantwoordelijk zijn voor schade die door die Verwerking is veroorzaakt, wordt elke Verwerkingsverantwoordelijke of Verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk wordt vergoed.
25.4. Een Verwerker is slechts aansprakelijk voor de schade die door Verwerking is veroorzaakt wanneer bij de Verwerking niet is voldaan aan de specifiek tot Verwerkers gerichte verplichtingen van de Algemene Verordening Gegevensbescherming of buiten dan wel in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke is gehandeld.
25.5. Onverminderd het gestelde in lid 4 kan iedere Verwerkingsverantwoordelijke of Verwerker die de volledige vergoeding heeft betaald vervolgens bij de andere Verwerkingsverantwoordelijken of Verwerkers die bij dezelfde Verwerking betrokken zijn, het deel van de schadevergoeding verhalen dat overeenkomt met hun deel van de aansprakelijkheid voor de schade. Een Verwerkingsverantwoordelijke of Verwerker kan door andere Verwerkingsverantwoordelijken of Verwerkers worden vrijgesteld van onderlinge betaling van schadevergoeding indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

Artikel 26. Toezicht en handhaving

26.1. Onverminderd de verantwoordelijkheden van de Functionarissen Gegevensbescherming van de verwerkingsverantwoordelijken houden de Manager en de Procesregisseur toezicht op de naleving van de verplichtingen in dit Protocol en zijn bevoegd aanwijzingen te geven aan medewerkers in het zorg- en veiligheidshuis omtrent de uitvoering van het bepaalde in dit Protocol.

Artikel 27. Wijzigingen

27.1. De bepalingen in dit Protocol kunnen door de Partijen in gezamenlijk overleg worden gewijzigd. Wijzigingen in dit Protocol worden door de [*Stuurgroep/het Partneroverleg*] besloten. Mondelinge mededelingen, toezeggingen of afspraken welke betrekking hebben op de inhoud van dit Protocol, hebben geen rechtskracht, tenzij deze uitdrukkelijk schriftelijk zijn bevestigd door [de Stuurgroep/het Partneroverleg].
27.2. Wijziging van het Protocol vergt het opnieuw ondertekenen door Partijen van het gewijzigde Protocol.
27.3. In geval van wijzigingen, waaronder inbegrepen toetreding van een nieuwe organisatie tot dit Protocol, die door een Partij onaanvaardbaar worden ervaren, kan deze Partij deelname aan het zorg- en veiligheidshuis schriftelijk opzeggen met ingang van het tijdstip waarop het gewijzigde Protocol van kracht wordt. Na opzegging van deelname aan het Convenant en dit Protocol verkrijgt die Partij niet langer toegang tot de Persoonsgegevens die op locatie of in de informatiesystemen van het zorg- en veiligheidshuis worden verwerkt onder dit Protocol.

Artikel 28. Toetreding

28.1. Toetreding door andere organisaties tot dit Protocol kan enkel wanneer die Partij is toegetreden tot het Convenant conform Artikel 20 van dat Convenant.

28.2. Partijen worden vooraf door de secretaris van de Stuurgroep op de hoogte gebracht van de voorgenomen toetreding. Indien de toetredende partij niet staat benoemd in het Handvat dient voorafgaand aan de uitwisseling van Persoonsgegevens met de toetredende partij een juridische analyse te worden opgesteld conform hoofdstuk 5 van het Handvat. De toetredende Partij voert waar nodig de aanbeveling uit die analyse uit, alvorens uitwisseling van Persoonsgegevens in het zorg- en veiligheidshuis met die partij plaatsvindt.
28.3. In geval van toetreding tot het Convenant, vindt toetreding tot het Protocol plaats door middel van ondertekening van Bijlage 1 bij dit Protocol door die andere organisatie en de [voorzitter van de Stuurgroep].

Artikel 29. Duur, opzegging, beëindiging

29.1. Dit Protocol treedt in werking op de dag van ondertekening door Partijen en wordt voor dezelfde duur als het Convenant. In geval van verlenging van het Convenant wordt dit Protocol met een gelijkluidende termijn verlengt.
29.2. *[De Stuurgroep*] kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een Partij met onmiddellijke ingang uitsluiten van de samenwerking in het zorg- en veiligheidshuis, indien de afspraken zoals neergelegd in dit Protocol niet door de desbetreffende Partij worden nagekomen.
29.3. Verplichtingen die naar hun aard zijn bestemd om ook na beëindiging of uitsluiting van het project voort te duren, blijven na beëindigingen van dit Protocol bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding en de beveiliging van Persoonsgegevens.

Artikel 30. Opvolging

30.1. Dit Protocol vervangt alle eerdere door Partijen gesloten Protocollen met betrekking tot de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis voor de doelen zoals beschreven in Artikel 3.1 van dit Protocol.

Artikel 31. Monitoring, toezicht, audit, wetenschappelijk onderzoek en evaluatie

a. In het kader van een opdracht tot uitvoering van een wetenschappelijk onderzoek
31.2. zijn Partijen gezamenlijk opdrachtgever en worden de specifieke bepalingen uit wet- en regelgeving alsmede de interne voor Partijen geldende voorschriften voor wetenschappelijk onderzoek van Partijen in acht genomen.
   a. Partijen zullen dit Protocol twee jaar na inwerking treden landelijk en regionaal evalueren, waarbij bij voorkeur een audit zal plaatsvinden door een externe onafhankelijke partij.

Artikel 32. Toepasselijk recht

32.1. Op dit Protocol is Nederlands recht van toepassing.

Aldus overeengekomen:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

[Naam Partij]

in dezen rechtsgeldig vertegenwoordig door: [*naam en functie]*

Datum en plaats:

Bijvoegsel 1 bij Privacy Protocol: Toetredingsformulier nieuwe partner tot Protocol

[naam organisatie], statutair gevestigd te […] en kantoorhoudend aan […], hierbij rechtsgeldig vertegenwoordigd door [naam, functie],

overwegende dat:

- Deelname aan het Protocol gelet op de publieke en/of maatschappelijke taak die zichzelf in het kader van integrale veiligheid en complexe casuïstiek toedicht en gelet op de verantwoordelijkheid en/of bevoegdheid van ondergetekende een bijdrage levert aan de doelstelling zoals geformuleerd in artikel 2 van het Convenant en artikel 3.2 van het Protocol;
- De Stuurgroep positief heeft besloten op toetreding van ondergetekende aan het Convenant en dit Protocol;

verklaart daartoe het volgende:

- Ondergetekende onderschrijft de in het Protocol geformuleerde doelstellingen, verplicht zich de bepalingen in het Protocol te zullen naleven en verklaart zich in dit kader gerechtigheid tot het uitwisselen van Persoonsgegevens met Partijen.

Aldus ondertekend te […], op datum […]

Naam organisatie:

Naam bevoegde functionaris:

…….

Namens Stuurgroep:

Naam:

……

Bijvoegsel 2 bij Privacy Protocol:

Doeleinden verwerking van persoonsgegevens per processtap

Partijen Verwerken in het kader van het zorg- en veiligheidshuis voor ieder van onderstaande fasen enkel de Persoonsgegevens die voor die afzonderlijke fase noodzakelijk zijn voor de uitvoering van ieder van de daarbij geformuleerde toepasselijke processtappen: Hier verwijzen naar het vertaaldocument waarin alle processtappen zijn beschreven.

Intake / Aanmelding

- Beoordelen of een Casus die door een Partij wordt aangedragen voldoet aan de criteria voor behandeling in het zorg- en veiligheidshuis. Deze criteria volgen uit het Landelijk Kader.

Triage

- Bepalen eerste beeld en verrijken van informatie uit Intake;
- Op basis van informatie van partners komen tot een nadere afweging ten aanzien van de routering van de casus, tot een bepaling van doel en thema's van een eventueel casusoverleg, en tot een afweging welke partners relevant zijn om te betrekken bij een casusoverleg;
- Voorbereiding Casusoverleg.

Casusoverleg

- Opstellen gezamenlijk toestandbeeld door bij het Casusoverleg betrokken Partijen;
- Opstellen integraal plan van aanpak;
- Monitoren van de uitvoering en resultaten van het plan van aanpak;
- Bepalen of verdere verstrekking van Persoonsgegevens aan andere samenwerkingsverbanden noodzakelijk en mogelijk is;
- Besluiten tot afbouwen betrokkenheid zorg- en veiligheidshuis;
- Besluiten tot Opschaling van de Casus;

Afschaling

- Bepalen van noodzakelijke te verstrekken Persoonsgegevens in het kader van Afschaling en de verstrekking daarvan aan bijvoorbeeld de Casusregisseur;

Bijvoegsel 3 bij Privacy Protocol: Beveiligingsbeleid persoonsgegevens

Partijen dienen een beleid op te stellen dat ziet op de bescherming van Persoonsgegevens. Hiervoor kan aansluiting worden gezocht bij het informatiebeveiligingsbeleid, doch daar dient dan expliciet aandacht te worden besteed aan de technische en organisatorische maatregelen ten behoeve van de bescherming van Persoonsgegevens. Deze maatregelen dienen passend te zijn met het oog op het risico voor Betrokkenen en conform de "Cbp Richtsnoeren – Beveiliging van persoonsgegevens" ten minste het volgende te bevatten:

- **Beleidsdocument voor informatiebeveiliging**
  Het beleidsdocument gaat expliciet in op de maatregelen die de verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.
- **Toewijzen van verantwoordelijkheden voor informatiebeveiliging**
  Alle verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, zijn duidelijk gedefinieerd en belegd.
- **Beveiligingsbewustzijn**
  Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met persoonsgegevens.
- **Fysieke beveiliging en beveiliging van apparatuur**
  ITvoorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.
- **Toegangsbeveiliging**
  Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen. De procedures omvatten alle fasen in de levenscyclus van de gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en diensten nodig hebben. Waar van toepassing wordt bijzondere aandacht besteed aan het beheren van toegangsrechten van gebruikers met extra ruime bevoegdheden, zoals systeembeheerders.
- **Logging en controle**
  Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrecht matige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.
  De verantwoordelijke moet er rekening mee houden dat er, als de gegevens in de logbestanden tot personen herleidbaar zijn, sprake is van een verwerking van persoonsgegevens in de zin van de [AVG] waarop de verplichtingen uit deze wet van toepassing zijn. In dat geval kan er ook sprake zijn van een personeelsvolgsysteem in de zin van artikel 27 lid 1 van de Wet op de ondernemingsraden (WOR), waarvoor instemming van de ondernemingsraad is vereist.

- **Correcte verwerking in toepassingssystemen**
  In alle toepassingssystemen, inclusief toepassingen die door gebruikers zelf zijn ontwikkeld, zijn beveiligingsmaatregelen ingebouwd. Tot deze beveiligingsmaatregelen behoort de controle dat de invoer, de interne verwerking en de uitvoer aan vooraf gestelde eisen voldoen (validatie). Voor systemen waarin bijzondere of strafrechtelijke persoonsgegevens worden verwerkt of die invloed hebben op de ver werking van bijzondere of strafrechtelijke persoonsgegevens, kunnen aanvullende beveiligingsmaatregelen nodig zijn.
- **Beheer van technische kwetsbaarheden**
  Software, zoals browsers, virusscanners en operating systems, wordt up-to-date gehouden. Ook installeert de verantwoordelijke tijdig oplossingen die de leverancier uitbrengt voor beveiligingslekken in deze software. Meer in het algemeen verkrijgt de verantwoordelijke tijdig informatie over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden wordt geëvalueerd en de verantwoordelijke treft geschikte maatregelen getroffen voor de behandeling van de risico's die daarmee samenhangen.
- **Incidentenbeheer**
  Er zijn procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd. Het beoordelen van de risico's voor de betrokkenen en het effectief informeren van de betrokkenen en, waar van toepassing,
  de toezichthouder is in deze procedures opgenomen. De lessen getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging waar mogelijk structureel te verbeteren. Als een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
- **Afhandeling van datalekken en beveiligingsincidenten**
  De verantwoordelijke meldt datalekken die onder een wettelijke meldplicht vallen bij de betreffende toezichthouder.73 Als hij daartoe wettelijk verplicht is, of als er anderszins aanleiding voor is, informeert hij ook de betrokkenen over het beveiligingsincident of het datalek.
- **Continuïteitsbeheer**
  Door natuurrampen, ongevallen, uitval van apparatuur of opzettelijk handelen kunnen persoons gegevens verloren gaan. Door in de organisatie continuïteitsbeheer in te richten worden de gevolgen tot een aanvaardbaar niveau beperkt, waarbij gebruik wordt gemaakt van een combinatie van preventieve maatregelen en herstelmaatregelen.

Er is pas sprake van een passend beveiligingsniveau als de gekozen maatregelen onderdeel zijn van de dagelijkse praktijk van de organisatie. De eerste stap is documentatie: de relevante beveiligingsmaatregelen zijn gespecificeerd en geïntegreerd in functionele en technische beschrijvingen van ICT systemen, in gebruikershandleidingen, werkinstructies, contracten, dienstenniveauovereenkomsten en andere relevante documenten. De tweede stap is daadwerkelijke implementatie van de gekozen maatregelen.

Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen."

De hierboven genoemde maatregelen ‘beveiligingsbewustzijn’, ‘toegangsbeveiliging’ en ‘logging en controle’ zijn er mede op gericht om ongeoorloofde omgang met persoonsgegevens binnen de organisatie tegen te gaan. “

De Autoriteit Persoonsgegevens sluit hierbij grotendeels aan op de EN-ISO/IEC 27002:2007. Voor de Verwerking van bijzondere Persoonsgegevens, meer in het bijzonder gegevens betreffende iemands gezondheid, verwijst de Autoriteit Persoonsgegevens ook naar de NEN7510.

Bijvoegsel 4 bij Privacy Protocol:
Categorieën persoonsgegevens en betrokkenen

Partijen Verwerken ten behoeve van de doelstellingen en onder voorwaarden zoals beschreven in dit Protocol enkel de volgende categorieën Persoonsgegevens van de volgende categorieën Betrokkenen:

Categorie 1:

Categorie Betrokkenen:

Van Personen, op wie het onder dit Protocol beschreven plan van aanpak en bijbehorende interventies zijn gericht, worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:.

Persoonsgegevens:

- volledige personalia (naam, geboorteplaats, geboortedatum);
- adresgegevens (straat, huisnummer, postcode, woonplaats);
- contactgegevens (telefoonnummer, e-mailadres);
- gegevens omtrent woonsituatie;
- financiële gegevens;
- gegevens betreffende relaties met overige gezinsleden/ directe sociale contacten;
- toezicht- en handhavingsgegevens, gegevens omtrent bestuursrechtelijke maatregelen of voornemens daartoe

Strafrechtelijke Persoonsgegeven, te weten:

- Politiegegevens (artikel 8 en 13 Politiegegevens);
- Strafvorderlijke gegevens en relevante justitiële gegevens;
- Tenuitvoerleggingsgegevens

Bijzondere Persoonsgegevens, te weten:

- […]
- […]

Categorie 2:

Categorie Betrokkenen:

Van directe relaties van Categorie1 Betrokkenen, waaronder gezinsleden en directe sociale contacten, worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- volledige personalia (naam, geboortedatum, geboorteplaats);
- adresgegevens (straat, huisnummer, postcode, woonplaats);
- contactgegevens (telefoonnummer, e-mailadres;
- toezicht- en handhavingsgegevens of omtrent bestuurlijke maatregelen of voornemens daartoe voor zo ver in directe relatie met Betrokkene van Categorie 1;
- gegevens omtrent inzage verzoeken, verzoeken om rectificatie, verzet en klachten.

Strafrechtelijke Persoonsgegeven, te weten:

- Politiegegevens (artikel 8 en 13 Politiegegevens);
- Strafvorderlijke gegevens;

Bijzondere Persoonsgegevens en gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals bedoeld in artikel 9 en 10 AVG, te weten:

- […]
- […]

Toelichting:

Voor de Verwerking van Bijzondere Persoonsgegevens kent de AVG in beginsel een verwerkingsverbod. De verwerking van deze gegevens is niet toegestaan, behoudens voor zover het verwerkingsverbod is opgeheven in artikel 9 en 10 AVG, alsook artikel 23 t/m 33 Uitvoeringswet AVG Voor een toelichting raadpleeg ook de MvT bij de UAVG p. 33 t/m 38 en de Handleiding AVG van het Ministerie van Justitie en Veiligheid.

Categorie 3:

Categorie Betrokkenen:

Van medewerkers van instanties of instellingen die betrokken zijn bij de begeleiding, zorg- en hulpverlening van betrokkene (ook interventies voorafgaande aan de Aanmelding), worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- Naam;
- Naam organisatie organisatieaanduiding (typering bijv. instelling voor GGZ);
- Contactgegevens (zakelijk telefoonnummer, e-mailadres);
- Datum start betrokkenheid en einde betrokkenheid

Categorie 4:

Categorie Betrokkenen:

Van Medewerkers van derden die betrokken zijn bij de uitvoering van interventies (ook interventies voorafgaande aan de Aanmelding), worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- naam;
- naam organisatie organisatieaanduiding (typering bijv. instelling voor GGZ);
- functie binnen het zorg- en veiligheidshuis;
- contactgegevens (zakelijk telefoonnummer, e-mailadres);

Toelichting:

Bovenstaande categorieën zijn voor de gemeenten en zorg en welzijnspartijen niet uitputtend en dienen door Partijen nader te worden ingevuld in overleg met de Privacyfunctionarissen privacyadviseurs van de gemeenten en zorginstellingen.

Bijlage 5:

Contactgegeven betrokken organisaties bij dit handvat

AEDES vereniging van woningcorporaties
Contactpersoon: Hanneke Nagtzaam
T 0882333700
E h.nagtzaam@aedes.nl

DJI
Contactpersoon: Marielle Mahieu
T 0880725000
E secretariaatDB&B@dji.minjus.nl / m.mahieu@dji.minjus.nl

GGZ Nederland
T 0334608900
E zorgenrecht@ggznederland.nl

Jeugdzorg Nederland
T 0302983400
E info@jeugdzorgnederland.nl

Landelijke Vereniging Managers Veiligheidshuizen (LVMV)
Contactpersoon: Marieke van Puijenbroek
Zorg- en Veiligheidshuis Brabant Noordoost
T 073-6153020
E veiligheidshuis@s-hertogenbosch.nl

Landelijke Vereniging Managers Veiligheidshuizen (LVMV)
Contactpersoon: Carmen Polman
Veiligheidshuis Rijk van Nijmegen
T 024 - 329 92 70
E c.polman@nijmegen.nl

Ministerie van Justitie en Veiligheid
Contactpersoon: Rob Teijl
T 0652 872 577
E r.teijl@minvenj.nl

Nationale Politie
Contactpersoon: Peter Daamen
T 0650290616
E peter.daamen@politie.nl

OM

Contactpersoon: Saskia Laaper

T 088 6998775

E secretariaatpag@om.nl

Raad voor de Kinderbescherming

Contactpersoon: Ingeborg Galema

T 030-088 82580

E i.galama@rvdk.minvenj.nl

Reclassering Nederland / 3RO

Contactpersoon: Gerja Bethlehem

T 0888041000

E g.bethlehem@reclassering.nl

Slachtofferhulp Nederland

Contactpersoon: Andrea Galama

T 0630291349

E a.galama@slachtofferhulp.nl

Stichting Halt

Contactpersoon: Karin Witteman

T 088-1153500

E privacy@halt.nl

VNG

Contactpersoon: Hans Versteeg

T 0610062594

E hans.versteeg@vng.nl