

Privacy Impact Assessment
In verband met gegevensverwerking
bij de uitvoering van de Jeugdwet door gemeenten

Opdrachtgevers: Directie Justitieel Jeugdbeleid, Ministerie van V&J en Ministerie van VWS
Uitgevoerd door: PrivacyCare
Versie: 0.7 26 oktober 2014

Inhoudsopgave

1. Werkwijze PIA en uitgangspunten	1
1.1 Achtergrond	1
1.2 Werkwijze PIA	1
1.3 Leeswijzer.....	2
1.4 Verantwoording	2
2. Toetsingskader	3
2.1 Inleiding	3
2.2 Wet en regelgeving.....	3
2.3 Uitgangspunten Wbp en de bijzondere wetten	4
3. Belangrijke uitgangspunten voor de privacycompliance bij gemeenten	11
3.1 Inleiding	11
3.2 Gestructureerde aanpak privacy.....	11
3.3 Onderscheiden van gegevensverwerkingen	12
3.4 Verantwoordelijkheid gegevensverwerking.....	12
3.5 Alleen noodzakelijke gegevens	14
3.6 Werkprocessen.....	14
3.7 Bevoegdheid en kwaliteit	14
3.8 Medische gegevens en strafrechtelijke gegevens.....	15
3.9 Waarborgen voor gegevensbeveiliging en ICT.....	16
3.10 Borging van de samenwerking.....	17
3.11 Dienstverlening van gekwalificeerde ICT-leveranciers.....	18
3.12 Rechten van burgers.....	18
4. Privacy impact op de uitvoering van de Jeugdwet en de keuzes door gemeenten	20
4.1 Informatiebehoefte	20
4.2 Taken Jeugdwet	20
4.3 Preventie.....	21
4.3.1 Gegevensverwerking preventie	21
4.3.1.1 Gemeentelijke keuzes	21
4.3.2 Gegevensverwerking vroegsignalering	21
4.4 De toegangstaak van gemeente.....	23
4.4.1. Gemeentelijke keuzes	23
4.5 Toegang via de huisarts, specialist en jeugdarts.....	24
4.5.1 Gemeentelijke keuzes.....	25
4.6 Jeugdhulpplicht en feitelijke jeugdhulpverlening	25
4.6.1. Gemeentelijke keuzes	26
4.7 Meldingen aan Raad voor de Kinderbescherming	27
4.7.1 Structureren van de gegevensverwerking	29
4.7.2 Meldingen aan het AMHK	29
4.8 Kinderbeschermingsmaatregelen en jeugdreclassering.....	30
4.9 Dossierverplichting; persoonlijk dossier.....	31
4.9.1 Een gezin, één plan	31
4.10 Financiering, persoonsgebonden budget en ouderbijdrage.....	32
4.11 Pleegzorg.....	33
4.12 Onder toezicht stelling (ots) en gesloten jeugdhulp	33

4.13	Verwijsindex risico jongeren	34
5.	Verwerken van het bsn	36
5.1	Uitgangspunt.....	36
5.2	Huidige situatie	36
5.3	Jeugdwet.....	36
5.4	Verwerken bsn op grond van Wmo	37
5.5	Controle van het nummer	37
5.6	Bsn in het wijkteam.....	37
6.	Aanvullende aanbevelingen bij waargenomen risico's	38
6.1	Integrale aanpak en intercollegiale toetsing	38
6.1.1	Casusoverleg	39
6.2	Regie van de cliënt	40
6.3	Verder verwerken van gegevens voor monitoring en beleid	40
6.4	Gebruik van meetinstrumenten (ZRM)	41
6.5	Inrichten van wijkteams	42
6.6	Regels in het wijkteam	42
7.	Stappenoverzicht voor gemeenten	44

1. Werkwijze PIA en uitgangspunten

1.1 Achtergrond

De gemeenten zijn per 1 januari aanstaande bestuurlijk en financieel verantwoordelijk voor uitvoering van de Jeugdwet. Dat betekent dat de gemeente er een flink aantal taken bij krijgt. De Eerste en Tweede Kamer hebben uitdrukkelijk aandacht gevraagd voor de privacyaspecten bij de inrichting van de nieuwe taken door gemeenten.

De verantwoordelijkheid voor de inrichting van de nieuwe taken ligt bij het college van B&W. Het college van B&W legt hier verantwoording over af aan de gemeenteraad.

Op verzoek van de Kamer worden gemeenten hierbij ondersteund met een Privacy Impact Assessment (PIA) uitgevoerd op de inrichtingsaspecten en voorgenomen gegevensverwerkingen die bij uitvoering van de Jeugdwet een rol gaan spelen bij de gemeenten.

Deze PIA wordt conform de motie Bergkamp, (TK 31 839, nr. 398) voorgelegd aan het CBP voor advies.

In deze rapportage wordt het kader voor de gegevensverwerking en de privacy impact daarop verwoord. De kennis voor de PIA is onder andere vergaard in gesprekken met diverse gemeenten en de PIA is mede gebaseerd op de referentiemodellen zoals deze door VNG zijn opgesteld.¹ De keuzes die gemeenten kunnen maken ter uitvoering van de Jeugdwet en de betekenis voor de verwerking van persoonsgegevens worden in deze PIA besproken.

1.2 Werkwijze PIA

In de PIA worden de taken uit de Jeugdwet, de keuzes die door gemeenten kunnen worden gemaakt bij uitvoering van de Jeugdwet en de consequenties voor de gegevensverwerking daarbij toegelicht.

De oorspronkelijke opzet was dat de PIA de gegevensmodellen van de VNG toetst. Omdat de modellen nog niet af zijn, is er door de opdrachtgever voor gekozen om naast elementen uit de modellen, de gemeentelijke taken zoals verwoord in de Jeugdwet mee te nemen in de PIA. Daarbij is uitgegaan van de keuzemogelijkheden die gemeenten hebben bij de inrichting van die taken en de privacyaspecten die daarbij een rol spelen. Daarnaast worden de aandachtspunten bij een aantal specifieke uitvoeringsrisico's besproken. Andere 3-D wetgeving wordt in de PIA betrokken waar dit nodig is in relatie tot de de uitvoering van de Jeugdwet, ter ondersteuning van de PIA.

In de PIA wordt een beschrijving gegeven van:

- het toetsingskader;
- de wettelijk taken en verantwoordelijkheden uit de Jeugdwet;
- aspecten van organisatie inrichting en aandachtspunten daarbij;

¹ Zie Referentie Modellen Gegevensuitwisseling Jeugd domein, concept VNG. Op dit moment is alleen een concept beschikbaar.

- relevante situaties en elementen van de werkwijze van gemeenten;
- privacyrisico's die daarin worden waargenomen;
- aanbevelingen voor maatregelen die gesignaleerde risico's kunnen beperken of ondervangen;
- de stappen die aandacht behoeven van gemeenten.

De belanghebbenden en deskundigen die hebben meegewerkt aan de kennismakingen met gemeenten zijn direct betrokken bij de inrichting en ontwikkeling van de werkwijze van gemeenten. Daaronder ook ICT afdelingen en beheerders van gemeenten en betrokken juristen.

1.3 Leeswijzer

Hoofdstuk 2 geeft het toetsingskader voor de PIA.

Hoofdstuk 3 beschrijft een aantal belangrijke uitgangspunten voor de privacycompliance.

Hoofdstuk 4 beschrijft de gegevensverwerkingen onder de Jeugdwet en de privacy impact op de keuzes die gemeenten kunnen maken bij de uitvoering van de Jeugdwet.

Hoofdstuk 5 gaat in op de verwerking van het bsn.

Hoofdstuk 6 gaat in op aanvullende aanbevelingen voor de praktijk in verband met gesignaleerde risico's.

Hoofdstuk 7 schetst tot slot een kort stappenplan voor gemeenten.

1.4 Verantwoording

De PIA is uitgevoerd door PrivacyCare in opdracht van het ministerie van VenJ en het ministerie van VWS gezamenlijk. De rapportage is opgesteld in afstemming met de projectleider Privacy jeugdtransitie rijksoverheid. Een review is uitgevoerd door medewerkers van de ministeries van VenJ en VWS.

2. Toetsingskader

2.1 Inleiding

Per 2015 worden de Jeugdwet, de nieuwe Wet maatschappelijk ondersteuning (Wmo) en de Participatiewet van toepassing. De gemeente krijgt de zorg voor Jeugdhulp, maatschappelijke ondersteuning, preventie en participatie. Niet alles daaraan is nieuw. De gemeente zal bij de uitvoering van de wetten met de hulp- en zorgaanbieders en andere wettelijke actoren zoals de Raad voor de kindbescherming en het AMHK samenwerken.

De invoering van de Jeugdwet (waarop deze PIA betrekking heeft) en de daarmee gepaard gaande decentralisatie leidt tot een veranderende informatievoorziening rondom het verlenen van jeugdhulp en verwante preventie, zorgverlening of ondersteuning. De gemeenten worden bestuurlijk en financieel verantwoordelijk voor de jeugdhulp: hulp en ondersteuning aan jeugdigen en ouders, alsmede de preventieve taken. Daarnaast worden de gemeenten verantwoordelijke voor de uitvoering van de jeugdbescherming en jeugdreclassering door gecertificeerde instellingen. Daarbij zal de gemeente met diverse soorten zorgaanbieders, jeugdhulpaanbieders, de gecertificeerde instellingen en andere betrokken partijen samenwerken. Het verwerken van persoonsgegevens van cliënten blijft voor jeugdhulpaanbieders grotendeels vergelijkbaar met de huidige gegevensverwerking. Maar in de samenwerking ter uitvoering van de nieuwe taken zullen bepaalde gegevens met de gemeente en andere actoren in de nieuwe wetgeving moeten worden gedeeld en veel andere gegevens (uit de hulpverleningsrelatie, medische gegevens uit het dossier) in beginsel niet mogen worden gedeeld. Het is van groot belang om dit goed vorm te geven, want hier schuilt een groot privacyrisico als bovenmatig wordt uitgewisseld of te ruime toegang wordt gegeven. De grote verandering zit in de nieuwe rol en verantwoordelijkheid van de gemeente en de informatiebehoefte die dat met zich mee brengt. Met de verantwoordelijkheid voor de Jeugdwet zullen gemeenten nieuwe of andere persoonsgegevens gaan verwerken.

Gemeenten, jeugdhulpaanbieders en gecertificeerde instellingen zullen in het kader van de hulpverlening dagelijks diverse gegevens van jeugdigen en ouders vastleggen. Die gegevens zijn afkomstig van de jeugdige en ouders zelf, maar ook van anderen, zoals bijvoorbeeld de Raad voor de Kinderbescherming, jeugdhulpverleners of andere professionals die bij de jeugdige betrokken zijn. Het vastleggen van bepaalde gegevens is voor de gemeente noodzakelijk om de wettelijk opgedragen taken te kunnen uitvoeren. Voor de jeugdhulpverlener zijn bepaalde gegevens noodzakelijk om verantwoorde en kwalitatieve jeugdhulp te kunnen leveren. Ook de gecertificeerde instelling heeft gegevens nodig om haar taken te kunnen uitvoeren.

2.2 Wet en regelgeving

Het verwerken van gegevens van de inwoners van een gemeente in verband met de jeugdhulp valt onder de werking van de Wet bescherming persoonsgegevens (Wbp). Deze wetgeving vormt de basis voor inrichting van de gegevensverwerking. De bijzondere wetten geven daaraan een specifieke invulling. De Jeugdwet bevat op een aantal punten een aanvulling en concretisering van de algemene normen van de Wbp.

Naast de Wbp en de Jeugdwet wordt het kader gevormd door de Wet op de geneeskundige behandelingsovereenkomst (WGBO) en de Wet BIG, waarin o.a. de dossierplicht en het beroepsgeheim voor zorgprofessionals geregeld is. Deze bepalingen gelden voor zorgverleners in het kader van behandeling, respectievelijk BIG geregistreerde hulpverleners. Daarbij kan gedacht worden aan de arts, de verpleegkundige, de psychiater, de psycholoog of psychotherapeut, de huisarts, en de ggd-arts. Deze wetten blijven van toepassing. In de Jeugdwet zijn vergelijkbare bepalingen opgenomen waarmee de dossierplicht en de geheimhouding voor jeugdhulpverleners en gecertificeerde instellingen geregeld wordt. De Wet publieke gezondheid (Wpg) bepaalt in aanvulling op de dossierplicht dat in de jeugdgezondheidszorg er sprake moet zijn van digitale dossiervorming. Ook in de Wmo 2015 wordt de geheimhoudingsplicht en de verplichting tot het vastleggen van gegevens bij de uitvoering van de Wmo in algemene zin wordt geregeld. Dit is aanpalend van belang.

De nieuwe wetgeving biedt ook een basis voor het lokaal beheren van de Verwijsindex Risicjongeren (VIR) door de gemeente (regievoerder VIR) en het gebruik ervan door professionals, alsmede een meldrecht in het kader van het AMHK. Via de Wbp zijn de geheimhoudingsverplichtingen uit andere bijzondere wetten gekoppeld aan het Wbp regime. De geheimhoudingsverplichtingen spelen in het jeugddomein een belangrijke rol. De verplichting is niet absoluut, maar kent een aantal uitzonderingsgronden die in 2.3 worden besproken.

Naast wet en regelgeving speelt natuurlijk ook gemeentelijke regelgeving een rol via de verordeningen per rechtsgebied. De verordeningen geven nadere invulling aan de 3-D wetgeving door middel van onder andere inrichtingskeuzes.

Daarnaast kunnen ook beroepscode nog een rol spelen bij bepaald handelen. Bijvoorbeeld als de ondersteuning door een maatschappelijk werkers wordt verleend en er geen sprake is van jeugdhulp. Daarvoor geldt de beroepscode van maatschappelijk werkers. Uit die code volgt dat een cliëntdossier wordt bijgehouden en dat de maatschappelijk werker geheimhouding over de gegevens verplicht is.

Voor psychologen is er de NIP gedragscode. Dit is relevant in gevallen dat de psycholoog geen BIGger is en niet als jeugdhulpaanbieder kwalificeert, maar toch betrokken is bij de jeugdhulp. De geheimhouding en de dossierplicht uit de codes werken in de praktijk op dezelfde manier als de wettelijke verplichtingen die hierboven beschreven zijn. Beroepscode spelen aanvullend een rol. De code moet altijd in overeenstemming met de wet worden uitgelegd.

2.3 Uitgangspunten Wbp en de bijzondere wetten

De Wbp is van toepassing voor zover het gaat om het verwerken van persoonsgegevens. Een persoonsgegeven is 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Daarbij gaat het ook om gegevens die in hun onderlinge samenhang of op zichzelf, indirect tot een persoon te herleiden zijn. Voor beleid of beheer kan met geaggregeerde data gewerkt worden, of zo nodig met pseudoniem. In het laatste geval kan niet herleidbaar 'gevolgd' worden.

Het 'verwerken' omvat elke handeling met betrekking tot de persoonsgegevens, zoals het inzien, opslaan en delen van de gegevens. Degene wiens persoonsgegevens worden verwerkt is de 'betrokkene' in de zin van de Wbp. Ook de Jeugdwet hanteert het begrip betrokkene op deze manier.

Verantwoordelijke en bewerker

De normen van de Wbp richten zich grotendeels tot de 'verantwoordelijke' voor de gegevensverwerking. Dit is volgens de Wbp 'degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt'. Niet alleen is de verantwoordelijke degene die de verplichtingen uit de Wbp moet opvolgen, ook is hij het aanspreekpunt voor betrokkenen met betrekking tot de gegevensverwerking en het uitoefenen van de rechten van de betrokkene. Het moet worden vastgelegd welke partij verantwoordelijke is voor de (onderdelen van de) gegevensverwerking. Het niet goed regelen van verantwoordelijkheid is een groot compliance risico.

Wanneer een partij de gegevens vastlegt in opdracht en voor doelstellingen van de verantwoordelijke treedt zij op als 'bewerker' van de gegevens in de zin van de Wbp. Dit is bijvoorbeeld aan de orde bij hosting van een database of informatiesysteem door een derde dienstverlener, die niet zelf medeverantwoordelijke is.

Onder de Wmo 2015 zal voor onderdelen van de gegevensverwerking de gemeente verantwoordelijk zijn en voor andere delen de betrokken uitvoerders van de Wmo zoals de aanbieders van voorzieningen. Dit bepaalt de wet. Betreffende de uitvoering van de Jeugdwet, moet afhankelijk van de inrichting, de verantwoordelijkheid belegd worden bij gemeente of ketenpartners. Gebeurt gegevensverwerking voor de gemeentelijke taken, dan is het logisch dat de gemeente daarvoor de verantwoordelijke is. Gebeurt gegevenverwerking door de jeugdhulpaanbieder in het dossier van de cliënt ten behoeve van de zorg? Dan is het logisch dat de aanbieder verantwoordelijkheid draagt. Hij moet immers de geheimhoudingsplicht ook kunnen borgen. Is de jeugdhulpverlener in dienst van de gemeente dan is de gemeente voor dat stuk zelf jeugdhulpaanbieder.

Grondslag

De Wbp vereist een grondslag voor elke persoonsgegevensverwerking op grond van artikel 8 Wbp. Daarin wordt aangegeven voor welke doeleinden persoonsgegevens verwerkt mogen worden.

Als daarbij ook 'bijzondere' gegevens worden verwerkt zoals bedoeld in artikel 16 Wbp, dan is een grondslag uit artikel 8 Wbp alleen niet voldoende. Dan is daarnaast een ontheffing nodig zoals opgenomen in de artikelen 17 t/m 23 Wbp. Het gaat dan bijvoorbeeld om strafrechtelijke gegevens, gezondheidsgegevens of gegevens over godsdienst. In de uitvoering van de Jeugdwet (en andere 3-D wetgeving) zal het verwerken van bijzondere gegevens vaak aan de orde zijn.

In de eerste plaats zal artikel 8 e Wbp, noodzakelijk verwerken voor de bestuursrechtelijke taak, van belang zijn. Veel van de noodzakelijke gegevensverwerking zal onder deze grondslag plaatsvinden omdat de taak en de verantwoordelijkheden van het bestuursorgaan gemeente in de Jeugdwet zijn vastgelegd. Hierbij kan ook gedacht worden aan de preventietaken die uit de Jeugdwet, maar ook uit de bestaande Wpg volgen, voorzover deze door de gemeente worden uitgevoerd. In veel gemeenten zal de uitvoering van de Jeugdwet (deels) naast de uitvoering van de Wpg gebeuren op één plek.

Sommige gegevensverwerking zal ook nodig zijn vanwege een wettelijke verplichting tot het verwerken van gegevens. Dan is artikel 8 c Wbp aan de orde. Deze verplichtingen worden afgeleid uit de bijzondere wetgeving. Deze grondslag is alleen aan de orde als de gegevensverwerking als verplichting geformuleerd is.

Toestemming is een grondslag die in het kader van gegevensverwerking door de overheid met terughoudendheid moet worden bekeken. De afhankelijk die een burger heeft ten opzichte van de overheid in het algemeen speelt daarbij een rol. Bij structurele gegevensverwerking, die onafhankelijk van toestemming nodig is speelt deze grondslag geen rol. Toestemming is alleen een geldige grondslag als aan de beginselen van vrije en specifieke toestemming is voldaan.

Natuurlijk is het in het kader van de bedoelde gegevensverwerking ook van belang te kijken naar de grondslagen voor gegevensverwerking door jeugdhulpverleners die niet door de gemeente plaatsvindt, zoals door de jeugdhulpaanbieders en gecertificeerde instellingen. Met name de wettelijke verplichting (dossierplicht) en soms de toestemming (behandelovereenkomst, geen gedwongen kader) spelen een rol.

Bijzondere gegevens

Artikel 16 Wbp gaat uit van een algemeen verbod op het verwerken van bijzondere gegevens, behoudens uitzonderingen. Het gaat om persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Daarnaast gaat het om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Gezondheidsgegevens

Bij het uitvoeren van de gemeentelijke taken onder de Jeugdwet zal het regelmatig om gegevens betreffende de gezondheid (zoals medische gegevens) van betrokkenen kunnen gaan. Voor de beoordeling van een hulpvraag zijn deze gegevens (zo beperkt mogelijk) nodig. Ook bij de hulpverlening worden deze gegevens verzameld zover noodzakelijk voor de goede hulp aan betrokkene.

De Wbp geeft een ontheffing voor het verwerken van 'gegevens betreffende de gezondheid' aan hulpverleners en instellingen wanneer dat noodzakelijk is voor de goede zorgverlening aan de betrokkene (artikel 21 lid 1 onder a Wbp).

Artikel 21 lid 1 sub f Wbp biedt daarnaast een ontheffing aan gemeenten voor het verwerken van gezondheidsgegevens voor bepaalde specifieke doeleinden. De wet stelt in verkorte bewoording dat een ontheffing geldt voor:

- Bestuursorganen of instellingen die ten behoeve daarvan werkzaam zijn voor zover dat noodzakelijk is voor een goede uitvoering van wettelijke voorschriften die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene.

Daarnaast kan de ontheffing soms voortvloeien uit de uitdrukkelijke toestemming van de betrokkene of enkele uitzonderlijke omstandigheden (vitaal belang van betrokkene), zoals geregeld in artikel 23 Wbp (restbepaling). Ook kan een ontheffing zijn gecreëerd in formele wetgeving, zoals de Jeugdwet (artikel 7.4.4 lid 2 jo. 7.4.1 lid 2 Jeugdwet).

Gegevens betreffende de gezondheid mogen uitsluitend worden verwerkt door personen op wie een geheimhoudingsplicht rust, dan wel aan wie deze contractueel is opgelegd. Dit is een belangrijk punt van aandacht.

Ook andere bijzondere gegevens kunnen worden verwerkt door hulpverleners en instellingen voor maatschappelijke dienstverlening als dat in aanvulling op de gezondheidsgegevens noodzakelijk is voor de goede behandeling of verzorging van betrokkenen. (artikel 21 lid 3 Wbp)

Strafrechtelijke gegevens

Het verbod om strafrechtelijke persoonsgegevens te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, alsmede door verantwoordelijken die deze hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens (artikel 22 Wbp).

Ook is het verbod niet van toepassing op de verantwoordelijke die deze gegevens voor zichzelf verwerkt ter:

- beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren of
- bescherming van zijn belangen voor zover het gaat om strafbare feiten die zijn gepleegd, of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd, jegens hem of jegens personen die in zijn dienst zijn.

In de artikelen 17 t/m 20 worden daarnaast specifieke ontheffingen gegeven voor het verwerken van andere bijzondere gegevens.

Artikel 7.4.1, tweede lid, jo artikel 7.4.4 van de Jeugdwet bieden daarnaast een specifieke wettelijke basis voor de gemeente om (bijzondere) persoonsgegevens te verwerken die zij nodig heeft voor de toegang tot jeugdhulp.

Verder verwerken van gegevens

Artikel 9 lid 4 Wbp regelt dat een verdere verwerking achterwege moet blijven wanneer een geheimhoudingsplicht aan het (verder) verwerken in de weg staat. De geheimhoudingsplicht

volgt (zoals onder 2.2 uitgebreider besproken) in het kader van jeugdhulp uit de Jeugdwet (artikel 7.3.11), de WGBO (7:457 BW) en de Wet BIG (artikel 88). De geheimhoudingsplicht is niet absoluut. Uitzonderingen worden gevormd door de vrije en specifieke toestemming van de cliënt of een wettelijke verplichting om gegevens te verstrekken over de cliënt of uit het dossier. Daarnaast mag de toestemming van de cliënt worden aangenomen als het gaat om het delen van uitsluitend noodzakelijke gegevens met diegene die beroepsmatig rechtstreeks bij de behandelingsovereenkomst, dan wel de jeugdhulpverlening, betrokken is. Dit laatste is behoudens bezwaar daartegen van de cliënt en voorzover nodig voor de taak van de betrokken persoon. Om eventueel bezwaar te kunnen maken dient de cliënt op de hoogte te worden gebracht van voorgenomen gegevensverwerking.

Het beroepsgeheim kan in bijzondere gevallen ook doorbroken worden als sprake is van een 'conflict van plichten', een noodsituatie die in het belang van de directe veiligheid van de cliënt of een ander dan de cliënt rechtvaardigd dat bepaalde, voor het afwenden van het gevaar noodzakelijke gegevens worden gedeeld met een ander. Voor dit soort situaties is in specifieke gevallen ook een meldrecht voor professionals verankerd in de wetgeving in het kader van de Verwijsindex Risicjongeren (VIR) en in het kader van het AMHK.

Als de geheimhoudingsplicht niet aan een verdere verwerking in de weg staat, is het overige van artikel 9 Wbp nog van belang. Daarin wordt geregeld dat verzamelde gegevens niet verder mogen worden verwerkt voor andere doeleinden die niet verenigbaar zijn met het doeleinde van verkrijging.

Persoonsnummers

Artikel 24 Wbp beperkt het gebruik van wettelijke persoonsnummers.

Dit is onder andere van toepassing op het verwerken van het burgerservicenummer (bsn). Wet algemene bepalingen bsn (Wabb) regelt het gebruik van het bsn. Aanvullende sectorale bepalingen volgen voor de 3-D inrichting uit de bijzondere wetgeving Jeugdwet, Wmo, Participatiewet en de Wet gebruik bsn in de zorg.

Bewaren van gegevens

Persoonsgegevens mogen slechts worden verwerkt als zij voor het specifieke doeleinde van verwerken noodzakelijk zijn en niet langer worden bewaard dan noodzakelijk. (artikel 10 en 11 Wbp).

Deze algemene norm is voor de jeugdhulpverlener en de gecertificeerde instelling ingevuld. Artikel 7.3.8, derde lid Jeugdwet, bepaalt dat het dossier gedurende vijftien jaar moet worden bewaard, of zoveel langer als uit de zorg van een goed hulverlener voortvloeit.

Artikel 7:454 BW (WGBO) regelt hetzelfde voor het dossier van de zorgaanbieder die onder de WGBO valt. De bewaartermijnen laten onverlet het recht van betrokkene om te verzoeken gegevens te corrigeren of te vernietigen.

Beveiligingseisen

Op grond van artikel 13 Wbp dient de verantwoordelijke passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. 'Passend' betekent in dit verband dat de beveiliging in overeenstemming is met het risico van de gegevensverwerking (in verband met onder andere de aard van de gegevens en het gebruik) en de stand van de techniek. Het College bescherming persoonsgegevens (CBP), toezichthouder op de Wbp, heeft in richtsnoeren de eisen omtrent beveiliging nader uitgewerkt.²

De open norm van artikel 13 Wbp kan op passende wijze worden ingevuld, door te voldoen aan de bestaande (Nederlandse en internationale) normen voor informatiebeveiliging. Er zal moeten worden afgewogen welke (aanvullende) maatregelen nodig zijn in verband met de bijzonderheden en risico's van de verwerking.

Onderdeel van beveiliging is het regelen van de toegang tot gegevens (autorisaties) voor gerechtvaardigde gebruikers. Er dient door de verantwoordelijke(n) een autorisatierichtlijn te worden vastgesteld en onderhouden en een daarop gebaseerd autorisatieprofiel, waarmee inzichtelijk is wie welke autorisatie heeft om persoonsgegevens die onder zijn verantwoordelijkheid worden verwerkt in te zien, daarbij rekening houdend met de specifieke taak, rol en verantwoordelijkheid van de gebruiker of professional (zoals omschreven in de werkprocessen).³

Daarnaast is ook de methode of het middel van toegang waarmee de gebruiker toegang krijgt van belang voor de beveiliging, in verband met de zorgvuldige identificatie en authenticatie van gebruikers.

In verband met de uitvoering van de Jeugdwet is het beveiligen en afschermen van geheimhoudingsplichtige gegevens uit de zorg- en hulpverleningsrelatie door middel van de juiste autorisaties een belangrijke voorwaarde voor rechtmatigheid. Hetzelfde geldt ook voor strafrechtelijke gegevens die alleen aan specifieke personen mogen worden verstrekt. (denk bijvoorbeeld aan het Besluit justitiële en strafvorderlijke gegevens)

Informatieplicht

Overeenkomstig artikel 33 en 34 van de Wbp bestaat een informatieplicht tegenover de betrokkene. Betrokkenen moeten worden geïnformeerd over het doel van de verwerking, de verantwoordelijke en het specifieke gebruik van de gegevens in de teams. Dit zorgt voor de nodige transparantie en is daarmee een voorwaarde voor het kunnen uitoefenen van rechten door de betrokkene.

² CBP Richtsnoeren, Beveiliging van persoonsgegevens, College Bescherming Persoonsgegevens, februari 2013.

³ Het is belangrijk om ook in kaart te brengen hoe dit binnen de totale gegevensverwerking in het jeugdstelsel past, door het uitwerken van een gegevensverwerkingsmodel, waarin (wettelijk toegelaten en noodzakelijke) gegevensstromen in beeld worden gebracht. (zie ook 3.1.en 3.3)

Rechten van betrokkenen

Een betrokkene heeft behoudens wettelijk geregelde uitzonderingssituaties het recht inzage en een overzicht te verkrijgen van de verwerking van zijn persoonsgegevens. Ook heeft hij het recht op correctie of verwijdering van gegevens. Dit wordt in de Wbp geregeld, maar ook in de bijzondere wetgeving. De Jeugdwet geeft aanvullende rechten aan betrokkenen en cliënten. Zo heeft de betrokkene in beginsel recht op vernietiging van het dossier dat op grond van de Jeugdwet of de WGBO door een zorg- of hulpverlener is vastgelegd.

3. Belangrijke uitgangspunten voor de privacycompliance bij gemeenten

3.1 Inleiding

Het voornaamste doel van de Jeugdwet is dat alle kinderen gezond en veilig opgroeien, hun talenten ontwikkelen en meedoen in de samenleving naar vermogen. Belangrijke uitgangspunten van het nieuwe stelsel zijn dat:

- ingezet wordt op meer preventie en betere ondersteuning;
- uitgegaan wordt van de eigen kracht van jeugdigen en hun ouders;
- beter samengewerkt wordt rond gezinnen;
- problemen minder gemedicaliseerd worden;
- zorg op maat verleend wordt;
- aansluiting van het gedwongen kader op de gemeentelijke jeugdhulp wordt gerealiseerd.

Voor de jeugdhulp worden veel gevoelige gegevens verwerkt. Niet alleen over de jeugdige zelf, maar zo nodig ook over familie en omgeving. De gegevens zullen in verschillende systemen worden verwerkt door verschillende actoren en tussen verschillende actoren. Een groot deel van die gegevens vallen onder de geheimhoudingsplicht van de behandelaar (zoals jeugdarts of psycholoog) of jeugdhulpverlener, zodat strenge voorwaarden gelden voor het delen van bepaalde gegevens, als dat voor de hulp noodzakelijk is. Het is aan gemeenten om (samen met deze partijen) ervoor zorg te dragen dat dit op een zorgvuldige en rechtmatige wijze zal plaatsvinden in het nieuw in te richten stelsel.

Informatieverwerking is essentieel voor de goede uitvoering van de Jeugdwet. Het gaat dan om onder meer preventie, toeleiding en uitvoering van jeugdhulp, noodzakelijke communicatie tussen ketenpartners, gegevensverwerking ten behoeve van de gesloten jeugdhulp en controle, gegevensverwerking voor beleidsdoeleinden en sturing, voor financiële afhandeling en toezicht.

Een kenmerkend element bij de nieuwe verdeling van taken en werkzaamheden is de nieuwe rol voor de gemeenten. Ruim 400 gemeenten moeten zorgvuldig en beheersbaar omgaan met voor hen nieuwe taken en een nieuwe infrastructuur voor de uitwisseling van gegevens. Omdat de werkzaamheden en taken nieuw zijn, kan niet worden teruggevallen op een bestaande structuur. Dit is een groot risico voor de privacy van betrokkenen. Gemeenten moeten dus op tijd zorgen voor een goed overzicht van de informatiebehoefte die zij hebben op grond van de inwerkingtreding van de Jeugdwet per 2015. Taken moeten zijn ingericht en zo nodig, op een zorgvuldige wijze bij anderen zijn belegd. Voor alle taken dient een gegevensverwerkingsmodel te worden gemaakt waarin de noodzakelijke en wettelijk toegelaten gegevensuitwisseling met de betrokken actoren in kaart is gebracht, de verantwoordelijkheid en de doeleinden voor de gegevensverwerkingen helder zijn verwoord en de grondslagen zijn vastgesteld. Voor elke gegevensstroom moeten de noodzakelijke gegevens worden vastgesteld.

3.2 Gestructureerde aanpak privacy

Elke organisatie die binnen het jeugdstelsel optreedt als verantwoordelijke in de zin van de Wbp voor persoonsgegevensverwerking heeft belang bij een gestructureerde aanpak van de

compliance. Alleen op die manier kan de verantwoordelijke daarin succesvol zijn en voorkomen dat de risico's van privacyschending, reputatieschade en handhaving bewaarheid worden. Het CBP vereist dit ook als voorwaarde om als verantwoordelijke 'accountable' te zijn voor een zorgvuldige gegevensverwerking en aantoonbaarheid daarvan te borgen. Dit geldt natuurlijk in de eerste plaats voor de gemeenten die voor een deel van de gegevensverwerking in het stelsel de verantwoordelijke in de zin van de Wbp zal zijn (zie ook 3.4 over verantwoordelijkheid). In de Richtsnoeren Beveiliging van persoonsgegevens gaat het CBP in op de stappen in het proces die noodzakelijk zijn. Het is van belang een privacybeleid te ontwikkelen en een 'keyholder' aan te wijzen die hiervoor in de organisatie verantwoordelijk is. Een privacy officer of een Chief Information Officer (CIO) kunnen deze rol bijvoorbeeld vervullen.

Gegevensverwerking dient vooraf te worden gegaan van een risico en/of impact analyse, op basis waarvan de juiste afspraken kunnen worden gemaakt over de toegestane en noodzakelijke gegevensverwerking en waarborgen kunnen worden getroffen voor adequate beveiliging. Om continuïteit in de privacy compliance te borgen is het noodzakelijk om een managementcyclus in te richten in de organisatie, een zogenaamde Plan-Do-Check-Act (PDCA) cyclus. Hierin wordt geborgd dat de privacy compliance een dynamisch en doorlopend proces is, waarin evaluatie en toetsing van de gegevensverwerking een periodieke plaats heeft en privacy maatregelen up to date blijven. Het (laten) uitvoeren van audits en controles is onderdeel van het noodzakelijk toezicht op de eigen compliance.

3.3 Onderscheiden van gegevensverwerkingen

Het is voor gemeenten en ketenpartners van groot belang de verschillende (voorgenomen) gegevensverwerkingen te onderscheiden en te kwalificeren. Daarmee wordt bedoeld dat het belangrijk is de gegevensverwerking (registraties en de uitwisseling (gegevensstromen)) in kaart te brengen in een gegevensverwerkingsmodel. In het model worden ook de informatiesystemen onderscheiden en de uitwisseling die tussen systemen plaatsvindt.

In het model worden de doeleinden van de verschillende gegevensverwerkingen vastgesteld en gekeken naar de betrokken actoren en de grondslag voor de verwerking van gegevens door en tussen hen. Daarbij is de vraag voor welke doeleinden (taken) gegevens worden verwerkt door wie? En van wie de gegevens worden verkregen of met wie ze moeten worden gedeeld? Zo worden de gegevensstromen inzichtelijk gemaakt en kunnen ze beoordeeld worden op hun rechtmatigheid. Aan de hand van de doeleinden en grondslagen moet worden bepaald welke gegevens noodzakelijk zijn voor realisatie van de doeleinden.

3.4 Verantwoordelijkheid gegevensverwerking

Bij elke persoonsgegevensverwerking is het allereerst van belang vast te stellen wie daarvoor wordt aangemerkt als de verantwoordelijke in de zin van de Wbp. De verantwoordelijke is namelijk degene die wordt aangesproken op naleving van de wet bij het verwerken van de gegevens. In de Jeugdwet zijn verschillende taken en verantwoordelijkheden beschreven en worden verschillende actoren daarbij betrokken. De gemeente is overkoepelend verantwoordelijk voor de uitvoering van de Jeugdwet in de gemeente. Verschillende taken zijn in de wet bij andere actoren belegd. Ook kan de gemeente een aantal taken door anderen laten uitvoeren. Verantwoordelijkheid voor de uitvoering betekent daarom niet per definitie

verantwoordelijk zijn voor alle gegevensverwerking die daarbij komt kijken. Wie verantwoordelijke is voor de gegevensverwerking is mede afhankelijk van de inrichting door gemeenten. Die inrichting bepaalt namelijk voor wie het nodig is om bepaalde persoonsgegevens te verwerken om de uit te voeren taken naar behoren te kunnen uitvoeren. Die inrichting bepaalt ook voor welk doeleinde gegevens op een bepaalde plek moeten worden verwerkt.

Anders dan bijvoorbeeld in de Wmo 2015 wordt in de Jeugdwet niet voorgeschreven wie voor een bepaalde gegevensverwerking de verantwoordelijke is. De Wbp is dus leidend om vast te stellen wie verantwoordelijke is voor de gegevensverwerking.

Het is belangrijk om bij de inrichting vooruit te blikken naar de verantwoordelijkheid die men creëert. Niet elke verantwoordelijke is namelijk op dezelfde manier bevoegd om bepaalde gegevens te verwerken, gelet op de grondslagen die de Wbp geeft. Het verwerken van bijzondere persoonsgegevens is gebonden aan een strenger regime. Het verwerken van gegevens over iemands gezondheid of strafrechtelijke gegevens is voorbehouden aan bepaalde verantwoordelijken voor bepaalde doeleinden. De inrichting dient daarop aan te sluiten. Bovendien mag de inrichting er niet toe leiden dan bepaalde persoonsgegevens onnodig op meerdere plekken worden verwerkt. Dat zou tot bovenmatige persoonsgegevensverwerking leiden.

Verantwoordelijke is degene onder wiens bevoegdheid de gegevensverwerking plaatsvindt. In beginsel zal de partij die voor eigen doeleinden de gegevens verwerkt de verantwoordelijke in de zin van de Wbp zijn. Zo zal de gemeente die voor zijn taken zelf persoonsgegevens verwerkt of doet verwerken daarvoor verantwoordelijke zijn. Terwijl bij uitbesteding van bepaalde taken, zoals het verlenen van jeugdhulp, aan derden *die dat uit eigen naam doen*, die derden de verantwoordelijke(n) zullen zijn voor de gegevens die voor dat doel door hen worden vastgelegd. Dit laatste sluit goed aan bij de verantwoordelijkheid die de derde (zorgverlener en jeugdhulpverlener) op grond van de WGBO of de Jeugdwet zal hebben om een dossier bij te houden van cliënten en geheimhouding van cliëntgegevens te borgen.

De verantwoordelijkheid zal uiteindelijk altijd getoetst moeten worden aan de werkelijkheid van de praktijk. Het is degene die doel en middelen, het hoe en wat van de gegevensverwerking vaststelt, die verantwoordelijke is. Het is de partij die werkelijk de zeggenschap heeft over de gegevensverwerking. Dat kunnen ook partijen gezamenlijk zijn. Dit kan bijvoorbeeld komen omdat een registratiesysteem wordt ingericht dat wordt gedeeld door verschillende partijen voor registratie. Een vooruitziende blik is hierbij van belang. Een slimme inrichting zorgt voor een simpele en overzichtelijke 'compliance'. Partijen op wie een geheimhoudingsplicht rust moeten zorg dragen dat de inrichting van de organisatie en de informatievoorziening zodanig is dat zij deze verplichting goed kunnen borgen. Een gedeeld informatiesysteem mag er niet toe leiden dat de verantwoordelijkheid niet goed kan worden nageleefd. Bij gezamenlijke verantwoordelijkheid dient zorgvuldig te worden beschreven wie waarvoor verantwoordelijk is. Naar de betrokkene toe dient helder te zijn wie als verantwoordelijke kan worden aangesproken.

3.5 Alleen noodzakelijke gegevens

Een zeer belangrijk element van regelgeving over het verwerken van persoonsgegevens is de zogenaamde noodzakelijkheids toets. Dit houdt in dat gegevens enkel verwerkt mogen worden voorzover dit noodzakelijk is voor een bepaald specifiek gerechtvaardigd doel. De te verwerken gegevens moeten ter zake dienend zijn en niet bovenmatig.

Gemeenten en ketenpartners moeten voor de gegevensverwerkingen waarvoor zij de verantwoordelijke zijn, vaststellen welke gegevens daarvoor echt noodzakelijk zijn. De noodzakelijkheidstoets wordt ingevuld door de vereisten van proportionaliteit en subsidiariteit. Proportionaliteit ziet daarbij op de verhouding tussen doel en middel: is de gegevensverwerking proportioneel om het doel te bereiken. Subsidiariteit ziet op de vraag of er voor de voorziene gegevensverwerking alternatieven zijn die minder inbreuk maken op de privacy van betrokkenen of die meer waarborgen bieden.

De gegevensset voor een voorgenomen gegevensverwerking moet worden vastgesteld op basis van de verwachte noodzaak van bepaalde gegevens. Doordat de ontwikkeling nog in gang is zal de beoordeling van de noodzaak om bepaalde gegevens te verwerken nog kunnen wijzigen. De gegevenssets dienen regulier geëvalueerd en onderhouden te worden door de verantwoordelijke, zodat bovenmatige gegevensverwerking steeds voorkomen wordt.

Het hier gestelde betekent niet dat alle gegevensverwerking altijd geheel gestandaardiseerd kan zijn. Het vaststellen van welke gegevens (aanvullend) noodzakelijk zijn voor opname in het dossier in de uitvoering van een behandeling of feitelijke jeugdhulp, kan pas door de betrokken hulpverlener worden vastgesteld.

3.6 Werkprocessen

Als de rechtmatigheid van gegevensverwerking is vastgesteld en de noodzakelijke gegevensverwerking in beeld is gebracht is het van groot belang de gegevensverwerking in duidelijke werkprocessen te verankeren. Op die manier kan op een zorgvuldige wijze uitvoering worden gegeven aan de taken en de gegevensverwerking die daarbij hoort. Naast werkprocessen kunnen gedragsregels of privacyprotocollen helpen om medewerkers de handvatten te bieden om op een voorziene en zorgvuldige wijze te handelen. Daarnaast is het van belang bepaalde afspraken contractueel te borgen zodat deze afdwingbaar zijn. Medewerkers die persoonsgegevens verwerken moeten een geheimhoudingsverklaring ondertekenen.

3.7 Bevoegdheid en kwaliteit

In de bijzondere wetgeving wordt ook de bevoegdheid en bekwaamheid die vereist is voor bepaald handelen geregeld. Dit is voor de inrichting een belangrijk aandachtspunt. Wanneer daarbij uit naam van de gemeente gehandeld wordt, is het mandaat van het bestuursorgaan gemeente daarvoor noodzakelijk. Dit wordt geregeld in een mandaatsbesluit. Als niet uit een overeenkomst een opdracht aan een hulpaanbieder of hulpaanbieders gezamenlijk tot het verrichten van bepaalde wettelijke taken waarvoor de gemeente de 'zorgplicht' heeft volgt, dan zal een machtiging door de gemeente nodig zijn om een duidelijke grondslag voor de uitvoering van deze taken door de gemachtigde te creëren. Dat is ook voor de transparantie naar de

burger van belang. Uitvoering door buurtteams kan ook in de verordening van de gemeente worden opgenomen. Daarnaast is het aspect kwaliteit, waaraan in de Jeugdwet en enkele andere zorgwetten eisen zijn gesteld een belangrijke voorwaarde bij de inrichting en vormgeving van de jeugdhulp bij gemeenten.

3.8 Medische gegevens en strafrechtelijke gegevens

Een bijzondere zorg voor de naleving van de privacywetgeving bij de uitvoering van de Jeugdwet en de verwante decentralisaties is het verwerken van bijzondere persoonsgegevens. Bij uitvoering van de Jeugdwet gaat het in de eerste plaats om gegevens over de gezondheid van betrokkenen en soms ook om zogenaamde strafrechtelijke gegevens. Gezondheidsgegevens omvatten medische gegevens die bijvoorbeeld door een psychiater worden vastgelegd voor de behandeling van een jeugdige. Maar bijvoorbeeld ook de minimale gegevens die afgeleid uit hulp of ondersteuning worden verwerkt op een factuur. Deze gegevens kennen een grote gevoeligheid. Omdat voor het verwerken van deze gegevens een streng regime geldt moet dit met extra waarborgen en zorg worden omkleed.

Nu bij de uitvoering van de Jeugdwet veel actoren betrokken zijn, waarbij het potentieel gaat om het verwerken van gegevens van vele burgers is het risico op (onbedoeld) onzorgvuldig handelen en een te ruime gegevensverwerking groot. Dit wordt verstrekt door de korte periode waarin de inrichting, het beleid en de processen moeten worden vorm gegeven. Maar ook door de nieuwe rol van de gemeente en de mogelijkheid voor gemeenten om de jeugdhulpverlening zelf uit te voeren (met inzet van professionals) en dus onder eigen verantwoordelijkheid hulpverleningsgegevens te gaan verwerken. Op de gegevens die in het kader van de hulpverlening ter kennis komen van de hulpverlener geldt altijd een beroepsgeheim voor de hulpverlener, welke materiewet ook van toepassing is. De verantwoordelijke - wanneer dat een ander is dan de hulpverlener, zoals de aanbieder of de gemeente- heeft daarnaast de zorgplicht om de geheimhoudingsplicht te waarborgen.

Voor gezondheidsgegevens geldt bovendien dat zij altijd moeten worden verwerkt door personen op wie een geheimhoudingsplicht rust. Deze gegevens mogen alleen verder worden verwerkt in een beperkt aantal gevallen zoals in het juridisch kader is toegelicht. De gegevens moeten bovendien met meer waarborgen worden bewaard en beveiligd. De toegang tot de gegevens dient beperkt te zijn tot de geheimhoudingsplichtige die de gegevens voor uitvoering van zijn taak nodig heeft en rechtmatig heeft verkregen. *Iedere gemeente zal hier veel aandacht aan moeten besteden.* Voor een goede uitvoering is het van belang dat gemeenten goed weten welke gegevens 'gegevens betreffende de gezondheid' zijn. Het gaat dan niet alleen om medische gegevens zelf maar ook om persoonsgegevens die in de context daarvan van een betrokkene worden verwerkt. Het gaat om alle gegeven die op zich of in hun onderlinge samenhang iets zeggen over de geestelijke of lichamelijke gezondheidstoestand van de betrokkene. Het feit dat iemand naar de psycholoog is geweest, is zo'n gegeven. Maar het feit dat iemand jeugdhulp ontvangt ook.

3.9 Waarborgen voor gegevensbeveiliging en ICT

Het College bescherming persoonsgegevens (CBP), toezichthouder op de Wbp, heeft in Richtsnoeren voor beveiliging van persoonsgegevens de eisen omtrent beveiliging nader uitgewerkt. Het CBP verlangt het uitvoeren van een risicoanalyse ten behoeve van een voorgenomen verwerking. De uitkomst van de risicoanalyse wordt gebruikt als uitgangspunt voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. De risicoanalyse dient te worden gezien in de context van gangbare standaarden en normen voor informatiebeveiliging. Er zijn algemene normen zoals de NEN-ISO/IEC 27000 en subnormen (27001 en 27002), maar van belang zijn ook sectorale normen, zoals normen voor gegevensbeveiliging in de zorg en standaarden voor bepaalde aspecten van beveiliging zoals authenticatiemiddelen.

Ook wordt in de richtsnoeren aandacht gegeven aan het inrichten van de juiste processen voor borging van adequate beveiliging. Deze processen zijn van belang voor de continuïteit van beveiliging. Hierboven is het inrichten van een Plan-Do-Check-Act cyclus (PDCA) al genoemd. Daarmee wordt een reguliere controle, evaluatie en zo nodig bijstelling van beveiligingsmaatregelen geborgd in het primaire proces.

Normen

De open norm van artikel 13 Wbp kan op passende wijze worden ingevuld, door te voldoen aan de bestaande (Nederlandse en internationale) normen voor informatiebeveiliging. Voor de zorgsector zijn er de NEN 7510 en subnormen NEN 7512 en NEN 7513 voor informatiebeveiliging in de zorg. Zorginstellingen moeten voldoen aan de voorschriften van de NEN 7510:2011. Maar ook in de rest van de zorgsector biedt de norm goede handvatten voor inrichten van de beveiliging. In toekomstige wetgeving zal het voldoen aan de norm breder verplicht worden gesteld. Nu met de 3-D wetgeving ook de gemeenten zich uitgebreid gaan bezig houden met zorg- en hulpverlening zijn deze normen relevant als toetskader voor de in te richten beveiliging. De normen zijn in elk geval richtinggevend om het niveau van beveiliging te beoordelen en vorm te geven.

NEN 7512

De NEN 7512 gaat in op het inrichten van een vertrouwensketen voor de gegevensuitwisseling tussen zorgaanbieders. Deze norm is in ontwikkeling en publiek beschikbaar op internet. Na een publieke consultatiefase zal de 7512:2013 de NEN 7512:2005 vervangen. Deze norm is vrij technisch van aard en gaat in op beveiligde kanalen voor berichten tussen de bij de zorg betrokken partijen en berichtversleuteling. Daarnaast gaat de norm in op de benodigde wijze van authenticatie van de partijen waarmee gecommuniceerd wordt, gelet op het risico van de soort gegevensverwerking. Deze norm kan een inspiratiebron zijn wanneer de beveiliging van gegevensuitwisseling aan de orde is.

NEN 7513

De NEN 7513 ziet op het inrichten van een 'gebruikersregistratie' van registratiesystemen in de zorg. In de gebruikersregistratie worden alle gebruikershandelingen in het registratiesysteem automatisch vastgelegd (gelogd). Daarmee wordt voldaan aan de controleerbaarheid die de

beveiligingsnormen vereisen voor gebruik van het systeem. Deze norm is toepasbaar als het gaat om de informatiesystemen waarin de dossiers van (jeugd)hulpverleners worden vastgelegd of gegevens uit die context worden uitgewisseld. Controleerbaarheid is nodig om misbruik in het gebruik van systemen tegen te gaan, zoals onbevoegde inzage. Logging en controleerbaarheid vormen ook onderdeel van de algemene normen voor informatiebeveiliging NEN-ISO/IEC 27000 en subnormen.

BIG

Gemeenten moeten voldoen aan de Baseline Informatiebeveiliging voor gemeenten (BIG).⁴ Deze bestaat uit een strategische en een tactische baseline. De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is gebaseerd op de NEN ISO/IEC 27001, bijlage A en NEN-ISO/IEC 27002. De BIG vervangt deze normen niet. In de BIG wordt toegelicht dat het beveiligingsniveau in lagen uitbreidbaar is.⁵ Bij de opbouw van de baseline wordt het principe van gelaagde opbouw gehanteerd. Er is een basisbeveiligingsniveau overeenkomend met departementaal of gemeentelijk 'vertrouwelijk'. Daar waar bepaalde toepassingen, werkomgevingen of specifieke dreigingen een hogere beveiligingsgraad of specialistische maatregelen vereisen, kunnen extra maatregelen getroffen worden bovenop het basisbeveiligingsniveau, zo stelt de norm. Hogere beveiligingsniveau's zijn niet in de baseline uitgewerkt.

Voor verschillende gegevensverwerkingen zal een hoger niveau van beveiliging nodig zijn. Dit volgt uit de eisen die in de sector worden gesteld aan informatiebeveiliging in de zorg. Dit is bijvoorbeeld relevant als de gemeente als jeugdhulpaanbieder optreedt en daartoe gegevens betreffende de hulpverlening moet vastleggen in een dossier, waarop een bijzondere geheimhoudingsplicht van toepassing is. Maar dit kan ook bij uitwisseling van zorg- of hulpverleningsgegevens aan de orde zijn.

3.10 Borging van de samenwerking

Tussen gemeente en ketenpartners zullen afspraken gemaakt moeten worden om een goede samenwerking te borgen. Daarbij moeten ook de noodzakelijke afspraken worden gemaakt om de informatievoorziening en zorgvuldige gegevensverwerking te organiseren en te regelen. Ook kan het daarbij nodig zijn de verantwoordelijkheidsverdeling voor de gegevensverwerking te regelen. Dit is aan de orde bij gezamenlijke verantwoordelijkheid voor bepaalde gegevensverwerking.

⁴ Zie Referentie Modellen Gegevensuitwisseling Jeugddomein, concept VNG.

⁵ Het basisvertrouwelijkheidsniveau in de BIG is vastgesteld als 'Departementaal Vertrouwelijk', zoals gedefinieerd in het Besluit Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie (VIRBI:2012). Voor wat betreft de bescherming van privacygevoelige informatie is uitgegaan van verwerking van persoonsgegevens zoals bedoeld in artikel 16 van de Wbp. De combinatie van beide niveaus komt veelvuldig voor bij de decentrale overheid. Voor gemeenten betekent dit 'vertrouwelijk'. Het gaat dan bijvoorbeeld om persoonsvertrouwelijke informatie, commercieel vertrouwelijke informatie of gevoelige informatie in het kader van beleidsvorming, zogenaamde beleidsintimiteit. (Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten)

De afspraken kunnen in de vorm van convenanten en overeenkomsten worden geregeld.

Tussen bepaalde partijen zijn afspraken wettelijk verplicht:

- Een samenwerkingsovereenkomst tussen gemeente en de Raad voor de Kinderbescherming, over de wijze van samenwerking, de gegevens die gedeeld kunnen worden en de gemeentelijke functies, de door de gemeente aangewezen organisaties of functionarissen waarmee deze gegevens gedeeld kunnen worden.
- Afspraken tussen gemeente en de gecertificeerde instellingen over de wijze van samenwerken bij de uitvoering van een justitiële maatregel. De instelling is verantwoordelijk voor uitvoering van de maatregel, maar de gemeente moet de bestuurlijke en financiële verantwoordelijkheid kunnen waarmaken.
- Een samenwerkingsconvenant VIR. In het convenant is afgesproken welke partijen regionaal mogen melden, hoe met meldingen wordt omgegaan en welke partijen voor welk doel de gegevens uit de melding mogen gebruiken. Het convenant dient door alle potentiële meldende partijen ondertekend te worden. De gemeenten moet het initiatief nemen om te komen tot een convenant.

3.11 Dienstverlening van gekwalificeerde ICT-leveranciers

Als de gemeente of ketenpartner een bewerker inschakelt die namens hem (een deel van) de gegevensverwerking uitvoert, is hij verplicht met de bewerker een bewerkersovereenkomst te sluiten waarin de afspraken over de gegevensverwerking worden vastgelegd. Belangrijk is dat de bewerker geen zeggenschap heeft over de gegevens en ze niet voor eigen doeleinden verder mag verwerken. De bewerker moet zorgen voor een adequate gegevensbeveiliging conform het risico van de gegevensverwerking. Voor gemeenten betekent dit dat soms verder gekeken moet worden naar aanbieders van informatiesystemen die ervaring hebben met de gevoelige gegevensverwerking in de zorg en die een voldoende niveau van beveiliging kennen. Daarbij is het van belang dat bedrijven gecertificeerd aan de normen voldoen.

Belangrijk is om waarborgen te treffen en contractueel te regelen dat gegevens beschikbaar zijn en blijven, ook als de gemeente (of de ketenpartner) de relatie met de leverancier wil beëindigen of deze onverhoeds de dienstverlening moet staken. De verantwoordelijke moet altijd over de gegevens kunnen blijven beschikken en er volledige zeggenschap over houden.

3.12 Rechten van burgers

Een van de uitgangspunten van de Wbp is transparantie, omdat de (on)rechtmatige verwerking van persoonsgegevens een inbreuk kan vormen op de persoonlijke levenssfeer. Om zijn rechten te kunnen uitoefenen moet een burger op de hoogte zijn dat er gegevens over hem worden verwerkt, en door wie en waarvoor.

Nu verschillende verantwoordelijken een rol spelen in de gegevensverwerking in het jeugdstelsel en het gaat om nieuwe situaties waarin gegevens worden verwerkt, is het niet zonder meer duidelijk voor de betrokkene dat zijn gegevens worden verwerkt, welke partijen daarvoor verantwoordelijk zijn en hoe de betrokkene invulling kan geven aan zijn rechten. Zo zal een burger bijvoorbeeld niet altijd meteen weten wat de taak en rol is van een buurtteam en welke gegevens daar worden verwerkt, onder wiens verantwoordelijkheid. Nu dit ook per gemeente kan verschillen is transparantie extra van belang.

Gemeenten moeten op tijd organiseren en inrichten dat burgers voor de uitoefening van hun rechten, zoals inzage en het verwijderen of corrigeren van gegevens terecht kunnen bij de verantwoordelijke voor de gegevensverwerking. Hiervoor moet een procedure worden ingericht die bij alle belanghebbende partijen goed bekend is. Burgers moeten actief worden voorgelicht over de werkwijze van de gemeente en ketenpartners en over de manier waarop zijn rechten kunnen worden geëffectueerd. In het jeugdstelsel moeten hiervoor met de ketenpartners en andere actoren goede afspraken worden gemaakt over een eventuele brievenbusfunctie of doorgeleiding van verzoeken van burgers die op een andere plek binnenkomen dan waar de afhandeling is ingericht.

4. Privacy impact op de uitvoering van de Jeugdwet en de keuzes door gemeenten

4.1 Informatiebehoefte

De specifieke informatiebehoefte en -noodzaak in verband met de uitvoering van de Jeugdwet volgt in de eerste plaats uit de in het wetsvoorstel vastgelegde taken en verantwoordelijkheden en de daarbij gecreëerde grondslagen voor gegevensverwerking. Om zicht te krijgen op de informatiebehoefte wordt gekeken naar de taken en verantwoordelijkheden van verschillende actoren in de Jeugdwet. De noodzakelijke gegevensverwerking kan daarvan afgeleid worden. Dit bepaalt ook wat er vastgelegd en uitgewisseld mag worden.

4.2 Taken Jeugdwet

De Jeugdwet (vanaf 2015 van kracht) bevat onder meer de volgende taken en verantwoordelijkheden waarbij het verwerken van persoonsgegevens aan de orde kan zijn voor de gemeente, jeugdhulpaanbieders, AMHK of gecertificeerde instellingen:

- Preventie en vroegsignalering (artikel 2.1),
- De toegangstaak (artikel 2.6, eerste lid, onderdeel b en g),
- De jeugdhulpplicht (artikel 2.3, eerste lid),
- Het doen van de meldingen aan de Raad voor de Kinderbescherming (artikel 2.4, eerste lid, artikel 3.1, artikel 1:240 BW),
- Het uitvoeren van de kinderschermingsmaatregelen en jeugdreclassering (artikel 2.4, tweede lid),
- Het voorzien in een kwalitatief en kwantitatief toereikend aanbod (artikel 2.6, eerste lid, onderdeel a),
- Gegevensverwerking uit basisadministratie aan de gecertificeerde instelling, artikel 3.6 id 1,
- Gegevensverwerking gemeente ten behoeve van gesloten jeugdhulp (6.1.2 en 6.1.4)
- De dossierplicht (artikel 7.3.8),
- Het verstrekken van een PGB; beoordeling college artikel 8.1.1 lid 3 en heffing eigen bijdrage artikel 8.2.1.

Hieronder wordt voor de taken en verantwoordelijkheden uitgewerkt welke persoonsgegevensverwerking voor de uitvoering van de wet zal kunnen plaatsvinden. Per taak of verantwoordelijkheid vindt gegevensverwerking plaats voor verschillende doeleinden. De wetgever onderscheidt gegevensverwerking ten behoeve van de toeleiding en het treffen van een individuele voorziening (kortgezegd toegang tot), de uitvoering van de jeugdhulp, de uitvoering van kinderschermings- maatregelen en jeugdreclassering en de financiering. Indien de gemeente ervoor kiest een jeugdhulptaak taak in de eigen organisatie met bekwame mensen uit te voeren (art. 2.7 lid 2), is zij voor dat onderdeel jeugdhulpaanbieder en zijn voor de gemeente voor die taak dezelfde regels en beperkingen voor het uitwisselen van gegevens van toepassing als op de jeugdhulpaanbieders.

4.3 Preventie

In de wet wordt preventie en vroegsignalering besproken als taken en activiteiten die door de gemeente worden uitgevoerd. Voor preventie en vroegsignalering is het niet steeds nodig om persoonsgegevens te verwerken. Preventietaken kunnen worden uitgevoerd zonder het verwerken van persoonsgegevens, dit houdt de drempel voor betrokkenen om informatie en steun te vergaren laag. Soms kan het verwerken van bepaalde persoonsgegevens noodzakelijk worden gevonden, bijvoorbeeld bij inschrijving voor een training die als algemene voorziening wordt aangeboden. Vroegsignalering kan helpen om problemen en de inzet van hulp te beperken. Vroegsignalering kan gebeuren bij het uitvoeren van preventie. Vroege signalen kunnen voortkomen uit het inventariseren van signalen die uit het contact met de burger voortkomen. Soms kan er aanleiding zijn om vroegsignalering te formaliseren in een proces, teneinde de inzet van hulp te beperken. Het gaat dan om actieve vroegsignalering. Dan is er sprake van het verwerken van persoonsgegevens.

4.3.1 Gegevensverwerking preventie

Voor preventie worden heel beperkt persoonsgegevens verwerkt, als dat nodig is. Het zal dan vaak in de eerste plaats gaan om contactgegevens en mogelijk is registratie van belang om de toegang te beperken tot inwoners van een gemeente of omdat de toegang aan voorwaarden is verbonden. Een grondslag voor de noodzakelijke gegevensverwerking is te vinden in de wettelijke taak van het bestuursorgaan gemeente om preventie uit te (doen) voeren (artikel 8 lid 1 sub e Wbp).

4.3.1.1 Gemeentelijke keuzes

Een gemeente kan het aanbieden van preventieaanbod en het uitvoeren van preventietaken uitbesteden aan anderen. Dit kan één andere partij zijn of meerdere aanbieders. Als opdracht wordt verleend aan een derde die de preventietaken uit eigen naam zal uitvoeren, dan zal het verwerken van persoonsgegevens, voorzover dat nodig is, gebaseerd zijn op het gerechtvaardigd belang van de aanbieder, of mogelijk ook uitvoering van een overeenkomst met de betrokkene (van zeer beperkte omvang) of de toestemming van de betrokkene conform artikel 8 lid 1 sub f, b of a Wbp. Het gaat dan om het vastleggen van zeer beperkte gegevens voor dit doeleinde door de aanbieder.

Een mogelijkheid is ook dat preventie door een derde in naam van de gemeente wordt uitgevoerd. Bijvoorbeeld in een wijkteam, of ergens anders. In dat geval wordt de preventie juridisch door de gemeente uitgevoerd en is het dus de gemeente die een grondslag behoeft (zie hierboven onder 3.3.1)

4.3.2 Gegevensverwerking vroegsignalering

Vroegsignalering wordt in de wet genoemd en is een methode om de inzet van hulp of ondersteuning zo vroeg mogelijk en zo passend mogelijk aan te bieden om verergering van problemen te kunnen voorkomen of beperken. Veel gemeenten denken daarbij aan het actief ophalen van signalen in bijzondere gevallen. Het actief inrichten van een proces of systeem van vroegsignalering moet met veel waarborgen zijn omkleed. Vroegsignalering is op die manier namelijk risicovol vanuit de invalshoek van de privacywetgeving. Bij actieve vroegsignalering wordt namelijk getracht om voorafgaand aan problematische situaties of bij de eerste tekenen

daarvan een signaal af te geven. Dit signaal betekent een gegevensverwerking van beperkte gegevens, die doorgaans een gevoelige context aanduiden. Actieve vroegsignalering vindt soms in eerste instantie plaats buiten de betrokkene om.⁶ Op basis van criteria die een indicatie van problemen geven wordt een signaal gegenereerd via gegevensverwerking door derden. Soms is er weliswaar een indicatie van problemen, maar heeft deze een andere aanleiding dan de aanloop naar een echt problematische situatie. Vroegsignalering heeft daarom inherent te maken met niet juiste signalen. Daarom zijn strenge voorwaarden verbonden aan het verwerken van persoonsgegevens voor dit doeleinde. Men moet zich voorstellen dat de noodzaak voor het doeleinde van de gegevensverwerking pas na controle van het signaal echt gestaafd kan worden. Dit komt omdat de echte noodzaak voor het verwerken van bepaalde gegevens pas duidelijk wordt bij de controle van een signaal. In de verhouding tussen de overheid en de burger is dit extra van belang omdat het de overheid niet is toegestaan zich in de privésfeer van de burger te mengen zonder dat de wet daarvoor opdracht of ontheffing verleent. Er moet dus altijd getoets worden of de wijze van voorgenomen vroegsignalering gerechtvaardigd is (een grondslag kent). De grondrechten bewaken dit aspect.

Conform de jeugdwet dient de gemeente te zorgen dat haar beleid mede is gericht op preventie en vroege signalering, waardoor de goede vervulling van de publiekrechtelijke taak van de gemeente als verantwoordelijke voor de goede uitvoering van de Jeugdwet kan rechtvaardigen om op gepaste wijze vroegsignalering in te zetten.

Er moet altijd een weging van belangen zijn tussen de doeleinden van de gemeente om erger te voorkomen en de privacybelangen van de betrokken burgers.

Voor vroegsignalering is in elk geval van belang:

- een duidelijk en gerechtvaardigd doel voor bepaalde vroegsignalering vast te stellen;
- strenge en geobjectiveerde criteria vast te stellen op basis waarvan een signaal kan worden gegenereerd (en door wie);
- de gegevensverwerking in het signaal beperken tot het strikt noodzakelijke;
- een zorgvuldig proces inrichten voor de opvolging van een signaal of melding, waarbij de bewaartermijn van onterechte meldingen zeer kort is en de bewaartermijn van terechte meldingen zo kort als mogelijk;
- een zorgvuldig proces in te richten voor het informeren van betrokkenen en het opvolgen van bezwaar van een betrokkene tegen (onjuiste) meldingen en de gegevensverwerking;
- dat in het proces geborgd is dat vroegsignalering niet mag leiden tot stigmatisering of uitsluiting van betrokkenen (en alleen mag worden gebruikt in het belang van betrokkenen).

⁶ Hier wordt niet bedoeld op situaties die onder de wettelijke regeling van de VIR vallen. Zie hieromtrent 4.13. Gedoeld wordt op bijvoorbeeld een melding door energiebedrijven aan de gemeente (waarvoor een wettelijke basis bestaat) dat een huishouden zal worden afgesloten vanwege het niet betalen van de energierekening sinds 6 maanden, of bijvoorbeeld een signaal over een dreigende huisuitzetting vanuit de woningcorporatie. Dit zijn voorbeelden van vroegsignalering en niet per se voorbeelden van vroege signalering in het kader van de Jeugdwet, gemeenten zullen zelf moeten beoordelen wat (mede) bij het Jeugd domein hoort en wat niet.

4.4 De toegangstaak van gemeente

Voor de toegang tot jeugdhulp (en het treffen van de voorziening op het gebied van jeugdhulp) moeten gegevens verwerkt worden om te bepalen of het nodig is dat voor een jeugdige een voorziening wordt getroffen en als dat het geval is, welke. Afhankelijk van de route die door de jeugdige en diens ouders wordt gevolgd (via de huisarts of specialist dan wel via de gemeentelijke toegang) zijn er verschillende mogelijkheden.

Artikel 7.4.1, tweede lid, van de Jeugdwet biedt de basis voor het vastleggen van gegevens door de gemeente voor de toegangstaak. De gemeente treft een individuele voorziening voor jeugdhulp als dat nodig is.

4.4.1. Gemeentelijke keuzes

De gemeente kan de toegang binnen de organisatie inrichten via een loket of in een wijkteam. Daarbij maakt de gemeente altijd gebruik van de expertise van professionals die deze beoordeling kunnen maken en aldus bevoegd en bekwaam zijn. De gemeente kan ook de toegangstaak uitbesteden, behoudens de vaststelling van de rechten en plichten, van de jeugdige of zijn ouders (artikel 2.11 eerste lid Jeugdwet). De gemeente kan aan een of meerdere jeugdhulpaanbieders de inhoudelijke beoordeling van een individuele voorziening uitbesteden. Ook dat kan plaatsvinden binnen een wijkteam, of op een andere plaats.

Wanneer de gemeente kiest voor uitbesteding van deze taak aan jeugdhulpaanbieders dan moet sprake zijn van een machtiging voor het uitvoeren van deze taak. De gemeente moet er daarbij op toezien dat de toegangstaak goed geborgd is. De persoonsgegevensverwerking voor de toegangstaak zal dan door de betreffende jeugdhulpaanbieders gebeuren.

Afhankelijk van de inrichting van de ‘toegangspoort’ kan het zijn dat geoordeeld wordt dat eenvoudige hulpverlening door een wijkteam aangewezen is. Ook kan het zijn dat een doorverwijzing naar meer specialistische hulp nodig is. Deze kan voorzien zijn met jeugdhulpverleners in een wijkteam, maar vaak zal dit op afstand gecontracteerde zorg of hulp zijn, bij de jeugdhulpaanbieder.

De jeugdhulpaanbieder waarnaar een cliënt verwezen wordt zal ook een beoordeling van de passende hulp moeten maken. Daarvoor verwerkt hij gegevens. Ook verwerkt hij gegevens voor de hulpverlening zelf.

Beschikking

Voor een niet vrij toegankelijke voorziening is op grond van de Jeugdwet een besluit van de gemeente nodig. Het is dus noodzakelijk dat bepaalde gegevens hiervoor verwerkt worden door de gemeente, dan wel in naam van de gemeente door een gemandateerde jeugdhulpverlener, al dan niet in een wijkteam. Er zal dus terugkoppeling van een beperkte set gegevens zijn door de jeugdhulpaanbieder die de omvang van de noodzakelijke jeugdhulp vaststelt aan degene die (al dan niet namens de gemeente) een beschikking afgeeft.

Het is van belang dat de gemeenten bij de inrichting van de toegangspoort met deze gegevensverwerking rekening houden en deze zorgvuldig inrichten. Alleen de noodzakelijke

gegevens mogen worden verwerkt. De jeugdhulpverlener legt gegevens van een cliënt vast in een dossier en is gehouden tot geheimhouding van de gegevens. Voor het maken van een beschikking door of in naam van de gemeente worden door de hulpverlener alleen de daarvoor noodzakelijke gegevens verstrekt of (wanneer hij gemandateerd is) gebruikt.

In een beschikking staan zeer beperkt gegevens betreffende de persoon zoals:

- NAW
- geboortedatum
- bsn
- de voorziening waarop de verwijzing betrekking heeft (op globaal zorgsoort niveau)
- eventueel een maximale tijdsduur voor deze voorziening

Gegevens over een diagnose of welke problemen iemand ervaart horen niet in de beschikking en blijven onder de geheimhouding van de professional in het dossier bewaard.

Nadere gegevens over hulpvraag of aanleiding kunnen voor zover noodzakelijk voor de hulpverlening aan betrokkene, tussen de verwijzer en de ontvangende jeugdhulpverlener uitgewisseld worden als de betrokkene daarover is geïnformeerd en ermee heeft ingestemd, en hebben geen plaats in een beschikking.

Het is dus mogelijk dat het maken van een beschikking is gemandateerd aan een private partij zoals de jeugdhulpaanbieder. Daarbij is het noodzakelijk dat de rechten van burgers voldoende geborgd zijn, ook gelet op de vereiste onafhankelijke beoordeling door de gemeente en andere bestuursrechtelijke uitgangspunten. Dit speelt ook mee in de vraag 'door wie' een beschikking gemaakt kan worden in een bepaald geval. Die keuze bepaalt door wie bepaalde persoonsgegevens zullen moeten worden verwerkt in het werkproces.

4.5 Toegang via de huisarts, specialist en jeugdarts

De gemeente zorgt ervoor dat jeugdhulp ook toegankelijk is na verwijzing door de huisarts, medisch specialist en de jeugdarts. De wetgever legt uit dat het daarbij gaat om een directe verwijzingsbevoegdheid. Een verwijzer moet handelen op basis van de voor hem geldende professionele standaard en zolang hij dat doet is voor een beoordeling van de verwijzing door de gemeente geen ruimte. De gemeente gaat niet op de stoel van de professional zitten en er vindt geen individuele sturing door de gemeente plaats. Sturing vindt plaats op basis van goede inkoop- en contractsafspraken vooraf (artikel 2.7 lid 4) en op basis van benchmarkinformatie achteraf.

Naar aanleiding van de verwijzing zal de jeugdhulpaanbieder die de hulp verleent bepalen welke hulp in welke omvang, overeenkomend met de professionele standaard en de inkoopafspraken, geboden is. Ten behoeve van de vergoeding van de hulp zal de jeugdhulpaanbieder enkele noodzakelijke gegevens (die onder de geheimhoudingsplicht vallen) aan de gemeente moeten terugkoppelen. Dit is vergelijkbaar met de huidige situatie bij zorgverzekeraars, wanneer die zorg vergoeden.

Alleen in speciale gevallen van jeugdhulp, waarbij het bijvoorbeeld gaat om een zeer schaarse of een erg dure jeugdhulpvoorziening, waarover in de inkoopafspraken voorwaarden zijn opgenomen, zal de jeugdhulpaanbieder voorafgaande machtiging behoeven van de gemeente om een jeugdhulp op basis van een verwijzing uit te voeren. Dit vereist een beperkte extra gegevensverwerking van noodzakelijke gegevens (die onder de geheimhoudingsplicht vallen van de jeugdhulpaanbieder) om het verzoek te kunnen beoordelen.

4.5.1 Gemeentelijke keuzes

De gemeente treft een individuele voorziening als dit noodzakelijk is voor de ondersteuning of hulp aan de cliënt. Dit betekent dat de gemeente een beschikking afgeeft aan de betrokken burger. Dit is een besluit waarin het recht op deze hulp wordt vastgelegd en waartegen bezwaar mogelijk is. Men kan zich afvragen of het treffen van een individuele voorziening (en dus van een beschikking) door de gemeente 'noodzakelijk' is op het moment dat verwijzing via de arts plaatsvindt, en hulpverlening vervolgens volgens afspraken tussen gemeente en de aanbieder in de tweede lijn plaatsvindt, en de betrokkene daarmee instemt.

Omdat een verwijzing via de arts niet mag worden geblokkeerd door het afgeven van een beschikking vooraf- dat zou de wettelijke verwijsbevoegdheid immers teniet doen- zal dit op een andere manier worden ingericht dan de verwijzing naar een niet vrij toegankelijke voorziening via de gemeentelijke toegangspoort. Het zal dan moeten gaan om een beschikking achteraf, nadat de verwijzing heeft plaatsgevonden en de jeugdhulpaanbieder die de cliënt ontvangt conform de inkoopafspraken heeft vastgesteld welke hulp nodig is. Er zal slechts een marginale toets hierop kunnen plaatsvinden en in beginsel wordt het voorstel voor hulp overgenomen in de beschikking. Dat is alleen anders indien de aangeboden hulp duidelijk afwijkt van de afspraken of de normen (beroepsrichtlijnen). Dit blijkt ook uit de toelichting van de wetgever.

De gemeente heeft verschillende inrichtingsopties voor het omgaan met het vastleggen van een individuele voorziening in een beschikking. De gemeente kan regelen dat bij een doorverwijzing door de arts naar niet vrij toegankelijke jeugdhulp (achteraf) in alle gevallen een beschikking wordt afgegeven. Maar de gemeente kan ook regelen dat zij alleen een beschikking afgeeft op aanvraag van de betrokken jeugdige of zijn ouders. Dit onderscheid wordt gemaakt in de modelverordening jeugdhulp van VNG.

4.6 Jeugdhulpplicht en feitelijke jeugdhulpverlening

Bij de uitvoering van de jeugdhulp zijn de instellingen die de jeugdhulp leveren gebonden aan de regels van het desbetreffende werkveld (jeugdhulp en geneeskundige behandeling).

De verplichting betekent voor de gemeente:

- het treffen van voorzieningen op het gebied van jeugdhulp,
- het waarborgen van een deskundige toeleiding naar de jeugdhulp,
- het waarborgen van advisering over de aangewezen voorziening,
- het waarborgen van het bepalen van de aangewezen voorziening en het daadwerkelijk inzetten daarvan.

De formulering drukt uit dat de gemeente een zorgplicht heeft om deze zaken te waarborgen. De gemeente zal de inhoudelijke afwegingen betreffende de aangewezen voorziening aan de professional overlaten. Hiertoe maakt de gemeente contractuele afspraken met partijen. De professionele standaarden van de jeugdhulpverlening zijn leidend voor de beoordeling door de professional en zullen de basis vormen voor de (inkoop)afspraken tussen gemeente en de aanbieders.

Bij de toeleiding naar de jeugdhulp en het bepalen van de aangewezen voorziening is persoonsgegevensverwerking aan de orde, zoals hierboven al is beschreven.

Jeugdhulpverleners leggen voor het feitelijk verlenen van jeugdhulp een dossier aan voor betrokkene, waarin alle voor de uitvoering van de hulp noodzakelijke gegevens worden vastgelegd (art. 7.3.8). Artsen en professionals die een cliënt zien in het kader van een behandelrelatie leggen een dossier aan op grond van art. 7:545 BW.

4.6.1. Gemeentelijke keuzes

De gemeente is vrij om de uitvoering van deze taken uit te besteden aan anderen (behoudens de vaststelling van de rechten en plichten van de betrokkenen (artikel 2.11 lid 1 Jw)). De eisen en voorwaarden moeten daarbij vanzelfsprekend worden nageleefd. Dat betekent dat de gemeente bij uitbesteding alleen met bevoegde en bekwame derden in zee mag gaan. De gemeente blijft bij uitbesteding verantwoordelijk voor naleving van de wettelijke opdracht.

Het is mogelijk dat professionals een of meerdere van de taken op zich nemen en deze uit eigen naam uitvoeren. Ook is het mogelijk dat de gemeente jeugdhulpaanbieders mandateert om bepaalde taken namens haar uit te voeren, bijvoorbeeld in een wijkteam, in de organisatie van de aanbieder of op een andere plek. De gemeente kan ook de professionals in dienst nemen en de taken intern laten uitvoeren. Voorzover het daarbij gaat om het feitelijk verlenen van jeugdhulp treedt de gemeente die dat zelf uitvoert op als jeugdhulpverlener in de zin van de Jeugdwet.

Als taken worden uitbesteed betekent het dat de noodzakelijke gegevensverwerking om de taken goed uit te voeren verplaatst naar de plek van uitvoering. De gegevensstromen vinden dan plaats tussen verschillende actoren. Dit doet aan de grondslagen voor het verwerken van gegevens voor de jeugdhulpplicht en de feitelijke jeugdhulpverlening niet af. Waar het daarbij steeds om gaat is dat alleen de noodzakelijke informatie wordt gedeeld voor de taak van de ontvanger. Een gemeente die meer 'in huis' doet heeft zelf een grotere gegevensbehoefte dan een gemeente die bijna alles uitbesteedt.

De gemeente die een deel van de jeugdhulp 'in huis' aanbiedt, bijvoorbeeld in een wijkteam waarin zij de jeugdhulpaanbieders in dienst heeft, verwerkt de dossiergegevens ten behoeve van de hulp onder haar eigen verantwoordelijkheid. Ze treedt voor dat stuk immers op als jeugdhulpaanbieder.

Deze andere informatiebehoefte betekent overigens alleen dat de gemeente in het laatste geval bevoegd is om de gegevens te verwerken: dat er voor haar een grondslag voor bestaat om dat te doen voor dit doeleinde. Het betekent niet dat de gemeente als organisatie ook toegang heeft tot de gegevens. Als de gemeente als jeughulpaanbieder optreedt dan geldt voor haar de geheimhoudingsplicht voor jeughulpaanbieders zoals opgenomen in de Jeugdwet. Dat houdt in dat alleen de bevoegde jeugdhulpverlener die de hulp aan de cliënt verleent in beginsel toegang tot het dossier heeft. Ook de organisatie dient deze geheimhoudingsplicht te borgen door middel van de juiste autorisaties in het informatiesysteem waarin dossiergegevens worden vastgelegd. De gegevens kunnen zo nodig door de hulpverlener met rechtstreeks betrokken hulpverleners van de cliënt worden gedeeld.

Natuurlijk bestaat er bij de gemeente op grond van andere taken dan nog een informatiebehoefte. Voor financiële afhandeling kunnen bijvoorbeeld *uitsluitend de noodzakelijke gegevens* door de jeughulpaanbieder die het dossier beheert worden gedeeld met de functionaris die belast is met de afrekening, onder verantwoordelijkheid van de gemeente. Een zorgvuldige manier om dit te doen is middels gestandaardiseerde berichten waarin de noodzakelijke gegevensset is vastgelegd. Net als in het zorgverzekeringsstelsel zullen gegevens betreffende de gezondheid die uit de hulpverleningsrelatie of zorgrelatie afkomstig zijn en voor afrekening moeten worden gedeeld onder verantwoordelijkheid van een geheimhoudingsplichtige moeten worden verwerkt, omdat het beroepsgeheim van de hulpverlener anders illusionair wordt. Aan alle betrokken medewerkers moet daarnaast een geheimhoudingsverplichting worden opgelegd. De gegevens mogen voor dat doeleinde alleen toegankelijk zijn voor degene die op grond van zijn functie toegang nodig heeft.

Welke gegevens de gemeente voor afrekening nodig heeft is vervolgens afhankelijk van de vorm van het financieringsmodel. Rekent de gemeente af per individuele cliënt of is er sprake van een lump sum of subsidiemodel? Dit beïnvloedt de informatiebehoefte van de gemeente voor dit doeleinde. Er mogen nooit meer dan de noodzakelijke gegevens worden verstrekt. Zowel de algemene beginselen van de Wbp als het beroepsgeheim van de professionals verzetten zich daartegen.

4.7 Meldingen aan Raad voor de Kinderbescherming

De Raad voor de Kinderbescherming (Raad) doet onderzoek naar de noodzaak tot het treffen van een kinderschermingsmaatregel. Wanneer de gemeente tot het oordeel komt dat een maatregel omtrent het gezag over de jeugdige overwogen moet worden, doet zij een melding aan de Raad voor de Kinderbescherming. Het is aan de gemeente om invulling te geven aan het systeem van meldingen aan de Raad voor de Kinderbescherming. De gemeente kan overwegen om een jeughulpaanbieder aan te wijzen die rechtstreeks bij de Raad voor de Kinderbescherming een verzoek tot onderzoek (VTO) kan doen.

Zo kan het college rechtstreeks een jeughulpaanbieder aanwijzen, waar deskundigen werkzaam zijn die contacten onderhouden met zowel de Raad voor de Kinderbescherming als met de wijkteams die lokaal diensten verlenen. Deze jeughulpaanbieder bekijkt of kan worden volstaan met vrijwillige hulp en levert deze zo mogelijk. Indien deze hulpverlening stagneert en

er substantiële risico's zijn ten aanzien van de ontwikkeling van de minderjarige, wendt de jeugdhulpaanbieder zich tot de Raad voor de Kinderbescherming. Door het aanwijzen van een jeugdhulpaanbieder kan de gemeente een snelle werkwijze creëren zonder onnodige tussenschakels.

De Raad onderzoekt de noodzaak tot het treffen van een kindbeschermingsmaatregel indien het college, een jeugdhulpaanbieder een gecertificeerde instelling of het AMHK hiertoe een verzoek heeft gedaan (artikel 3.1 Jeugdwet). Als de Raad uit eigen werkzaamheden daartoe aanleiding heeft of kennis heeft van een acute en ernstig bedreigende situatie kan zij ook tot onderzoek overgaan. De Raad doet van het uitvoeren van een onderzoek mededeling aan de gemeente (het college) of de daartoe door het college aangewezen jeugdhulpaanbieder. De gecertificeerde instelling en het AMHK doen ook mededeling aan de gemeente als zij rechtstreeks een verzoek aan de Raad hebben gedaan, zodat de gemeente geïnformeerd blijft en dubbel werk wordt voorkomen.

In uitzonderingssituaties kan een ieder de Raad voor de Kinderbescherming verzoeken een onderzoek te starten. Dit kan indien er sprake is van een acute en ernstig bedreigende situatie voor de minderjarige, wanneer er geen tijd te verliezen is.

Voor de volledigheid wordt opgemerkt dat de burgemeester van de gemeente de bevoegdheid krijgt om de Raad voor de Kinderbescherming te dwingen de rechter een uitspraak te laten doen, indien er een conflict bestaat tussen de gemeente en de Raad voor de Kinderbescherming. Deze bevoegdheid is opgenomen in het wetsvoorstel herziening kindbeschermingsmaatregelen.

De Raad voor de Kinderbescherming en de gemeente hebben hun wijze van samenwerken vastgelegd in een protocol. Het is de bedoeling dat de Raad en de gemeenten op landelijk niveau een kader afspreken, dat in de samenwerkingsverbanden nadere invulling krijgt. In het protocol staan de afspraken omtrent de toeleiding naar het gedwongen kader, de samenwerking tijdens het raadsonderzoek, de afronding van het raadsonderzoek en de samenwerking tijdens de uitvoering van een kindbeschermingsmaatregel. Ook voor jeugdreclassering worden dergelijke afspraken gemaakt.⁷

Als blijkt dat een maatregel nodig is wordt een verzoekschrift aan de rechter opgesteld waarin de gecertificeerde instelling van keuze wordt opgenomen.

Alle bovengenoemde verzoeken en mededelingen vergen een persoonsgegevensverwerking van het betreffende kind en zijn ouders, waarbij de noodzakelijke gegevens moeten worden verstrekt. Het recht om het beroepsgeheim ten behoeve van deze verzoeken aan de Raad te doorbreken volgt uit artikel 1:240 BW. Bij het verstrekken van gegevens aan de Raad zal het gaan om de NAW-gegevens van de betrokkenen en eventueel andere identificerende gegevens

⁷http://www.voordejeugd.nl/images/pdf/handreikingen/Handreiking_voor_samenwerking._Model_samenwerking_protocol.pdf

die noodzakelijk zijn om de gegevens van de juiste personen te verwerken. Daarnaast zullen de noodzakelijke gegevens die de aanleiding van het verzoek duidelijk maken kunnen worden verstrekt. Daaronder zullen vaak bijzondere persoonsgegevens zijn. Het AMHK kan gegevens betreffende de gezondheid uit (lichamelijk) onderzoek aan de Raad verstrekken ten behoeve van het verzoek.

4.7.1 Structureren van de gegevensverwerking

Landelijk dient de uitgangspositie voor een beschermingsonderzoek door de Raad voor de Kinderbescherming uniform te zijn. Mede in het kader van rechtszekerheid is het van belang dat dezelfde informatie worden aangeleverd door de verzoeker. Standaardisering borgt dat langs één lijn de benodigde inzet van zorg beoordeeld kan worden. Daarnaast mag bij de verzoeker geen onduidelijkheid bestaan over hetgeen aangeleverd dient te worden aan de Raad voor de Kinderbescherming.

Om de uniformiteit te bevorderen bij de uitwisseling van gegevens tussen de ketenpartners is een voorziening voor de uitwisseling van deze gegevens ingericht. Het gaat om de Collectieve opdrachtrouteervoorziening (CORV). Deze voorziening dient als een routeervoorziening bij de uitwisseling van de (persoons)gegevens in berichten. Er vindt geen opslag plaats van de verstuurd berichten in het systeem, alleen van de verkeersgegevens. In de opzet van de routeervoorziening is 'privacy by design' toegepast.⁸

Het systeem moet voorkomen dat noodzakelijke gegevensverwerkingen adhoc of op niet gestructureerde wijze wordt uitgevoerd.

4.7.2 Meldingen aan het AMHK

Voor de jeugdhulp is ook van belang dat er een meldrecht aan het AMHK bestaat. De gemeente is ook verantwoordelijk voor het inrichten van een AMHK. Het AMHK zal bovenlokaal gaan functioneren. De inrichting en taken van het AMHK is geregeld in de Wmo 2015, maar het meldrecht is zeer van belang voor de professionals en anderen in de jeugdhulp. Het AMHK wordt wettelijk verankerd in de Wmo, zodat één wettelijk kader voor alle meldingen van huiselijk geweld en kindermishandeling ontstaat.

Het AMHK fungeert als meldpunt voor alle gevallen of vermoedens van huiselijk geweld en kindermishandeling. Het AMHK geeft advies aan de melder. Het AMHK doet onderzoek naar aanleiding van een melding van (een vermoeden van) geweld in huiselijke kring, waaronder kindermishandeling, om te bepalen of sprake is van kindermishandeling of een andere vorm van geweld in huiselijke kring. Het AMHK informeert zo nodig de politie en de Raad voor de Kinderbescherming en schakelt passende hulpverlening in. Zodra blijkt dat vrijwillige hulpverlening de problemen niet kan oplossen en een kind bedreigd wordt in zijn ontwikkeling, draagt het AMHK de casus over aan de Raad voor de Kinderbescherming.

⁸ Op de justitiële ketenberichten en de CORV is een Privacy Impact Assessment uitgevoerd: *'Risico's en Privacy by Design bij de justitiële ketenberichten voor de Jeugdwet'*, in opdracht van het ministerie van VenJ en VWS, door Net2legal (15 juni 2014).

Voor gemeenten is van belang dat de meldingen van professionals op de juiste plek terecht komen. Er moeten dus goede voorzieningen zijn om de meldingen te kunnen doen. Een aantal actoren in de keten (justitiële keten) gebruikt het informatiesysteem CORV voor het doen van meldingen die gericht zijn aan het AMHK.

Met meldingen aan het AMHK dient zeer zorgvuldig om te worden gegaan. Om de melding te kunnen doen is bijna altijd sprake van doorbreking van een geheimhoudingsplicht. De noodzakelijke gegevens mogen uitsluitend worden gedeeld met de beoogde ontvanger, het AMHK. Het versturen van meldingen via een onbevoegde partij is niet toegestaan en moet worden voorkomen. De wetgever voorziet in een wijziging van het besluit politiegegevens de mogelijkheid voor gemeenten om zorgmeldingen van de politie, ook die bestemd zijn voor het wijkteam, via het AMHK te laten verlopen.

Het AMHK zal de uitvoering van deze taak gescheiden moeten houden van de overige aan het AMHK wettelijk toebedeelde taken.

4.8 Kinderbeschermingsmaatregelen en jeugdreclassering

Binnen het geheel van het jeugdterrein zijn de jeugdbescherming en de jeugdreclassering twee bijzondere taken. Deze taken worden vanwege het verplichtende karakter voor ouder en kind ook wel het gedwongen kader genoemd. Alleen de kinderrechter kan besluiten tot een kinderschermingsmaatregel na zorgvuldige beoordeling door de Raad voor de Kinderbescherming.

De uitvoering van kinderschermingsmaatregelen en jeugdreclassering gebeurt uitsluitend door een gecertificeerde instelling. De gemeente zorgt voor een voldoende aanbod van gecertificeerde instellingen. Gemeenten zullen voor de nakoming van deze leveringsplicht bovenlokaal samen gaan werken. Het bovenlokale samenwerkingsverband zal de uitvoering van de kinderschermingsmaatregelen en jeugdreclassering inkopen bij verschillende gecertificeerde instellingen.

Jeugdbescherming en jeugdreclassering zijn taken waarin de rol van de gemeente beperkt zal blijven. De gemeente heeft echter wel de bestuurlijke en financiële verantwoordelijkheid waardoor er wel sprake is van bepaalde informatieuitwisseling.

De gecertificeerde instelling ontvangt ten behoeve van de uitvoering de beschikking en het rapport van de Raad voor de kinderscherming, met daarin de NAW gegevens van de betrokkene en gegevens over de soort maatregel en de gestelde voorwaarden. Daarbij zal het ook gaan om gegevens betreffende de gezondheid en soms andere bijzondere gegevens.

De instelling heeft op grond van artikel 7.3.8 Jeugdwet een dossierplicht en verwerkt de voor de uitvoering van de maatregel of de reclassering noodzakelijke gegevens in het dossier, waaronder ook gegevens over de gezondheid. Voor de uitvoering van jeugdreclassering zal de gecertificeerde instelling ook de noodzakelijke strafrechtelijke persoonsgegevens verwerken.

De gecertificeerde instelling bepaalt of en welke jeugdhulp aangewezen is in het kader van de uitvoering van een kinderschermingsmaatregel of jeugdreclassering (art. 3.5 lid 1). Daarvoor vindt overleg met de gemeente plaats en zal enige persoonsgegevensverwerking nodig zijn. Indien de verplichting tot het bieden van jeugdhulp rechtstreeks voortvloeit uit een strafbeschikking of een rechterlijke beslissing waarbij in jeugdreclassering is voorzien, hoeft de afstemming met de gemeente en de bepaling door de instelling niet plaats te vinden.

De gemeente registreert de opgelegde maatregel gekoppeld aan de uitvoerende instelling. Dit vereist enige persoonsgegevensverwerking van betrokkenen. Ten behoeve van financiering en de regierol van de gemeente ontvangt de gemeente een notificatiebericht met daarin het bsn, de duur en soort maatregel.

4.9 Dossierverplichting; persoonlijk dossier

De jeugdhulpverlener richt een dossier in met betrekking tot de verlening van jeugdhulp. Hij houdt in het dossier aantekening van de gegevens omtrent de geconstateerde opgroei- en opvoedingsproblemen, psychische problemen en stoornissen en uitgevoerde verrichtingen en neemt andere stukken op zover dit voor een goede hulpverlening aan de betrokkene noodzakelijk is. De jeugdhulpverlener voegt desgevraagd een door de betrokkene afgegeven verklaring met betrekking tot de in het dossier opgenomen stukken aan het dossier toe (art. 7.3.8). De bepaling is van overeenkomstige toepassing op de medewerker van de gecertificeerde instelling bij uitvoering van een kinderschermingsmaatregel of jeugdreclassering (art. 7.3.1).

In het dossier van een hulpverlener mogen de gegevens van anderen dan de cliënt (zoals de ouders of andere gezinsleden van de jeugdige) slechts worden opgenomen voorzover het opnemen van de gegevens noodzakelijk is voor de hulpverlening aan de cliënt.

Als er meerdere hulpverleners betrokken zijn, rust op elk van die hulpverleners de plicht om een dossier in te richten. Op grond van dit wetsvoorstel kan geen sprake kan zijn van een gezamenlijk dossier of van een gezinsdossier (Memorie van toelichting).

De ratio achter het feit dat een gezinsdossier geen mogelijkheid is, komt voort uit het feit dat elk mens recht heeft op de bescherming van zijn privéleven, ook ten opzichte van zijn familieleden. Dit is in de Grondwet en het EVRM verankerd. Dit betekent dat cliënten in de zorg recht hebben op een persoonlijk dossier. Een dossier dat te isoleren is van het dossier van een gezinslid of ander. Ook de Jeugdwet en de Wgbo sluiten een gezinsdossier uit. Het is daarbij niet erg dat de behandelaar van meerdere gezinsleden het verband tussen de dossiers in beeld heeft. De techniek kan dat juist ondersteunen.

4.9.1 Een gezin, één plan

Een gezin, één plan, één regisseur behoeft daarom een nuancering. Het gaat daarbij uitdrukkelijk om één plan en één regisseur en niet om één dossier. De wet verzet zich uitdrukkelijk tegen dat laatste. Overigens is een plan van aanpak over een gezin en een regisseur

in de praktijk lang niet altijd aan de orde. Dit is in de Jeugdwet ook niet bedoeld of voorzien.⁹ Jeugdhulp is vaak ook lichte hulp en enkelvoudig van aard. Eén plan en één regisseur speelt alleen bij gezinnen waarbij dit echt noodzakelijk is, in verband met multiproblematiek, volgens minister Plassterk in zijn kamerbrief bij de beleidsvisie over privacy in het sociaal domein in ongeveer 3% van de gevallen.¹⁰

Familiegroepsplan

De Jeugdwet schrijft gemeenten, jeugdhulpaanbieders en gecertificeerde instellingen voor om te werken met het familiegroepsplan, als dat er is. Bij het uitvoeren van jeugdhulp en jeugdbescherming waarbij de ouders niet ontheven zijn uit het gezag, en indien sprake is van vroege signalering van opgroei- en opvoedingsproblemen, psychische problemen en stoornissen biedt de gemeente (artikel 2.1, onderdeel g), de jeugdhulpaanbieder of de gecertificeerde instelling (artikel 4.1.2) als eerste de mogelijkheid aan de ouders van de jeugdige om samen met andere familie en betrokkenen bij de jeugdige een familiegroepsplan op te stellen. Indien afgezien wordt van het opstellen van een familiegroepsplan, wordt bij het uitvoeren van hulp door de jeugdhulpaanbieder en de gecertificeerde instelling gewerkt op basis van een plan waarover is overlegd met de jeugdige en de ouders en dat is afgestemd op de behoeften van de jeugdige.

4.10 Financiering, persoonsgebonden budget en ouderbijdrage

De gemeente moet haar verantwoordelijkheid voor het jeugdbeleid kunnen waarmaken en dus op de hoogte zijn van wat er met jongeren en gezinnen gebeurt, niet in de laatste plaats omdat de gemeente ook de financiële verantwoordelijkheid draagt.

De uitgevoerde jeugdhulp en de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering wordt bij de gemeente in rekening gebracht. Daarvoor zijn beperkte gegevens noodzakelijk. Ten behoeve van financiering ontvangt de gemeente een notificatiebericht met daarin het bsn, de duur en soort maatregel.

Ook waar sprake is van zeldzame, kostbare jeugdhulp, die niet door de gemeente op voorhand is ingekocht, zal de gemeente om zijn jeugdhulplicht uit te kunnen voeren, moeten weten voor welke persoon en welke hulpvraag (globaal) een voorziening moet worden getroffen.

Op verzoek van ouders en jeugdigen kan de gemeente ook een persoonsgebonden budget (pgb) verstrekken. Daarbij moet worden voldaan aan de voorwaarden van artikel 8.1.1 van de Jeugdwet. Bij verstrekken van een pgb zullen noodzakelijke gegevens van betrokkenen moeten worden verwerkt door de gemeente in verband met de beoordeling van de aanvraag. Het

⁹ Zie artikel 2.1 sub f Jeugdwet en de uitleg hierover in de MvT op de Jeugdwet, § 3.4. Integrale jeugdhulp: één gezin, één plan, één regisseur, Tweede Kamer, vergaderjaar 2012–2013, 33 684, nr. 3, p.19.

¹⁰ Brief van minister Plasterk (BZK) aan de Tweede Kamer over de beleidsvisie met richtlijnen voor het zorgvuldig omgaan met persoonsgegevens in de gemeentelijke praktijk in het kader van de decentralisaties van 27 mei 2104.

verstrekken van het pgb gebeurt middels een beschikking, waarvoor gegevensverwerking plaatsvindt.

Beperkte gegevensverwerking vindt plaats om na te gaan of een ouderbijdrage verschuldigd is (artikel 8.2.1). Dit kan inhouden dat de gemeente gegevens verstrekt aan het bestuursorgaan dat met inning is belast (het CAK). Ook betrokkenen dienen noodzakelijke gegevens te verstrekken aan het bestuursorgaan voorzover nodig voor het vaststellen en innen van de bijdrage (artikel 8.2.4).

4.11 Pleegzorg

In verband met pleegzorg kan een pleegzorgaanbieder als bedoeld in de Jeugdwet aan een pleegouder de gegevens en inlichtingen verstrekken die de pleegouder nodig heeft voorafgaand aan plaatsing van het kind bij de pleegouder. Het gaat daarbij om de persoonsgegevens van het kind en eventuele anderen in het netwerk van het kind en kan ook om gezondheidsgegevens gaan (artikel 5.4 Jeugdwet).

4.12 Onder toezicht stelling (ots) en gesloten jeugdhulp

De kinderrechter kan op verzoek een machtiging verlenen om een jeugdige in een gesloten accommodatie te laten opnemen en verblijven wanneer dat noodzakelijk is en aan de voorwaarden van artikel 6.1.2 van de Jeugdwet is voldaan. Zowel de gemeente als de gecertificeerde instelling, wanneer die ots of voogdij over de jeugdige uitvoert, zijn hierbij betrokken. Soms is de Raad voor de Kinderbescherming hierbij betrokken. Een machtiging kan alleen worden verleend als hetzij de gecertificeerde instelling, hetzij de gemeente heeft bepaald dat jeugdhulp voor de betrokkene en verblijf (niet zijnde verblijf bij een pleegouder) nodig is, of als de Raad voor de Kinderbescherming de machtiging op grond van het bepaalde in artikel 6.1.2 lid 2 nodig acht. Daarbij is een onderzoek door een gekwalificeerd gedragswetenschapper nodig, die op grond daarvan instemt met het verzoek.

Er kan sprake zijn van het verlenen van een spoedmachtiging of een voorwaardelijke machtiging. Het college moet bepalen dat een voorwaardelijke machtiging voor een voorziening van jeugdhulp (door de rechter) nodig is (artikel 6.1.4 lid 3 Jeugdwet). Om een voorwaardelijke machtiging te kunnen krijgen moet door de instelling een hulpverleningsplan worden overlegd waarmee de betrokkene zich akkoord verklaard.

Een en ander vereist de daarvoor noodzakelijke gegevensverwerking door gemeente, de Raad en de gecertificeerde instelling. De gedragswetenschapper legt de gegevens betreffende het onderzoek vast in een dossier overeenkomstig de dossierplicht. De uitslag van het onderzoek zal met de kinderrechter moeten worden gedeeld.

Op grond van artikel 6.1.11 Jeugdwet wordt een afschrift van de beschikking inzake de machtiging aan een aantal actoren toegezonden waaronder de verzoeker (dat kan de gemeente zijn), en degene die het gezag over de jeugdige heeft (dat kan de gecertificeerde instelling zijn).

Gegevensverwerking vindt daarnaast ook plaats door de gecertificeerde instelling die de betrokkene opneemt in de gesloten accommodatie. De gegevens worden vastgelegd in het dossier dat op grond van artikel 7.3.8 wordt bijgehouden over de betrokkene. Het gaat daarbij zowel om gegevens over de verleende jeugdhulp en gezondheidsgegevens als gegevens die van belang zijn in verband met de machtiging.

Ten behoeve van financiering en de regierol van de gemeente ontvangt de gemeente een notificatiebericht met daarin het bsn, de duur en soort maatregel.

4.13 Verwijsindex risico jongeren

Een belangrijk aspect van de Jeugdwet is daarnaast de Verwijsindex risicojongeren (VIR). De regeling rondom de verwijsindex bestond al en is overgenomen in de Jeugdwet. De voorwaarden rondom de verwijsindex zijn opgenomen in artikel 7.1.4.3 Jeugdwet en verder. De gemeente die verantwoordelijk is voor de goede inrichting van de verwijsindex in de gemeente is hierbij gehouden aan de beperkingen en voorwaarden die de wet stelt.

Veel gemeenten hebben een regionale applicatie ingericht waarmee vorm gegevens wordt aan de VIR. Het is van belang erop toe te zien dat de regionale inrichting niet meer mogelijk maakt dan wettelijk is voorgeschreven. In artikel 7.1.4.3 wordt beschreven welke gegevens uitsluitend mogen worden verwerkt:

Artikel 7.1.4.3

1. Naast het burgerservicenummer van de jeugdige worden in de verwijsindex bij een melding uitsluitend de volgende gegevens opgeslagen:
 - a. de identificatiegegevens en contactgegevens van de meldingsbevoegde die de melding doet, en, in voorkomend geval, van de coördinator, bedoeld in artikel 7.1.3.3;
 - b. de datum en het tijdstip van de melding, en
 - c. de datum waarop de melding op grond van artikel 7.1.4.5, tweede lid, onderdeel a, uit de verwijsindex zal worden verwijderd.
2. Een signaal uit de verwijsindex bevat uitsluitend de gegevens, genoemd in het eerste lid, onderdeel a, en, indien het signaal voortvloeit uit twee of meer meldingen die niet dezelfde jeugdige betreffen, dit gegeven.

In artikel 7.1.4.4 wordt geregeld dat persoonsgegevens betreffende de gezondheid, alsmede strafrechtelijke persoonsgegevens als bedoeld in artikel 16 van de Wbp worden verwerkt. De verwerking van deze gegevens vindt uitsluitend plaats om meldingsbevoegden uit de domeinen jeugdgezondheidszorg, gezondheidszorg en politie en justitie in staat te stellen een jeugdige aan de verwijsindex te melden. Dit is een ingewikkelde bepaling en betekent *niet* dat naast de bovengenoemde gegevens ook aanvullend gegevens over gezondheid of strafrechtelijke gegevens mogen worden verwerkt in de regionale applicaties van gemeenten. Deze bepaling is uitsluitend in de wet opgenomen omdat door het melden door bepaalde beroepsgroepen van de gegevens genoemd in artikel 7.1.4.3 automatisch sprake is van het verwerken van deze categorieën gegevens.

5. Verwerken van het bsn

5.1 Uitgangspunt

Artikel 24 Wbp beperkt het gebruik van wettelijke persoonsnummers. Het artikel stelt dat een nummer ter identificatie van een persoon bij wet voorgeschreven, bij de verwerking van persoonsgegevens slechts wordt gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.

5.2 Huidige situatie

Het verwerken en gebruik van het bsn wordt in algemene zin geregeld in de Wet algemene bepalingen burgerservicenummer (Wabb). De gemeente is bevoegd tot het verwerken van het nummer bij het verwerken van persoonsgegevens. Op dit moment is het gebruik van het bsn verplicht voor instellingen die vallen onder de Kwaliteitswet zorginstellingen alsmede voor beroepsbeoefenaren van wie het beroep of de opleiding worden geregeld in of ingevolge de Wet BIG. Dat volgt uit de Wet gebruik bsn in de zorg. Jeugdhulpaanbieders zullen op grond van de aanstaande Wet gebruik bsn in de jeugdzorg het bsn gaan gebruiken in hun administratie en bij uitwisseling met elkaar, andere zorgaanbieders en gemeente.

5.3 Jeugdwet

Het gebruik van het bsn vanaf de inwerkingtreding van de Jeugdwet is opgenomen in § 7.2. van het wetsvoorstel Jeugdwet. In dit artikel is de verplichting opgenomen voor de gecertificeerde instellingen, de jeugdhulpaanbieders, de Raad voor de Kinderbescherming en het college om het bsn van een jeugdige te gebruiken met het doel te waarborgen dat de in het kader van de uitvoering van deze wet te verwerken persoonsgegevens op die jeugdige betrekking hebben. Artikel 10.4, derde lid, onder a, van het wetsvoorstel Jeugdwet regelt het gebruik van het bsn bij de eenmalige overdracht van cliëntgegevens vanuit de huidige Bureaus Jeugdzorg naar de gemeente, jeugdhulpaanbieders of gecertificeerde instellingen. Daarom treedt de Wet gebruik bsn in de jeugdzorg in 2014 in werking, voorafgaand aan de Jeugdwet. Deze bepalingen vormen de in artikel 24 van de Wbp vereiste wettelijke grondslag om het bsn te gebruiken.

AMHK

in hoofdstuk 11.2 van het wetsvoorstel Jeugdwet worden de artikelen 7.2.1 tot en met 7.2.6 van overeenkomstige toepassing verklaard op het AMHK. Ook het AMHK zal derhalve het bsn moeten gebruiken in de eigen administratie en in de uitwisseling met de andere actoren die het bsn verwerken.

Preventie geen grondslag

Nu het voorkomen van psychische problemen en stoornissen, psychosociale problemen of gedragsproblemen van de jeugdige of opvoedingsproblemen van de ouders niet onder het begrip jeugdhulp valt, worden aanbieders van deze vormen van preventieve hulp niet gezien als jeugdhulpaanbieder. Deze aanbieders zijn dan niet bevoegd het bsn te gebruiken bij de verwerking van gegevens. Dat is anders als de gemeente deze taken uitvoert, de gemeente is uit andere hoofde bevoegd het bsn te gebruiken en in het kader van de verantwoordelijkheden uit de Jeugdwet verplicht het nummer te gebruiken. Bij uitbesteding van taken aan derden wordt

deze grondslag niet 'mee uitbesteed'. Het is de vraag of het de bedoeling van de wetgever is hier onderscheid in te maken. Logisch zou zijn dat de actoren uit de Jeugdwet in hun administratie en onderlinge communicatie het nummer gebruiken bij alle taken die (gerechtvaardigd) voortvloeien uit de Jeugdwet.

5.4 Verwerken bsn op grond van Wmo

In artikel 5.2.9 van de Wmo 2015 wordt geregeld dat alle actoren uit de Wmo 2015 alsmede de zorgverzekeraar en de zorgaanbieder als bedoeld in de Zorverzekeringwet het bsn verwerken bij het verstrekken van persoonsgegevens van een persoon conform hoofdstuk 5 Wmo 2015, met het doel te waarborgen dat de in het kader van de uitvoering van deze wet te verwerken persoonsgegevens op die persoon betrekking hebben. In verband met de overlap binnen bijvoorbeeld wijkteams in de uitvoering van de 3-D wetten is het relevant dit hier te vermelden. De bedoelde instanties en personen stellen het burgerservicenummer van betrokkene vast wanneer zij voor de eerste maal contact met betrokkene hebben in het kader van de uitvoering van de Wmo 2015 en de daarop berustende bepalingen.

5.5 Controle van het nummer

Het bsn dient door degene die het vaststelt te worden geverifieerd in het nummerregister, via de aangewezen voorzieningen zoals bedoeld in de Wabb. Het gaat daarbij, afhankelijk van de verwerkende partij, om de BV-bsn of de SBV-Z. Het is niet nodig de voorzieningen en het register te raadplegen als het nummer verkregen is van een andere gebruiker op grond van de Wabb die gehouden is het nummer te verifiëren in het register en/of via een van de voorzieningen of als het nummer verkregen is uit de gemeentelijke basisadministratie van persoonsgegevens.

5.6 Bsn in het wijkteam

Valt de werkzaamheid in een wijkteam bijvoorbeeld buiten de uitvoering van de Jeugdwet of de Wmo (en wordt deze bovendien niet uitgevoerd door een zorgverlener zoals bedoeld in de Wet bsn in de zorg) en gebeurt deze ook niet uit naam van de gemeente (gemandateerd), dan is er geen grondslag voor het verwerken van het bsn. Dit kan in de praktijk tot een gekke situatie leiden in de wijkteams, waar het soms wel moet en mogelijk bij andere activiteiten niet mag. Aanbevolen wordt om goed te kijken naar de taakomschrijving van eventuele wijkteams en de (juridische) inrichting van de teams.

6. Aanvullende aanbevelingen bij waargenomen risico's

6.1 Integrale aanpak en intercollegiale toetsing

Voor de goede uitvoering van taken, hulpverlening en ondersteuning kan het noodzakelijk zijn om intercollegiale toetsing te hebben. De kwaliteit en zorgvuldigheid in processen kan ook vergen dat afstemming of gezamenlijke aanpak nodig is. In werkprocessen moet worden vastgelegd hoe bepaalde taken worden vormgegeven en welke medewerkers of disciplines daarbij betrokken moeten zijn. Dit is ook van belang voor bijvoorbeeld de vraag hoe intake plaatsvindt of hoe cliënten aan een ondersteuner worden 'toebedeeld'. De inrichting kan beïnvloed worden door het gegeven dat met generalisten of juist met specialisten wordt gewerkt op de plek waar toeleiding plaatsvindt en/of (lichte) jeugdhulp wordt verleend.

Belangrijk uitgangspunt is dat betrokken medewerkers altijd voor de taken bevoegd en bekwaam moeten zijn. Maar het is niet ondenkbaar dat zij dat voor bepaalde taken of in bepaalde gevallen niet 'alleen' zijn. Als de hulpvraag of situatie het verlangt kan het een keuze in het proces zijn om bepaalde taken door een team te laten uitvoeren van bijvoorbeeld twee generalisten met een andere achtergrond of door een generalist en een specialist in een bepaald werkveld samen. Dit zijn keuzes die worden gemaakt voor een zorgvuldige taakuitvoering.

In de fase van (lichte) hulpverlening wordt in beginsel uitgegaan van een (hoofd)behandelaar of ondersteuner (soms regisseur) van de cliënt die het dossier van de cliënt beheert. Ook daarbij kan het nodig zijn dat andere hulpverleners direct betrokken worden bij de hulp of ondersteuning om zo de beste ondersteuning te bieden. Dit gebeurt in afstemming met de cliënt. In al deze gevallen is de uitwisseling van noodzakelijke gegevens een inherente voorwaarde voor een zorgvuldig ingericht proces en professionele ondersteuning.

Een privacyrisico bestaat in het zonder absolute noodzaak voor dit doel breder delen van gegevens. Het inrichten van processen die leiden tot een bredere deling dan nodig is niet toegestaan. Ook niet in het kader van 'integraal werken'. 'Integraliteit' wordt in de Jeugdwet alleen genoemd in artikel 2.1 sub f. 'Integraliteit' mag niet zo worden opgevat alsof het een keuze is van gemeenten om afstemming binnen disciplines en tussen verwante disciplines naar eigen inzicht en behoefte in te richten.¹¹ Grondslag, noodzaak en proportionaliteit zijn altijd leidend. Daarbij komt dat in het jeugdhulpdomein en verwante domeinen in het sociale domein de vertrouwelijkheid uitgangspunt is voor gegevens die door de hulpverlener over de cliënt verkregen zijn. De persoonsgegevens van de cliënt worden daarom door zo min mogelijk personen verwerkt of ingezien. Samenwerking is dus van belang, maar persoonsgegevensverwerking vindt alleen plaats zover nodig en wettelijk toegestaan.

Ook bij het verzamelen van gegevens van de cliënt ten behoeve van zijn hulp- of ondersteuningsvraag speelt dit aspect een belangrijke rol. Een 'integrale aanpak' door gemeenten mag ook niet betekenen dat over het hoofd van de cliënt met 'een druk op de knop'

¹¹ Zie ook 4.9.1 en de voetnoot daarbij.

gegevens uit allerlei voor de gemeente beschikbare bronnen worden betrokken. De wettelijke bepalingen over doelbinding en vertrouwelijkheid staan daaraan in de weg. Een zorgvuldige werkwijze kan worden ingericht door de noodzakelijke gegevensverwerking voor verschillende wettelijke taken vast te stellen en daarbij de nodige gegevensstromen in kaart te brengen.¹² In werkprocessen kan op hoofdlijnen al worden bepaald waar en wanneer voor bepaalde taken gegevens en gegevensdeling noodzakelijk of mogelijk (kunnen) zijn. Bijvoorbeeld tussen een gemeenteloket en een wijkteam bij de uitvoering van bepaalde taken. Daarnaast zal per situatie een beoordeling kunnen worden gemaakt van de noodzakelijke gegevensverwerking die aanvullend nodig is en de grondslag waarop die is toegestaan. Processen moeten echter zo veel mogelijk gestructureerd worden om bovenmatige gegevensverwerking en onzorgvuldige uitwisseling te voorkomen. Structurering is niet alleen nodig voor de processen en de inhoud van de gegevensverwerking, maar ook voor de manier waarop gegevens worden gedeeld. Ad hoc gegevensverwerking leidt er vaak toe dat op een onveilige manier wordt uitgewisseld. In een grote operatie als deze, waarbij persoonsgegevensverwerking van veel personen in veel diverse situaties aan de orde is en waarbij heel veel medewerkers betrokken zijn, is de kans daarop alleen maar groter. Goede werkprocessen, gedragsrichtlijnen voor medewerkers en voldoende waarborgen in de inrichting zijn daarom van groot belang.

6.1.1 Casusoverleg

Casusoverleg is een bijzondere vorm van gegevensuitwisseling. De uitvoering van de hulpverlening en ondersteuning dient aan de wet te voldoen. Casusoverleg is niet iets waar aparte regels voor gelden. Als bij casusoverleg persoonsgegevens worden uitgewisseld dan dient dit dus aan de Wbp en de bijzondere wetgeving te voldoen. Degene die als professional gegevens wil delen met een ander dient daarvoor een grondslag te hebben en de noodzaak tot het delen van bepaalde gegevens met bepaalde anderen te hebben vastgesteld. De reden dat casusoverleg extra aandacht verdient bij bespreken van de privacy impact is dat er een uitvoeringspraktijk bestaat van allerlei (al dan niet gerechtvaardigde) casusoverleggen.

Zoals uit het wettelijk kader en het bovenstaande volgt is het uitgangspunt bij persoonsgegevensverwerking altijd dat niet meer dan noodzakelijk wordt verwerkt. Daarnaast moeten actoren die gegevens verwerken (door ze beschikbaar te stellen of te ontvangen) daar een grondslag voor hebben. Casusoverleg is dus nooit een vertrekpunt. Het kan hooguit, door omstandigheden genoodzaakt, toegelaten zijn. Omdat de inzet van casusoverleg op verschillende plekken en bij verschillende taken speelt, of juist bij taken die op elkaar aansluiten, wordt hier alleen in algemene zin iets over casusoverleg gezegd. Een bekend voorbeeld van casusoverleg is overleg in het kader van het Veiligheidshuis, overleg in een ZAT (Zorg Advies Team) in het onderwijs, maar er vinden ook casusoverleggen plaats in buurtteams. Over de specifieke aspecten daarvan en de risico's voor de privacy compliance is door het CBP en in privacy rapportages al veel geschreven.

¹² In de Memorie van Antwoord en de Nadere memorie van Antwoord bij de Jeugdwet wordt in schema's een overzicht gegeven van de noodzakelijke gegevensverwerking bij wettelijke taken. Uiteraard gaat het om een uitgangspunt dat in de praktijk moet worden uitgewerkt en in werkprocessen moet worden vormgegeven.

De toepassing van de wet betekent in elk geval dat:

- casusoverleg waar mogelijk niet herleidbaar tot betrokkenen plaatsvindt;
- overleg alleen plaatsvindt met de personen die noodzakelijk betrokken moeten worden;
- van elk (soort) overleg het gerechtvaardigde doeleinde vast moet staan en op basis daarvan deelnemers en de in te brengen soort casus kunnen worden bepaald;
- criteria voor inbreng van een bepaalde casus moeten worden vastgesteld;
- er nooit een verplichting tot inbreng van bepaalde casus is, maar dat de inbrenger een afweging per geval maakt van de rechtmatigheid;
- elke deelnemer gehouden is aan de regels van zijn beroepsgroep (er gelden o.a. bijzondere beperkingen voor zorgverleners en politie en justitie);
- De geheimhoudingsplicht en de waarborgen en voorzorgen die daarbij horen door geheimhouders worden nageleefd;
- Alleen besproken wordt wat nodig is en alleen wordt vastgelegd of (schriftelijk) gedeeld wat strikt noodzakelijk is;
- De afspraken over casusoverleg en de verplichtingen van de deelnemers schriftelijk zijn vastgelegd.

6.2 Regie van de cliënt

In de referentiemodellen van VNG wordt ook de regie van de cliënt als een inrichtingskeuze beschreven. Hoewel er wel enige nuance mogelijk is in de kijk van gemeenten hierop, is er niet echt sprake van een inrichtingskeuze. Dat heeft twee belangrijke redenen.

Vanuit grondrechtsbeginselen heeft een betrokkene in beginsel 'regie' over hulp of ondersteuning die hem wordt geboden. Het is geen keuze van de overheid om hiervan af te wijken. Alleen als een cliënt in een situatie zit waarin er ook in dit opzicht geen zelfredzaamheid is, is ondersteuning hierin geboden.¹³ Er moet dan een rechtvaardiging zijn voor drang of dwang. Dit kan een rol spelen bij met name multi-problematiek, zoals in de beleidsvisie van BZK ook besproken wordt.

Anderzijds is er om bepaalde taken goed te kunnen uitvoeren, noodzaak tot bepaalde persoonsgegevensverwerking door de verantwoordelijke. Het zou dan onzorgvuldig kunnen zijn dit bij de cliënt te laten. Daarnaast is er in veel gevallen een dossierverplichting als het gaat om hulpverlening en ondersteuning. Het is dan niet mogelijk dat de cliënt die gegevens (ook over de noodzakelijke betrokkenheid van andere zorgverleners bij een hulptraject) in plaats van de hulpverlener beheert.

6.3 Verder verwerken van gegevens voor monitoring en beleid

De gemeente zal monitoringinformatie gaan vastleggen op basis van gegevens die in verband met de Jeugdwet worden verwerkt, bijvoorbeeld in verband met de werkzaamheden van wijkteams. Het is goed daarbij aandacht te hebben voor de uitgangspunten voor persoonsgegevensverwerking: informatie ten behoeve van beleid mag niet herleidbaar worden gedeeld met beleidsmakers. Resultaatmeting en sturingsinformatie voor bestuur van de

¹³ Zie ook de toelichting van de wetgever (MvT Jeugdwet) op artikel 2.1 sub f Jeugdwet.

gemeente en het rijk horen niet op herleidbaar niveau verwerkt te worden buiten de macht van de bron bij de ontvanger. Bij de bron (waar de gegevens met grondslag worden vastgelegd) kunnen de gegevens wel herleidbaar worden bewerkt door een bevoegd persoon voor (niet herleidbare) rapportage.

Gegevens worden voor dit doeleinde zoveel mogelijk geanonimiseerd. Zo nodig kunnen gegevens door zorgvuldige pseudonimisering niet herleidbaar worden gekoppeld met andere gegevens. Pseudonimiseren is aan voorwaarden gebonden om ervoor te zorgen dat gegevens niet herleidbaar zijn. Het CBP heeft de voorwaarden hiervoor uitgewerkt.

6.4 Gebruik van meetinstrumenten (ZRM)

Gebruik van meetinstrumenten in het jeugdstelsel en het verwerken van gegevens daaruit valt evenzeer onder de Wbp als andere verwerking van persoonsgegevens.

Bij gemeenten wordt op diverse plaatsen gebruik gemaakt van de Zelfredzaamheidsmatrix (ZRM). Deze ZRM geeft een indicatie van de mate waarin cliënten op elf leefgebieden al dan niet zelfredzaam zijn. Het gaat om onder andere de domeinen van het dagelijks leven, financiën, wonen, werken, justitie en gezondheid. Bij beperkte zelfredzaamheid op meerdere domeinen worden cliënten in de praktijk aangemeld bij een buurtteam of wordt er op andere wijze actie ondernomen. In veel gevallen wordt de uitkomst van de ZRM dan ook verwerkt in een registratie.

Een waarneming bij gemeenten is dat de cliënten soms schrikken van het gebruik van de ZRM, omdat zij de vragen daaruit niet verwachten en deze diep ingrijpen in de privésfeer. Registratie van de ZRM leidt tot het verwerken van verschillende soorten bijzondere persoonsgegevens waarvoor een strikt regime geldt. Het gebruik van de ZRM is wijdverbreid. Het 'standaard' verwerken van gegevens afkomstig uit een ZRM is zonder meer bovenmatig. Het is noodzakelijk om (opnieuw) na te gaan waar en wanneer het gebruik van de ZRM in de gegevensverwerking echt noodzakelijk en toegestaan is. Uitdrukkelijke toestemming kan mogelijk voor het verwerken van de ZRM soms een grondslag zijn (buiten de sfeer van een behandelrelatie, bijvoorbeeld bij vermoedens van multiproblematiek bij het loket van Werk en Inkomen), maar dat kan alleen als de ZRM in het proces niet verplicht wordt gesteld. Daarboven is het niet billijk om toestemming te vragen voor het afnemen en verwerken van (onderdelen van) de ZRM, in de gevallen dat het niet echt nodig zou zijn om deze gegevens te verwerken of de betrokkene zich niet vrij voelt om 'nee' te zeggen.

Bij de noodzakelijkheidstoets moet ook worden betrokken of alle onderdelen van de ZRM steeds noodzakelijk zijn. Over het algemeen worden alle velden ingevuld omdat de interpretatiewijze dat voorschrijft. Maar het is denkbaar dat de informatie uit de ZRM op een andere manier gewogen wordt. Ook kan overwogen worden in welke gevallen de ZRM als hulpmiddel voor de professional gebruikt kan worden, zonder dat de gegevens uit de ZRM daarbij worden vastgelegd.

De praktijk beschikt ook over andere toestinstrumenten die soms worden toegepast. Een voorbeeld daarvan is het Licht Instrument Risicotaxatie Kindveiligheid (LIRIK). De LIRIK is een

hulpmiddel dat is ontwikkeld voor professionals in de jeugdzorg bij het beoordelen of er sprake is van kindermishandeling of dat het kind risico loopt in de toekomst. De LIRIK is een checklist die hulpverleners helpt om gestructureerd een oordeel te vormen. Ook voor het verwerken van gegevens uit het gebruik van de LIRIK geldt dat dit steeds noodzakelijk moet zijn. Het uitbreiden van het doel van het gebruik of de soort gebruikers zal al snel tot bovenmatige gegevensverwerking leiden. Het is daarom noodzakelijk om ook voor andere meetinstrumenten zoals de LIRIK na te gaan waar en wanneer de gegevensverwerking volgend uit het gebruik gerechtvaardigd is. Voor alle meetinstrumenten geldt dat de rechtmatigheidstoets voor het verwerken van gegevens daaruit dus samenhangt met de plaats waar en door wie (voor welk doel) het instrument wordt afgenomen.

6.5 Inrichten van wijkteams

Hierboven is al beschreven dat voor de uitvoering van taken in wijkteams de juiste bevoegdheid en bekwaamheid van de teamleden nodig is. Daarnaast hebben de teamleden een bepaalde achtergrond. Als de teamleden bepaalde werkzaamheden blijven uitvoeren naast de taken in het team dan kunnen zij te maken krijgen met 'twee petten problematiek'. Het is dan de vraag of het naar de burger gerechtvaardigd is om deze dubbele functie in stand te houden. Daarbij kan gedacht worden aan medewerkers van de gemeente (bijvoorbeeld van Werk en Inkomen) in een team van professionals die belast zijn met toeleiding, preventie en hulpverlening. Medewerkers van de gemeente kunnen cliënten van het loket kennen en in het team weer tegenkomen. Wanneer bijvoorbeeld de kennis over cliënten in het team bepaalde beslissingen in de andere functie beïnvloed, is de dubbelrol problematisch in deze verhouding tussen burger en overheid. Dat kan de gegevensverwerking voor de betreffende werkzaamheden die daaruit voortvloeit onrechtmatig maken. Dat speelt des te meer als gegevens in het team worden verkregen onder de geheimhoudingsplicht van het teamlid als hulpverlener. Die kunnen dan niet worden aangewend in de uitvoering van een andere rol, bijvoorbeeld als handhaver. Dubbelrollen dienen daarom zorgvuldig beoordeeld en geëvalueerd te worden.

Iets dergelijks speelt bijvoorbeeld ook wanneer de schoolmaatschappelijk werker die inmiddels alleen wijkteammedewerker is, nog steeds aan het interne zorgoverleg op de school deelneemt en daarover in het schoolsysteem registreert. Als de wijkteammedewerker niet meer optreedt als schoolmaatschappelijk werker is dat niet wenselijk. Dit doet niet af aan de mogelijkheid van de wijkteammedewerker om een adviesrol te hebben naar de scholen als dat nodig is. Als uitgangspunt zou dat zonder het verwerken van persoonsgegevens moeten gebeuren, tenzij er sprake is van een uitzonderingsgrond waarvoor het verwerken van persoonsgegevens noodzakelijk is. Over de rol van de wijkteammedewerker moeten duidelijke afspraken en keuzes worden gemaakt, om te voorkomen dat de medewerker onbevoegd persoonsgegevens vergaart en burgers ongevraagd, onverwacht en onnodig gaat 'monitoren'.

6.6 Regels in het wijkteam

In de WGBO en de Jeugdwet worden bepaalde eisen gesteld aan degene die de hulp aanbiedt en de manier waarop hij werkt. Als een van deze wetten van toepassing is op de hulp die door een teamlid in een wijkteam verleend wordt, geldt de wettelijke dossierplicht, bewaartermijn en het beroepsgeheim ten aanzien van de gegevens die van de cliënt worden verkregen. Het

werkproces en het registratiesysteem moeten deze zaken ondersteunen en borgen. Dit heeft ook consequenties voor de autorisaties op het systeem.

Op het verwerken van persoonsgegevens van cliënten in een wijkteam kunnen, afhankelijk van de toedeling van taken en de inrichting, naast de regels van de Wbp ook de Jeugdwet, de WGBO, de Wet publieke gezondheid (Wpg) en de Wet BIG bij bepaald handelen van toepassing zijn. Dit maakt het voor de teamleden soms lastig om te weten waaraan ze moeten voldoen als dat niet duidelijk wordt verankerd in het werkproces. Het kan raadzaam zijn om ook een speciale instructie voor gegevensverwerking op te stellen.

7. Stappenoverzicht voor gemeenten

Gemeenten moeten een groot aantal stappen nemen om aan de privacywetgeving te voldoen. Deze rapportage beschrijft de stappen en acties hieronder grotendeels. In dit hoofdstuk worden de stappen die in elk geval nodig zijn nog eens kort opgesomd. Het betreft geen limitatieve opsomming maar een geheugensteuntje:

- Breng de gegevensverwerking die nodig is voor alle wettelijke taken in kaart;
- Bepaal wie bepaalde taken of onderdelen zal uitvoeren;
- Maak een gegevensverwerkingsmodel per deelverwerking of taak, waarmee de betrokken actoren en gegevensstromen in kaart worden gebracht; onderscheidt in het model ook de informatiesystemen en de uitwisseling die tussen systemen plaatsvindt;
- Bepaal voor elke gegevensverwerking of logisch onderdeel daarvan wie de verantwoordelijke in de zin van de Wbp is voor de gegevensverwerking;
- Stel vast (als verantwoordelijke) wat het doeleinde van een bepaalde gegevensverwerking is en de juridische grondslag;
- Bepaal of voor bepaalde gegevensverwerking extra regels van toepassing zijn, zoals een wettelijke geheimhoudingsplicht of dossierverplichting (WGBO, Jeugdwet). Denk ook in speciale gevallen aan de Wet Politiegegevens. (De gemeent zelf heeft daar als verantwoordelijke niet mee te maken, maar een ketenpartner kan er wel mee te maken hebben).
- Zorg voor de goede handhaving van de geheimhoudingsplicht in de organisatie, de processen en informatievoorziening moeten dit ondersteunen;
- Bepaal welke informatievoorzieningen (informatiesystemen) worden gebruikt voor de gegevensverwerkingen;
- Stel vast wat de noodzakelijke gegevens zijn voor een bepaalde gegevensverwerking;
- Stel de bewaartermijnen vast van de onderscheiden gegevensverwerkingen;
- Richt heldere werkprocessen in en maakt gedragsregels voor medewerkers; geef training aan de medewerkers;
- Zorg voor een helpdesk voor medewerkers en betrokken professionals;
- Stel en privacyofficer aan of beleg het privacybeleid bij een ander in de organisatie;
- Stel en privacybeleid vast, waarbij verantwoordelijkheden in de organisatie goed belegd worden voor goede beheersbaarheid en accountability;
- Stel een informatiebeveiligingsbeleid vast, waarin risicoanalyse en privacy impact analyse een plaats heeft;
- Stel een informatiebeveiligingsplan vast waarin autorisatie, authenticatie en logging geregeld is;
- Richt een PDCA-cyclus voor het privacybeleid en de informatiebeveiliging in de organisatie in;
- Richt toezicht in op de gegevensverwerking door de verantwoordelijke; Onderdeel van het toezicht zijn interne audits en audits door geaccrediteerde specialisten; De

verantwoordelijk houdt ook toezicht op de naleving van afspraken door de bewerkers;

- Zorg voor de juridische borging van de samenwerking met alle ketenpartners en bovenregionale samenwerkingspartners; denk aan convenanten en samenwerkingsovereenkomsten; denk aan machtiging;
- Zorg voor de juridische borging van medewerkers, denk aan geheimhoudingsverplichtingen;
- Zorg voor het creëren van de juiste omstandigheden voor het zorgvuldig kunnen verlenen van mandaat indien gewenst;
- Zorg voor het juiste mandaatbesluit;
- Leg de noodzakelijke zaken vast in de Verordening van de gemeente;
- Zorg dat een ICT dienstverlener aantoonbaar maakt dat hij voldoet aan de eisen van gegevenbeveiliging die passen bij het risico van de verwerking; het risico van de verwerking van gezondheidsgegevens is hoog; kies een dienstverlener met aantoonbare ervaring op dit gebied;
- Zorg voor de juridische borging en garanties bij inschakelen van een dienstverlener die optreedt als bewerker (zoals een ICT dienstverlener); stel een degelijke bewerkersovereenkomst op met deze partij waarin de zeggenschap over de gegevens te allen tijde reëel is voor de verantwoordelijke;
- Richt een adequate procedure in voor de uitoefening van de rechten door betrokkenen;
- Zorg voor een goede klachten- en bezwaarprocedure;
- Zorg voor transparantie naar de burger over de inrichting en organisatie van de jeugdhulp door de gemeente; zorg voor goede informatie, voorlichtingsbijeenkomsten en een helpdesk (virtueel of live);
- Zorg voor inspraakavonden voor burgers en betrokkenen conform de Algemene wet bestuursrecht.