Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding

Aandachtspunten, risico's en suggesties voor gegevensverwerking bij de uitvoering van de gemeentelijke taken en werkzaamheden in een gedecentraliseerd sociaal domein

---

INHOUDSOPGAVE

INLEIDING 5

DEEL I ONDERWERP, ACHTERGROND EN AANDACHTSPUNTEN EN RISICO'S 6

1 Onderwerp van de rapportage 6
1.1 Gegevensverwerking voor de gemeentelijke taken en werkzaamheden in een gedecentraliseerd sociaal domein 6
1.2 Typen problematiek, organisatie van de dienstverlening en inrichting van de informatiehuishouding 8
1.2.1 Typen problematiek in het sociaal domein en organisatie van de dienstverlening 8
1.2.2 Inrichting van de informatiehuishouding en de onderwerpen van de rapportage 9
1.3 Nadruk op de transitiefase 10

2 Aandachtspunten en risico's 10
2.1 Risico's in verband met de persoonlijke levenssfeer en het grondrecht 10
2.2 Risico's in verband met regelgeving over het verwerken van persoonsgegevens 12

DEEL II – KEUZEN IN DE PRAKTIJK 14

3. Organisatie van de dienstverlening en uitbesteding 14
3.1 Zelf doen, uitbesteden, samenwerken 15
3.2 Horizontale integratie van taken 18
3.2.1 Archetype transitieproof 18
3.2.2 Archetypen met verschillende maten van integraliteit 19
3.3 Verticale integratie van taken 20
3.3.1 Minimale verticale integratie van taken 20
3.3.2 Verticale integratie van intake, onderzoek en besluitvorming 21
3.3.3 'Maximale' integratie van taken 21

4. Werkprocessen en triage 22
4.1 Omgang met gegevens bij triage 22
4.1.1 Impliciete en expliciete triage 23
4.1.2 Omgang met persoonsgegevens: De burger aan het stuur versus de gemeente aan het stuur 24
4.1.3 Escalatie 25
4.2 Signalering: Meldingen door derden 26
4.3 Casusoverleg 27
4.4 De omgang met toestemming 28
4.5 Gegevensuitwisseling tussen gemeente en hulpverleners in de uitvoeringsfase en bij financiële verantwoording 29
4.5.1 Gegevensuitwisseling tussen de gemeente en de hulpverlener of maatwerkaanbieder ten behoeve van de opdrachtverstrekking en declaratie van te verlenen van zorg of een maatwerkvoorziening 29
4.5.2 De gegevensverwerking ten behoeve van de regie op zorg bij een integrale aanpak 30
4.5.3 Gegevensverwerking in het kader van de Jeugdwet in de situatie waarbij een jeugdhulpaanbieder hulp verleend op basis van een verwijzing door anderen dan de gemeente, waarvoor de gemeente financieel verantwoordelijk is 31

5 Inrichting van informatiesystemen, registratie, toegang, bewaren en vernietigen van gegevens 31
5.1 De mate van integratie en scheiding van dossiers 31

5.1.1	Volledig gescheiden domeindossiers	32
5.1.2	Koppelbare domeindossiers	32
5.1.3	Volledig geïntegreerde dossiers / gezinsdossiers	33
5.2	De mate van integratie en scheiding in informatieniveaus	33
5.2.1	Scheiding van wat en dat informatie	34
5.2.2	Scheiding van informatieniveaus voor de verschillende fasen van het werkproces	34
5.3	De wijze waarop de toegang tot persoonsgegevens is georganiseerd	35
5.3.1	Autorisatie op basis van functie	35
5.3.2	Autorisatie op teamniveau	35
5.3.3	Autorisatie op basis van betrokkenheid	36
5.4	Bewaren en vernietigen van persoonsgegevens	36
6.	Transparantie en positie van de burger	37
6.1	De positie van de burger tijdens het dienstverleningsproces	37
6.2	Informatie aan de burger met betrekking tot rechten en plichten	37
7.	Kennis en bewustwording van medewerkers	38
8.	Beleid voor Privacy en verwerking van persoonsgegevens in het Sociaal domein	39

INLEIDING

De gemeenten krijgen er in het kader van de decentralisaties taken bij in het sociaal domein. De decentralisaties en de beoogde integrale werkwijze van gemeenten brengt met zich mee dat gemeenten, meer dan voorheen, persoonsgegevens van burgers zullen verwerken. Dit heeft bij zowel gemeenten als bij het Rijk, in de politiek en bij het CBP geleid tot extra aandacht voor het aspect van bescherming van de privacy van de burger en de verwerking van persoonsgegevens in het sociaal domen. Bij brief 10 februari 2014 33750-VII-45 is toegezegd dat er een Priavcy Impact Assessment gedaan zou worden wanneer zich binnen de gemeentelijke praktijk een beperkt aantal modellen uitgekristalliseerd zou hebben volgens welke gemeenten hun nieuwe taken vorm gaan geven. In de begeleidende brief van 27 mei 2014 [TK 32 761, nr. 62] bij de kabinetsvisie 'Zorgvuldig en bewust; gegevensverwerking en privacy in een gedecentraliseerd sociaal domein' kondigt het kabinet aan dat er een PIA gedaan zal worden op de archetypen zoals die door VNG/KING beschreven zijn.

Deze rapportage bevat de resultaten van de genoemde Privacy Impact Assessment voor dienstverlening door gemeenten in verband met de transitie in het sociaal domein. In deel I wordt nader ingegaan op het onderwerp en de achtergrond van deze rapportage en de risico's die bij het verwerken van persoonsgegevens kunnen spelen in algemene zin. In deel II worden de keuzes beschreven die gemaakt kunnen worden bij de uitvoering van de gemeentelijke taken en werkzaamheden in een gedecentraliseerd sociaal domein en de privacyrisico's die daarbij optreden en aanbevelingen voor de toepassing van het juridisch kader in de praktijk om deze risico's te voorkomen.

Alhoewel in deze rapportage informatieverwerking en de privacyaspecten daarbij centraal staan, moet benadrukt worden dat het bij de dienstverlening door gemeenten in het sociaal domein niet zozeer gaat om processen, verwerking en registratie van gegevens. Het gaat uiteindelijk om een goede dienstverlening waarbij kwetsbare burgers niet uit het ook verloren worden, burgers de ruimte krijgen om de eigen regie die ze kunnen voeren ook daadwerkelijk te voeren, en dat burgers de ondersteuning ontvangen die voor hen nodig is. Het zijn dan ook de burger, diens hulpvraag, diens eigen regie en de daarbij passende dienstverlening die steeds centraal dienen te staan bij de afweging welke persoonsgegevens in een bepaald geval wel of niet verwerkt dienen te worden. Daarbij is vertrouwen nodig in het vermogen van professionals en ambtenaren om precies die gegevens te verwerken en te gebruiken die noodzakelijk zijn. Uiteraard is het centraal stellen van de hulpvraag en de daarbij passende dienstverlening géén excuus om privacybescherming en de regelgeving over het verwerken van persoonsgegevens terzijde te stellen of te veronachtzamen. Maar onnodig wantrouwen vooraf, of een situatie waarin door een sterke en wellicht soms wat eenzijdige nadruk op regels over gegevensverwerking de uitvoerders in de praktijk onzeker en wellicht zelf kopschuw worden, draagt ook niet bij aan een goede dienstverlening waarbij burgers de ondersteuning ontvangen die nodig is.

De centrale positie van de hulpvraag van de burger en de mate waarin de burger zelf wel of geen regie kan voeren, hebben bijvoorbeeld tot gevolg dat in acute noodsituaties of bij complexe multiproblematiek meer gegevens verwerkt en uitgewisseld moeten en mogen worden dan bij een enkelvoudige hulpvraag van een burger die zelf de regie voert. Dit uitgangspunt heeft echter ook tot gevolg dat een uniforme werkwijze bij het (breed) verzamelen van gegevens voor alle hulpvragen niet passend is. De centrale positie van de hulpvraag en de regie van de burger houdt eveneens in dat de mate waarin de burger zelf als bron voor de benodigde informatie kan fungeren per situatie verschilt. Het is wellicht verleidelijk om in alle gevallen de gegevens die reeds bij de gemeente aanwezig zijn zelf te verzamelen of bij andere partijen op te vragen, maar men kan zich afvragen hoe een dergelijke "zelfstandige verzamelstrategie" zich verhoudt tot een zorgvuldige omgang met de burger als deze zeer goed in staat is om zelf regie te voeren. Dit dan nog los van de vraag of en in welke mate een dergelijk verzamelen juridisch toegestaan zou kunnen zijn. Ook bij het zelfstandig verzamelen van gegevens gaat het niet om wat juridisch bezien wellicht maximaal mogelijk is of in bijvoorbeeld een convenant afgesproken wordt, maar gaat het uiteindelijk om een handelwijze die past bij de hulpvraag in een bepaalde situatie.

Daar waar binnen het sociaal domein het streven is om bij de dienstverlening en de bejegening van de burger een overgang, een transitie, te maken van ‘zorgen voor’ naar ‘zorgen dat’, past ook een dergelijke overgang bij het verzamelen en verwerken van gegevens over de burger. Anders gezegd: ook bij de gegevensverwerking in het sociaal domein dient het uitgangspunt te zijn dat de dienstverleners niet altijd meer zelf ‘zorgen voor’ alle benodigde gegevens, maar dat men in samenspraak met de burger ‘zorgt dat’ de benodigde gegevens verwerkt worden. Uiteraard zal er een verschil zijn tussen enerzijds situaties waarin de burger en de dienstverleners het volledig eens zijn over de aanpak van de hulpvraag en anderzijds situaties waarbij er duidelijk sprake is van een gedwongen kader, maar het is en blijft van belang in het oog te houden dat er verschillen zijn.

Gemeenten worstelen met de regels over het verwerken van persoonsgegevens die deels zijn vastgelegd in de Wbp en deels in verschillende materiewetten. Een algemene observatie is dat mede daardoor de juridische inbedding van gemeentelijke taken en werkzaamheden en de daarbij behorende gegevensverwerking nog niet altijd volledig is uitgewerkt en geëxpliciteerd. Een andere algemene observatie is dat bij de interpretatie en toepassing van de regels over het verwerken van persoonsgegevens misverstanden bestaan, waardoor - wellicht eerder onbedoeld dan bedoeld – werkwijzen kunnen ontstaan die zich soms niet of nauwelijks verhouden met de toepasselijke regelgeving. Dit speelt bijvoorbeeld bij de interpretatie en toepassing van de diverse juridisch verschillende vormen van toestemming van de burger. Om die reden gaat deel II niet in op het juridisch kader en de wettelijke regels maar op de mogelijkheden om door toepassing van het juridisch kader in de praktijk de privacy van burgers te waarborgen Het juridisch kader voor de gegevensverwerking in het sociaal domein is reeds uitgebreid beschreven in de kabinetsvisie ‘Zorgvuldig en bewust’.

DEEL I ONDERWERP, ACHTERGROND EN AANDACHTSPUNTEN EN RISICO'S

1 Onderwerp van de rapportage

1.1 Gegevensverwerking voor de gemeentelijke taken en werkzaamheden in een gedecentraliseerd sociaal domein

> Bij de decentralisaties in het sociaal domein die op dit moment worden voorbereid, krijgen gemeenten omvangrijke nieuwe taken en een nieuwe rol. Gemeenten worden eerst verantwoordelijke voor taken met betrekking tot jeugdzorg, participatie en maatschappelijke ondersteuning. Zij worden geacht daarbij regie te voeren. Integraliteit vormt hierbij in de visie van het kabinet een cruciaal aspect. Beleidsmatig uit zich dit onder andere in het adagium 'één gezin, één plan, één regisseur'.
>
> De decentralisaties in het sociale domein brengen met zich mee dat gemeenten meer taken krijgen waarbij zij ook, meer dan voorheen, persoonsgegevens van burgers zullen verwerken. De integraliteit impliceert daarbij dat gemeenten 'ontschot' moeten kijken, over de grenzen van sectoren in het sociaal domein heen en dus ook persoonsgegevens uit verschillende sectoren bij elkaar moeten kunnen brengen als de situatie dat vraagt. Doel daarvan is om burgers die dat nodig hebben, ondersteuning op maat te bieden met het oog op hun zelfredzaamheid en participatie in de samenleving. Deze 'ontschotte' manier van werken is een logisch en noodzakelijk gevolg van de kabinetsdoelstellingen. Maar het is ook een gevolg dat vragen oproept over de wijze waarop gemeenten om zullen gaan met de noodzakelijke gegevensverwerking en de bescherming van de privacy.

Bron: Kabinetsvisie 'Zorgvuldige en bewust; gegevensverwerking en privacy in een gedecentraliseerd sociaal domein.

In deze rapportage staat centraal op welke wijze gemeenten in de uitvoeringspraktijk vorm (kunnen) geven aan de noodzakelijke gegevensverwerking en hoe daarbij tegelijkertijd de bescherming van de privacy kan worden geborgd en recht gedaan kan worden aan de diverse regels over het verwerken van persoonsgegevens. Het gaat daarbij om de uitvoering van de verschillende taken en werkzaamheden die in de diverse wetten, zoals bijvoorbeeld de Jeugdwet, de Wmo en de Participatiewet, toebedeeld zijn aan de gemeenten. In juridische zin gaat het daarbij overigens om toedeling aan het college van B&W. In deze rapportage wordt, in navolging van het spraakgebruik, gesproken over de gemeente.

Het onderwerp van deze rapportage is daarmee de inrichting van de informatiehuishouding die gebruikt wordt voor de uitvoering van de gemeentelijke taken. Meer concreet: de bij die informatiehuishouding in verband met privacy en gegevensverwerking spelende aandachtspunten, risico's en aanbevelingen zijn het onderwerp van deze rapportage. Dit betekent echter niet dat de rapportage beperkt is tot gegevensverwerking die (enkel) door gemeenten c.q. enkel door gemeenteambtenaren uitgevoerd wordt. Als een gemeente bepaalde gemeentelijke taken uitbesteedt, behoort ook de daarbij behorende gegevensverwerking nadrukkelijk tot de scope van de rapportage. De nadruk op de gegevensverwerking voor de uitvoering van de gemeentelijke taken en werkzaamheden heeft wel tot gevolg dat gegevensverwerking bij bijvoorbeeld de aanbieders van maatwerkvoorzieningen, de aanbieders van collectieve voorzieningen, jeugdhulpaanbieders, gecertificeerde instelling of het UWV, slechts zijdelings aan bod komen als dit direct van belang is voor de gegevensverwerking ter uitvoering van de gemeentelijke taken. Ook heeft de gekozen scope tot gevolg dat gegevensverwerking die weliswaar uitgevoerd wordt door een gemeente maar die niet voortvloeit uit de (specifieke) gemeentelijke taken en werkzaamheden, eveneens slechts zijdelings aan bod komt. Een voorbeeld hiervan is de gegevensverwerking die plaats zou vinden als een gemeente een eigen gemeentelijke afdeling zou belasten met de uitvoering van jeugdhulp of als een gemeentelijke afdeling zelf daadwerkelijk Wmo-maatwerkvoorzieningen aan zou bieden.

Uitgaande van de dagelijkse praktijk zoals die zich nu ontwikkelt, worden in deze rapportage een aantal fasen onderscheiden bij de gemeentelijke taken en werkzaamheden in het sociaal domein. Daarbij sluiten we aan bij de fasering zoals deze beschreven is in het 'Programma van eisen ten aanzien van de informatievoorziening – Applicatie architectuur' van 26 juni 2014 van het programma VISD.

De werkzaamheden en fasen zijn:

Klantcontact en intake: Het doel van deze fase is om te komen tot een eerste inschatting van een vraag van een burger of van een signaal dat wordt afgegeven door een professional of iemand uit de omgeving van een burger. Daarbij staat de vraag voorop: gaat het om een informatieve, eenvoudige, enkelvoudige vraag, of om een potentieel meervoudige of zelfs complexe vraag. Op basis daarvan bepaalt een medewerker waar de beantwoording van de vraag thuis hoort.

Behoeftenbepaling en planvorming: Het doel van deze fase is het verhelderen van de klantvraag, het in kaart brengen van de behoeften van de burger of het gezin en te bepalen of, en zo ja, welke ondersteuning noodzakelijk is. Deze fase eindigt met een advies aan betrokkene of een ondersteuningsplan, en indien nodig en aanvraag voor maatwerkvoorzieningen. Onderdeel van deze fase kan zijn een casusoverleg waarbij ook andere expertises en mantelzorgers betrokken worden.

Besluitvorming: In deze fase gaat het om het (formeel) beoordelen van de aanvraag en het nemen van een besluit over een voorziening voor de burger. In de regel wordt het besluit genomen door de gemeente. Bij de jeugdhulp kan dit ook gebeuren door derden.

Uitvoering en levering: hierbij gaat het om het leveren van de toegewezen hulp of voorziening en de uitvoering van de hulp door bijvoorbeeld aanbieders van maatwerkvoorzieningen en jeugdhulpaanbieders, het verstrekken van een persoonsgebonden budget (pgb) of het uitvoeren van de gemeentelijke schuldsanering.

Regievoering: De fase van regievoering heeft betrekking op het voeren van regie door de gemeente of een daartoe door de gemeente ingeschakelde instelling op de uitvoering van de toegekende voorziening of hulp en de uitvoering van bijvoorbeeld het ondersteuningsplan. Deze fase loopt paralel aan de fase van uitvoering en levering.

Naast deze werkzaamheden en fasen die meer gericht zijn op de inhoudelijke ondersteuning en het bieden van hulp of voorzieningen aan de burger, worden een tweetal meer ondersteunende processen onderscheiden. Dit zijn:

De financiële afwikkeling van de uitvoering: Hierbij gaat het bijvoorbeeld om de betaling van de facturen van maatwerkaanbieders en jeugdhulpverleners, de financiering van gecertificeerde instellingen en de daadwerkelijke uitkering van een pgb.

Managementinformatie, inkoopinformatie en planning: Hierbij gaat het om het gebruik van gemeentelijke gegevens voor bijvoorbeeld inkoop (hoeveel hulp dient voor de komende jaren ingekocht te worden?), managementrapportages (worden de doelstellingen zoals bijvoorbeeld vermindering van zwaardere vormen van hulp bereikt?) en planning (wat is een juiste omvang van het wijkteam in een bepaalde wijk gelet op de hulpvragen in die wijk?).

Het belang van goede managementinformatie, inkoopinformatie en planning komt bijvoorbeeld nadrukkelijk aan de orde in de Rekenkamerrapporten van de G4 [Decentralisatie Jeugdzorg van de Rekenkamer Den Haag van september 2014, Jeugdhulp in ontwikkeling van de Rekenkamer Utrecht van 23 september 2014, Transformatie zorg voor de jeugd van de Rekenkamer Amsterdam van september 2014, zorg om de jeugd van

de Rekenkamer Rotterdam van september 2014] over de voorbereidingen bij de transitie naar de nieuwe jeugdhulp.

1.2 Typen problematiek, organisatie van de dienstverlening en inrichting van de informatiehuishouding

1.2.1 Typen problematiek in het sociaal domein en organisatie van de dienstverlening

In de rapportage van de Verkenning Informatievoorziening Sociaal Domein worden verschillende typen problematiek beschreven. Kortgezegd gaat het om de volgende typen problematiek:

- Burgers die soms een beroep doen op een lichte vorm van ondersteuning of advies via een laagdrempelige collectieve voorziening zoals een consultatiebureau of een buurtcentrum of. Deze ondersteuning is vooral gericht op preventie en (versterking van) de zelfredzaamheid.
- Burgers die enige vorm van individuele ondersteuning nodig hebben zoals een WWB-uitkering of een thuiszorgvoorziening, maar over het algemeen uitstekend in staat zijn om zelf de regie te voeren.
- Burgers die kampen met meervoudige complexe problematiek.

Het is vanzelfsprekend dat gemeenten bij de organisatie van de dienstverlening rekening houden met deze verschillende typen hulpvragen. Als de organisatorische vormgeving hoofdzakelijk ingericht is op enkelvoudige hulpvragen waarbij burgers ondersteuning nodig hebben binnen een bepaald deeldomein, zal er (in extreme vorm) sprake zijn van meerdere gescheiden loketten voor de burger en afzonderlijke afdelingen waarbinnen de dienstverlening plaats vindt. Bij een organisatorische inrichting die juist gericht is op complexe hulpvragen en multiprobleem gezinnen zal er (in extreme vorm) sprake zijn van slechts 1 loket en 1 afdeling voor het gehele sociaal domein. In de praktijk zijn er vele verschillende tussenvormen. De diverse keuzen die gemeenten bij de organisatorische inrichting van het sociaal domein kunnen maken komen tot uitdrukking in de archetypen zoals deze beschreven zijn in “Archetypen in het sociaal domein” van VNG/KING van juni 2014. De archetypen die beschreven worden zijn:

Archetype 1: Transitie-proof
Archetype 2: Totaal integraal
Archetype 3: Geclusterd integraal
Arcetype 4: Integraal in 2e instantie
Arcehtype 5: Geclusterde integraliteit elders

type	doel	wat	waarom
1 transformatie-proof	Borgen van continuïteit van (tijdelijke) ondersteuning op huidig kwaliteitsniveau, en minimalisering van niet financiële uitvoeringsrisico’s	• De kolommen blijven naast elkaar bestaan • De ambitie 1 gezin, 1 plan, 1 regisseur wordt voorlopig niet ingevuld	• Geen financiële zekerheid • Onvoldoende kennis over nieuwe doelgroepen • ‘kaders’nog onvoldoende duidelijk • Keuze om even te wachten tot er meer duidelijkheid is
2 totaal integraal	• Bieden van de beste oplossing voor het gezin tegen de laagste maatschappelijke kosten. • Met inachtneming van de houdbaarheid van het stelsel van regelingen in het sociaal domein	• Vanaf het eerste contact integrale beoordeling • Grote preventieve en vroegsignalerende werking (erger voorkomen) • Eerder terug naar de)e lijn (eigen kracht) • 1 toegang tot het totale sociale domein creëren (kan dmv wijkteam, maar ook op centraal of ander niveau)	• Omdat je overtuigd bent dat je met vroegtijdige signalering en vroegtijdig (preventief) ingrijpen erger kunt voorkomen • Omdat je overtuigd bent dat ieder huishouden uniek is en niet te categoriseren is
3 geclusterd integraal	• De beste oplossing voor het gezin • Tegen de laagste maatschappelijke kosten • Met inachtneming van de	• Geclusterde toegang, bijvoorbeeld 1 voor zorg en jeugdzorg en 1 voor fiancniële en inkomensondersteuning (incl. SDV	• De tijdelijke ondersteuningsbehoefte van huishoudens blijkt zich vooral binnen een bepaald cluster te

	houdbaarheid van het stelsel van regelingen in het sociaal domein	en minima) • NB er zijn vele vormen van clustering mogelijk	bevinden • De werkwijze, behoefte aan (tijdelijke) ondersteuning wordt specifiek geacht voor een bepaald cluster
4 integraal in 2e instantie	• De beste oplossing voor het gezin • Tegen de laagste maatschappelijke kosten • Met inachtneming van de houdbaarheid van het stelsel van regelingen in het sociaal domein	• De toegang (1e instantie) blijft per kolom, daar wordt naar de tijdelijke ondersteuningsvraag gekeken, • Wanneer in de kolom blijkt dat er veel meer aan de hand is wordt een gezin/ huishouden doorgezonden naar een integraal team (2e instantie) • Er wordt vanuit gegaan dat het gezin/ de burger zelf en/ of de betrokken specialisten de benodigde input (informatie) over een gezin aanlevert.	• Het gros van de burgers met een (tijdelijke) ondersteuningsvraag komt met een enkel- en/ of eenvoudige vraag, of is grotendeels zelfredzaam • Het loont, financieel om dmv standaardisatie een efficiencyslag (standaardisatie in 1e instantie) te maken.
5 geclusterde integraliteit elders	• De beste oplossing voor het gezin • Tegen de laagste maatschappelijke kosten • In ogenschouw houdend de houdbaarheid van je sociale stelsel	• Geclusterde toegang, bijv. 1 voor zorg, 1 voor jeugdzorg en 1 voor finanicële en inkomensondersteuning • Kenmerkend is dat toegang bij een **derde** partij is ondergebracht: bijvoorbeeld zorg bij de zorgverzekeraar en bijvoorbeeld jeugdzorg bij een regionale eenheid buiten de deur	• De (tijdelijke) ondersteuningsbehoefte van huishoudens blijkt zich vooral binnen een bepaald cluster te bevinden. • De werkwijze, behoefte aan ondersteuning, wort specifiek geacht voor een cluster • Daarnaast wordt in dit type de integraliteit het grootst geacht wanneer de taak, omwille van elders te bieden integraliteit op zorg, elders wordt ondergebracht.

De archetypen zijn modellen, en dus vereenvoudigde weergaven van de praktijk. KING heeft de archetypen in de eerste plaats ontwikkeld vanuit informatiekundig perspectief, als hulp, ter ordening en prioriteitstelling.

1.2.2 Inrichting van de informatiehuishouding en de onderwerpen van de rapportage

In deze rapportage staat voorop dat de manier waarop gemeenten vorm en inhoud gaan geven aan hun dienstverlening in het sociaal domein in hoge mate lokaal wordt bepaald. Lokale voorkeuren zullen leiden tot variatie in beleid en daarmee tot uitvoeringsverschillen tussen gemeenten. Dat is een logisch gevolg van het decentraal beleggen van taken bij autonome gemeenten.

Om inhoud te kunnen geven aan een PIA over de archetypen hebben daarom bijeenkomsten plaats gevonden met gemeenten die grofweg volgens een van deze modellen (gaan) werken. Samen met deze gemeenten zijn de organisatie van taken, werkprocessen en inrichting van systemen doorgenomen en is gekeken naar de afwegingen die daarin mogelijk zijn ten aanzien van gegevensverwerking en de mogelijke impact daarvan op de privacy van burgers. Deze hebben de input gevormd voor deel II van deze rapportage.

Bij de voorbereiding van deze PIA is gebleken dat gemeenten gaandeweg het proces van inrichting van de organisatie en werkwijze hun keuzes bijstellen ook ten aanzien van de omgang met gegevens. De verwachting is dat gemeenten hun organisatie en werkwijze ook na 1-1-2015 zullen blijven bijstellen, mede op basis van rapportages als deze PIA.

Op basis van de archetypen en bijeenkomsten met gemeenten zijn zes meer algemene onderwerpen geïdentificeerd waarop gemeenten keuzes kunnen maken die consequenties hebben voor privacy. Deze onderwerpen, men zou ook van componenten kunnen spreken,spelen bij alle archetypen in meerdere of mindere mate een rol. of minder mate spelen bij de diverse archetypen. Die onderwerpen zijn:

- Organisatie van de dienstverlening en uitbesteding (onderdeel 3)
- Werkprocessen en triage (onderdeel 4)
- ICT, registratie, toegang, bewaren en vernietigen (onderdeel 5)

- Transparantie en positie van de burger (onderdeel 6)
- Kennis en bewustwording medewerkers (onderdeel 7)
- Beleid (onderdeel 8)

Deze onderwerpen sluiten onder andere aan bij de *Factsheet Privacy* en de *Privacy Scan VISD* van KING. Zie hiervoor https://www.visd.nl/visd/gegevensuitwisseling-en-privacybescherming

1.3 Nadruk op de transitiefase

Bij de decentralisaties is er zowel sprake van transitie als transformatie. De transitie betreft de overgang van taken naar de gemeenten. De transformatie ziet op een nieuwe werkwijze binnen het sociaal domein met onder andere regie voor de burger, meer preventie, de inzet van wijkteams en een omslag van 'zorgen voor' naar 'zorgen dat'.

Deze rapportage is gebaseerd op informatie en bevindingen uit de periode waarin de gemeentelijke informatiehuishouding voor het sociaal domein nog volop in ontwikkeling is, en waarbij een deel van de gemeentelijke taken nog niet uitgevoerd wordt. De nadruk in deze rapportage ligt dan ook op de (komende) transitie. Dit betekent dat de rapportage betrekking heeft op de keuzen die gemeenten kunnen maken bij de verwerking van persoonsgegevens. Soms is al uitgekristalliseerd hoe bepaalde processen vorm gegeven worden en welke gegevensverwerking daarbij plaats zal vinden. In andere gevallen, bijvoorbeeld ten aanzien van vroegsignalering of de financiële administratie, is nog onduidelijk hoe de processen en gegevensverwerkingen plaats zullen vinden. Die plannen zijn nog in ontwikkeling. Het is dan ook van belang om in het achterhoofd te houden dat bepaalde beschreven risico's of problemen ten aanzien van het verwerken van persoonsgegevens theoretisch zijn. Of deze risico's zullen spelen wordt mede bepaald door de mate waarin gemeenten de in deze rapportage aan de risico's gekoppelde aanbevelingen invulling geven. Ook zal er sprake zijn van een lerende praktijk zoals geschetst is in onderdeel 3.3 van de visie 'Zorgvuldig en bewust; gegevensverwerking en privacy in een gedecentraliseerd sociaal domein'. Dat wil zeggen dat gemeenten gaandeweg op basis van de ervaringen hun organisatie en processen bij zullen stellen, ook ten aanzien van de verwerking van persoonsgegevens.

Zoals het College bescherming persoonsgegevens in de brief van 3 juni 2014 over *Zorgvuldige gegevensuitwisseling over sectoren heen ik het kader van decentralisaties in het sociaal domein* (kenmerk Z2014-00393) ook aangeeft, geeft deze lerende praktijk uiteraard geen excuus om de bestaande regelgeving niet te volgen of daar "al lerende van af te wijken".

2 Aandachtspunten en risico's

Een PIA legt de risico's bloot van projecten die te maken hebben met privacy, en draagt bij aan het vermijden of verminderen van deze privacy risico's. De PIA doet dit - in beginsel - door op gestructureerde wijze door de mogelijke (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen en de risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren. Dit, zo mogelijk, aangevuld met aanbevelingen gericht op het verminderen van risico's.

Niet alle risico's zijn hetzelfde. Hieronder gaan wij kort in op een typering van risico's die wij hanteren in deze rapportage.

2.1 Risico's in verband met de persoonlijke levenssfeer en het grondrecht

Op basis van de uitvoering van de PIA en ook wel op basis van de diverse privacy-discussies, kan de observatie gemaakt worden dat de privacy-discussie soms beperkt lijkt te blijven tot de aspecten die direct verbonden zijn aan het verwerken van persoonsgegevens. Hierdoor kunnen de meer algemene privacy en het grondrecht op bescherming van de gehele persoonlijke levenssfeer buiten beeld raken. Het privacy-onderwerp blijft dan beperkt tot enkel de juridische aspecten van gegevensverwerking.
Het verengen van de privacy-discussie tot een persoonsgegevens-discussie, draagt daarbij het risico in zich dat de mate waarin het noodzakelijk is om in een bepaald geval persoonsgegevens te verwerken, als het ware los komt te staan van de vraag naar de mate waarin de overheid gerechtigd is zich met het dagelijks doen en laten van de burger te bemoeien.

Bij het grondrecht op bescherming van de persoonlijke levenssfeer gaat het niet enkel om gegevensverwerking en de aantasting daardoor, maar gaat het ook om de vraag of en in welke mate bijvoorbeeld het gezinsleven geraakt wordt en of en in welke mate het door burgers gepercipieerde huisrecht aangetast wordt. Hierbij gaat het over de vraag of het grondrecht op bescherming van de persoonlijke levenssfeer, zoals o.a. vastgelegd in artikel 8 EVRM, aangetast wordt door de wijze waarop de dienstverlening plaatsvindt. Dit dan nog los van de vraag of en hoe persoonsgegevens verwerkt worden.

In een uitspraak van de rechtbank Oost-Brabant over het uitgangspunt van het grondrecht van art. 8 EVRM stelt de rechter daarover “Dit uitgangspunt in de relatie tussen burger en overheid is niet het veelgehoorde "wie niets te verbergen heeft, heeft ook niets te vrezen" maar "het dagelijks doen en laten van de burgers gaat de overheid niets aan". Vervolgens zijn het dan de in het tweede lid van art. 8 EVRM geregelde mogelijkheden voor het maken van een inbreuk, die aangeven wanneer de overheid wel gerechtigd is zich met het dagelijks doen en laten van de burger te bemoeien.

[zie de overwegingen 4.11 en 4.15 in een zaak over SMS-parking (ECLI:NL:RBOBR:2013:6553) en overweging 4.15. Het feit dat de feitelijke uitspraak door de Rb in deze zaak in een later hoger beroep (ECLI:GHSHE:2014:2803) niet overeind beleef, doet aan deze schets van het uitgangspunt van het grondrecht niet af.]

Het uitgaan van en het bevorderen van de "eigen regie" en "eigen kracht" van en voor de burger is ook van belang bij de bescherming van de persoonlijke levenssfeer en de mate van inbreuk (het bemoeien met het dagelijks doen en laten van de burger). Immers: daar waar burgers zelf regie kunnen voeren, behoeft de overheid zich (ook) niet of slechts minder te bemoeien met het dagelijks doen en laten van die burger. In die zin kan, wellicht enigszins onverwacht, opgemerkt worden dat de uitgangspunten van 'eigen regie' en 'eigen kracht' ook bij kunnen dragen aan een opstelling en optreden door de overheid waarbij inbreuken op de persoonlijke levenssfeer en directe bemoeienis met de dagelijkse gang van zaken daar waar mogelijk is juist beperkt worden.

De algemene inbreuk op de persoonlijke levenssfeer bij de wijze waarop de dienstverlening plaatsvindt, komt bijvoorbeeld ook tot uitdrukking bij de vraag of de burger instemt met de aanpak en dienstverlening of dat er in meer of mindere mate sprake is van drang of van een gedwongen kader. In een concreet geval kan dit ook spelen bij de vraag of en in welke mate een burger bijvoorbeeld een "keukentafel gesprek" als een wel of niet aanvaardbare inbreuk op zijn of haar dagelijkse doen en laten beschouwt.

Mede op basis van bovenstaande is duidelijk dat de overheid zich rekenschap moet geven van de noodzaak tot bemoeienis. Dit betekent dat doel en noodzaak tot verwerking van persoonsgegevens veeleer gelegen zijn in de specifieke omstandigheden van een concreet geval en niet zozeer in meer algemene doelen zoals de uitvoering van de taken en werkzaamheden binnen het (gehele) sociaal domein.

Dit betekent dat, zoals ook in de kabinetsvisie 'Zorgvuldig en bewust' is aangegeven, de hulpvraag van de burger en de mate waarin de burger zelf wel of geen regie kan voeren, mede bepalend zijn voor de mate waarin persoonsgegevens verwerkt kunnen worden. Bij bijvoorbeeld een enkelvoudige hulpvraag van een regie voerende burger zullen minder gegevens noodzakelijk zijn dan in een acute noodsituaties of bij complexe multi-problematiek.

2.2 Risico's in verband met regelgeving over het verwerken van persoonsgegevens

In algemene zin kan het bij risico's in verband met regelgeving over het verwerken van persoonsgegevens gaan om:

A) Het niet of niet volledig voldoen aan de toepasselijke inhoudelijke regelgeving
B) Het niet of op een onjuiste wijze uitvoeren van de werkzaamheden

A) <u>Het niet of niet volledig voldoen aan de toepasselijke inhoudelijke regelgeving</u>
Bij het niet of niet volledig voldoen aan de toepasselijke inhoudelijke regelgeving zijn er diverse typen risico's die ieder een eigen aanpak vergen. Zo kan het gaan om:

A1) Gegevensverwerking die eenvoudigweg niet toegestaan is. Daarbij zit de aanpak van risico's op het terrein van aanpassing van de wijze waarop werkzaamheden uitgevoerd worden of systemen ingericht worden.

A2) Gegevensverwerking waarbij de regelgeving niet juist wordt toegepast door bijvoorbeeld een onjuiste interpretatie of onduidelijkheid in de regelgeving. Hierbij hoeft de gegevensverwerking niet per se onrechtmatig te zijn omdat mogelijk enkel sprake is van een onjuiste motivering, onderbouwing, van het gebruik van persoonsgegevens. Hierbij zit de aanpak van risico's veeleer in uitleg en bevorderen van de kennis van medewerkers en het, zo nodig, verduidelijken van de regelgeving zelf.

A3) Gegevensverwerking waarbij zogenaamde open en algemene normen toegepast dienen te worden in concrete situaties. Hierbij is er in feite geen onduidelijkheid of misverstand over de inhoud (tekst) van de regelgeving zelf, maar kan de regelgeving slechts invulling krijgen in concrete situaties omdat er bijvoorbeeld sprake is van normen zoals "zorgvuldig", "professioneel", "noodzakelijk", "evenredig" en "verenigbaar". Het zijn in het bijzonder deze risico's bij de toepassing van de open en algemene normen die in bijvoorbeeld de brief van het CBP van 3 juni 2014 (Z2014-00393) over Zorgvuldige gegevensuitwisseling over sectoren heen in het kader van decentralisaties in het sociaal domein aan de orde komen en waar het CBP aangeeft:

> *"..Het CBP stelt vast dat gemeenten bij het treffen van voorbereidingen om de integrale uitvoering van taken in het sociaal domein ter hand te nemen, van meet af aan rekening dienen te houden met de eisen die uit de Wbp voortvloeien ter zake van de verwerking van persoonsgegevens. De verwerking van persoonsgegevens moet proportioneel zijn c.q. niet bovenmatig gelet op gespecificeerde en gerechtvaardigde doeleinden, transparant, controleerbaar en voldoen aan beveiligingseisen. Het daarbij ontbreken van op centraal niveau vastgelegde richtinggevende bepalingen biedt ruimte voor enige variatie in de uitwerkingen die gemeenten (kunnen) gaan geven aan de verwerking van persoonsgegevens bij de uitvoering van de aan hen opgedragen taken in het sociaal domein. Die bandbreedte voor variaties in de uitwerking wordt wel begrensd door de kernbegrippen uit de Wbp. Het CBP wijst er op dat bovenmatige c.q. niet noodzakelijke verwerking van persoonsgegevens in dit verband ook niet gelegitimeerd kan worden door het verkrijgen van toestemming van de betrokkene…."*

Ook de motie Bergkamp en Otwin van Dijk van 5 februari 2014 over privacyaspecten bij de ontwikkeling van sociale wijkteams [TK, 2013-2014, 33 841, nr. 11] legt de nadruk op risico's bij de toepassing van open en algemene normen. Het is juist bij deze risico's dat zelfregulering en 'best practices' invulling kunnen geven aan de open normen van de regelgeving. Ook hierbij is uitleg en bevorderen van de kennis van medewerkers van belang.

B) Het niet of op een onjuiste wijze uitvoeren van de werkzaamheden

Hierbij kan het gaan om het informeren van burgers, het behandelen van klachten of de wijze waarop verzoeken van burgers behandeld worden ten aanzien van gegevensverwerking. Rechten zoals bijvoorbeeld het recht op inzage, kennisneming, correctie of het recht op verwijdering of vernietiging van gegevens. Het kan ook gaan om de implementatie van beveiligingsmaatregelen. Maatregelen om dergelijke risico's te voorkomen kunnen bestaan uit het opstellen van de juiste procedures en het op een juiste wijze toebedelen van taken en werkzaamheden. Ook hierbij kunnen zelfregulering en 'best practices' een nadere invulling geven.

Deel II – Keuzen in de Praktijk

Dit deel beschrijft verschillende manieren waarop gemeenten invulling kunnen geven aan de thema's benoemd in deel I en de privacy-risico's die zich daarbij voor zouden kunnen doen. Bij de verschillende risico's wordt, waar relevant, aangegeven welk type risico het betreft. De verschillende typen risico's zijn beschreven in paragraaf 2,2 van deel I.

De beschreven varianten zijn schetsmatig. Daar waar mogelijk beschrijven we de mogelijke keuzen door een schaal aan te geven waarop gemeenten keuzen kunnen maken. In die gevallen beschrijven we dan de uitersten van de schaal, de middenpositie, en de risico's die bij elke variant behoren. Veel van de risico's die aan de orde komen, zijn relatief eenvoudig te ondervangen, zonder dat de gekozen werkwijze ingrijpend gewijzigd zou dienen te worden. Bij de risico's doen wij een aantal aanbevelingen. Of de hier beschreven risico's zich in de praktijk ook voor zullen doen, hangt in belangrijke mate af van de wijze waarop gemeenten bij het inrichten van de dienstverlening in het sociaal domein invulling geven aan de in dit deel beschreven aanbevelingen om de privacy te borgen. Dit hoofdstuk laat zich in die zin lezen als een serie aandachtspunten voor gemeenten bij het op adequate wijze borgen van de privacy in het sociaal domein.

In dit deel komen achtereenvolgens aan bod:

3 Organisatie van de dienstverlening en uitbesteding
4 Werkprocessen en triage
5 Informatiehuishouding, registratie, toegang, bewaren en vernietigen van gegevens
6 Transparantie en positie van de burger
7 Kennis en bewustwording medewerkers
8 Beleid

3. Organisatie van de dienstverlening en uitbesteding

Algemene toelichting
Op het gebied van de organisatie van de dienstverlening in het sociaal domein zal de praktijk verschillende varianten laten zien. Drie aspecten springen eruit in verband met het borgen van de privacy.

Het eerste aspect dat in beeld komt is de mate van uitbesteding bij gemeenten die bijvoorbeeld werken met wijkteams. Sommige gemeenten organiseren intake, vraagverheldering en besluitvorming rond ondersteuningsverzoeken van de burger zoveel mogelijk in huis. Andere gemeenten richten een aparte stichting op waarin een deel van de dienstverlening plaatsvindt, en soms ook een deel van de hulpverlening zelf. Sommige gemeenten kennen wijkteams die op zichzelf weer een samenwerkingsverband zijn. Weer andere gemeenten overwegen om het hele proces uit te besteden aan een contractpartner die op basis van een vooraf vastgesteld bedrag zowel de intake, vraagverheldering, beschikking en dienstverlening organiseert.

Het tweede aspect dat in beeld komt is de mate van horizontale integratie van taken. Werkt de gemeente met generalisten die bijvoorbeeld zowel de taken op het gebied van Wmo, Jeugdwet als Participatiewet, of blijven verschillende loketten of specialismen herkenbaar.

Een derde aspect dat in beeld komt is de mate van verticale integratie. Hierbij gaat het om de vraag in hoeverre een medewerker meerdere stappen in het proces voor zijn of haar rekening neemt. Sommige gemeenten hanteren een strikte scheiding tussen intake, behoeftebepaling en planvorming, besluitvorming, uitvoering en regie. Andere gemeenten hanteren het principe van 'wie wikt, beschikt' en zien het liefste dat 'het ondersteuningsplan' ook meteen de aanvraag en zo mogelijk het besluit voor een voorziening is. Daarnaast organiseren sommige gemeenten ook een deel van de lichte hulpverlening of algemeen toegankelijke ondersteuning in hetzelfde team dat het onderzoek doet en het ondersteuningsplan opstelt.

De keuzes die gemeenten op de bovengenoemde aspecten maken kunnen specifieke privacyissues met zich meebrengen. In dit hoofdstuk gaan wij nader in op de mogelijke keuzes voor gemeenten en de specifieke privacyrisico's die zich bij de verschillende keuzes voor kunnen doen.

3.1 Zelf doen, uitbesteden, samenwerken

Deze paragraaf gaat in op de organisatorische positionering van met name wijkteams zoals die nu bij veel gemeenten in oprichting zijn. Daarin worden een aantal varianten zichtbaar die we hier op hoofdlijnen beschrijven.

De kabinetsvisie 'Zorgvuldig en bewust' stelt dat het College van B&W ervoor verantwoordelijk is dat de gegevensverwerking door samenwerkingsverbanden en contractpartners die gemeentelijke taken uitvoeren zorgvuldig en in overeenstemming met de wetgeving gebeurt. Een belangrijk aandachtspunt bij dit organiseren is de vraag of het College deze verantwoordelijkheid kan waarmaken.

We kijken naar de volgende varianten:

Variant a. Het wijkteam(of de gemeentelijke afdeling) als organisatieonderdeel van de gemeente, al dan niet met detachering van externen.

Variant b. Het wijkteam als externe organisatie, dat werkt onder aansturing van de gemeente

Variant c. Het wijkteam als externe organisatie, dat haar eigen wijkteam concept aanbiedt aan een of meerdere gemeenten

Variant d. Het wijkteam als samenwerkingsverband

Variant e. Het wijkdienstenmodel

Variant a. Het wijkteam als organisatieonderdeel van de gemeente
Het wijkteam is in dit geval een afdeling van de gemeentelijke organisatie. Het team werkt volgens de werkprocessen die door het management van de gemeente zijn vastgesteld en maakt gebruik van het ICT-systeem van de gemeente. Teamleden voeren hun taken uit op basis van bevoegdheidsverlening door het college (bijv. mandaat, volmacht of machtiging). Teamleden kunnen zijn ingehuurd. Maar het team en de medewerkers werken onder de directe gezagsverhoudingen van de gemeente.

Risico's

- Deze wijze van organiseren kent weinig specifieke privacy-risico's ten opzichte van de gangbare werkwijzen bij gemeenten, zoals bijvoorbeeld de huidige uitvoering van de Wmo.

Variant b. Het wijkteam als externe organisatie, dat werkt onder aansturing van de gemeente
De gemeente laat hierbij de taken in het sociaal domein uitvoeren door teams die ondergebracht zijn in een externe organisatie. De organisatie werkt volledig onder regie van de gemeente. De gemeente bepaalt de werkprocessen en beheert ook het ICT-systeem. Desalniettemin is er de facto sprake van uitbesteding van taken. Het uitbesteden van gemeentelijke taken aan een contractpartner brengt altijd extra risico's met zich mee ten aanzien van privacy en informatiebeveiliging. En het is van belang dat de gemeente hier in de af te sluiten contracten aandacht aan besteed.

Risico's:
In principe kunnen zich bij deze variant de volgende risico's voordoen:

- De bevoegdheidsverlening is onvoldoende geregeld of loopt achter op personele wijzigingen, waardoor niet alle medewerkers voldoende duidelijk bevoegd zijn voor de taken die zij uitvoeren en de daarbij behorende gegevensverwerkingen (risico type B).
- De partner verwerkt onnodig of bovenmatig persoonsgegevens bij de uitvoering van de taken of beveiligt (gevoelige) persoonsgegevens onvoldoende en niet geheel conform de beveiligingsvoorschriften die de gemeente hanteert, waardoor de privacy van burgers niet kan worden gegarandeerd. De gemeente kan dan aansprakelijk gesteld worden voor het handelen van de contractpartner (risico type A3 en B).
- Bij verandering van contractpartner, faillissement of overname is kan er onduidelijkheid ontstaan wat er met gegevens bij de contractpartner moet gebeuren, en hoe en op welke wijze gegevens overgedragen dienen te worden naar de nieuwe contractpartner. Persoonsgegevens kunnen daardoor in 'verkeerde handen' raken (risico type A1 en B).

Aanbevelingen

- Werk de bevoegdheidsverlening, zoals de inhoud van de mandaatbesluiten zorgvuldig uit , en maak afspraken over procedures bij personele wijzigingen.
- Maak in de contracten die worden afgesloten met de organisatie waarin de teams zijn ondergebracht afspraken over gegevensverwerking, het borgen van de privacy en het naleven van de richtlijnen voor informatieveiligheid. Borg daarin dat de contractpartner hier tenminste net zo zorgvuldig mee om zal gaan als dat de gemeente verplicht is te doen.
- Onderdelen van deze afspraken kunnen zijn: dat de contractpartners inzichtelijk maken hoe zij de privacy van burgers borgen in hun werkproces, en invulling geven aan de uitgangspunten van noodzaak, subsidiariteit en proportionaliteit uit de Wbp; organisatorische waarborgen, en training van medewerkers op de gebieden van privacy en informatieveiligheid.
- Beoordeel of het nodig is in de contracten aandacht te besteden aan zaken als overdracht van gegevens bij verandering van contractpartner, faillissement of overname.

Variant c. Het wijkteam als externe organisatie, dat haar eigen ' team concept' aanbiedt aan een of meerdere gemeenten en daarbij gebruik maakt van eigen ICT-systemen

De gemeente koopt de uitvoering van (een deel van) haar taken in het sociaal domein in, bij een partner die daarvoor reeds een eigen werkproces heeft ontwikkeld, gebruik maakt van eigen mensen die werken met eigen systemen van de betrokken organisatie. Daarbij kan het voorkomen dat de betrokken partij werkt voor meerdere gemeenten, en naast 'het product' wijkteam ook nog andere diensten aanbiedt in het sociaal domein.

Het uitbesteden van gemeentelijke taken aan een samenwerkingsverband, of contractpartner brengt altijd extra risico's met zich mee ten aanzien van privacy en informatiebeveiliging, en het is van belang dat de gemeente hier in de af te sluiten contracten aandacht aan besteedt.

Risico's:

- De risico's zoals genoemd bij variant b, doen zich hier in versterkte mate voor omdat de contractpartner zich meer manifesteert als een autonome organisatie met eigen systemen en werkprocessen. Deze staat daardoor meer op afstand, waardoor de gemeente minder zicht heeft op de dagelijkse gang van zaken.. Hierdoor bestaat het risico dat gegevensverwerking uit de pas loopt met de gemeentelijke uitgangspunten of dat mogelijk onzorgvuldige omgang met gegevens pas in een laat stadium zichtbaar wordt voor de gemeente.

Daarnaast doen zich een aantal specifieke risico's voor:

- Persoonsgegevens van cliënten van het wijkteam worden gedeeld met collega's in de organisatie ten behoeve van andere taken of activiteiten van de organisatie (risico type A3).
- Gegevens worden mogelijk opgeslagen bij externe partijen, eventueel in het buitenland waar andere wettelijke voorschriften gelden. Er ontstaat zo een keten van gegevensopslag waardoor de privacy en informatieveiligheid niet altijd goed worden gegarandeerd. Dit risico doet zich met name voor als de organisatie eigen systemen gebruikt en voor de systemen weer externe partijen inschakelt voor bijvoorbeeld het beheer van de systemen of de opslag van gegevens (risico type B).

Aanbevelingen

- De aanbevelingen genoemd onder variant b, zijn hier op dezelfde wijze van toepasing.
- Het is van belang dat de gemeente in contracten expliciet bepalingen opneemt over de afscherming van gegevens die verkregen zijn in het kader van de gemeentelijke taken ten opzichte van gegevens die voor eventuele andere taken gebruikt worden (hergebruik verbiedt) en passende sancties afspreekt op overtreding van die bepalingen.
- Het is van belang dat gemeenten in contracten verzekeren dat er in de gehele keten, ook als er sprake is van uitbesteding van ICT naar het buitenland, sprake is van een zorgvuldige verwerking van persoonsgegevens en adequate informatiebeveiliging die voldoet aan de eisen van de Nederlandse wetgeving.

Variant d. Het wijkteam als samenwerkingsverband

Bij deze variant wordt het wijkteam gevormd door een samenwerkingsverband tussen gemeenten en instellingen. Soms functioneren de teamleden onder een teamleider van de gemeente of van één van de

samenwerkingspartners. Soms functioneren ze volledig vanuit hun eigen organisatorische kaders en discipline. Aan de samenwerking ligt vaak een samenwerkingsconvenant ten grondslag waarin doel en middelen van de samenwerking zijn vastgelegd. Veelal worden deze ondersteund door afspraken over gegevensuitwisseling.

Het laten uitvoeren van gemeentelijke taken door een samenwerkingsverband, kan gezien worden als een bijzondere vorm van uitbesteding en brengt als zodanig altijd extra risico's met zich mee ten aanzien van privacy en informatiebeveiliging. Het is van belang dat de gemeente hier in de af te sluiten contracten en convenanten aandacht aan besteed.

Risico's:
De risico's onder varianten b en c doen zich ook hier voor. Er doen zich echter een aantal specifieke risico's voor die te maken hebben met het karakter van sommige samenwerkingsverbanden.

- Door het hybride karakter van samenwerking is niet altijd duidelijk of teamleiders en teamleden binnen dezelfde organisatorische regels functioneren. Of adequate (aan)sturing en beoordeling van teamleden mogelijk is, is dan ook niet altijd duidelijk.[1] Hierdoor kan ook onduidelijkheid ontstaan ten aanzien van de verantwoordelijkheid ten aanzien van gegevensverwerking en het borgen van de privacy (risico type B).
- Als medewerkers zowel taken uitvoeren voor de gemeente - bijvoorbeeld intake, onderzoek en besluiten over voorzieningen - als hulpverleningstaken namens hun eigen organisatie, krijgen zij te maken met verschillende juridische regimes voor het verwerken van gegevens. Dit vergroot de onduidelijkheid over de bij de verschillende werkzaamheden toe te passen regels en vergroot de kans op fouten bij gegevensverwerking (risico type A1 en A3).
- Indien het wijkteam geen gebruik maakt van een afzonderlijk systeem voor de gemeentelijke taken en de voor de gemeentelijke taken noodzakelijke persoonsgegevens verwerken met systemen van de eigen moederorganisaties ontstaan er een aantal extra risico's:
    - het risico neemt toe dat gegevens die verwerkt worden voor de gemeentelijke taken vermengd raken met gegevens die verwerkt worden voor de eigen taken van de moederorganisatie. Bijvoorbeeld: gegevens voor gemeentelijke toegangstaak, worden in een dossier geregistreerd met het hulpverleningsdossier (risico type A1).
    - persoonsgegevens voor de gemeentelijke taken worden op verschillende plekken geregistreerd, waardoor het niet mogelijk is voor de gemeente om hier goed toezicht op en beheer over uit te oefenen (risico type B).
    - Het risico van de onder variant b en c genoemde risico's met betrekking tot veranderingen van contractpartner, faillissement of overname van samenwerkingspartners, doet zich hier in versterkte mate voor omdat er meerdere partners zijn;
- Persoonsgegevens van cliënten van het wijkteam worden gedeeld met collega's van de moederorganisatie ten behoeve van andere taken van de moederorganisatie (risico type A1 en A3).

Aanbevelingen
De aanbevelingen bij variant b en c zijn hier ook van toepassing.

- Het hybride karakter vraagt om een extra nauwkeurige omschrijving van de gemeentelijke taken die in het samenwerkingsverband worden uitgevoerd en scheiding van andere taken. Uitgangspunt daarbij moet zijn dat medewerkers als zij bezig zijn met het uitvoeren van de gemeentelijke taak, handelen volgens de daarvoor geldende juridische regimes en niet de regimes van hun moederorganisatie van toepassing verklaren op de gemeentelijke taak. Dit vraagt van de medewerkers een zeer hoog rolbewustzijn.
- Met betrekking tot de systemen waarmee gegevens verwerkt worden verdient het voorkeur om ervoor te zorgen dat alle medewerkers de gegevens in het kader van de gemeentelijke taken met hetzelfde systeem en op dezelfde wijze verwerken (niet verspreid over de systemen van de moederorganisaties). Bij voorkeur wordt voor de gemeentelijke taken een specifiek ingericht systeem gebruikt.

Variant e. Het wijkdienstenmodel

[1] De vormgeving van sociale wijkteams, Platform 31, BMC advies en Universiteit Twente, oktober 2014

Een variant die door sommige gemeenten wordt overwogen is het wijkdienstenmodel. In het wijkdienstenmodel ontvangt een hoofdaannemer een lumpsum financiering voor een wijk en organiseert voor dit bedrag de dienstverlening in het sociaal domein, inclusief de levering van noodzakelijke zorg, al dan niet via onderaannemers. De gemeente positioneert zich volledig in de rol van opdrachtgever op basis van vooraf afgesproken prestaties. Desalniettemin blijft de gemeente ook hierbij verantwoordelijk voor een zorgvuldige uitvoering van de taken en het voldoen aan de wettelijke verplichtingen ook met betrekking tot de gegevensverwerking en borging van de privacy. Het betreft een experimentele vorm van dienstverlening, waarover nog slechts weinig informatie bekend is.

Risico's:

- De risico's onder varianten b, c en d doen zich ook hier voor. De afstand van de opdrachtgevende gemeente is hierbij echter groter waardoor deze risico's zich in versterkte mate voor kunnen doen.
- Daarnaast kan de zeer zelfstandige positie van de uitvoerende organisatie tot gevolg hebben dat zowel burgers als contractspartijen van die organisatie als het ware uit het oog verloren wordt dat er sprake is van gemeentelijke dienstverlening (risico type B).

Aanbevelingen

De aanbevelingen beschreven onder b, c en d zijn ook hier van toepassing. Daarnaast komen wij tot de volgende aanvullende aanbevelingen:

- Besteed extra aandacht aan de positie van de burger, bijvoorbeeld door een laagdrempelige mogelijkheid voor de burger om in contact te kunnen treden met de gemeente bij bijvoorbeeld klachten of privacy bezwaren.

3.2 Horizontale integratie van taken

Deze paragraaf gaat in op privacy-risico's die gerelateerd zijn aan de mate waarin taken in het sociaal domein 'horizontaal zijn geïntegreerd'. Bij een gemeente die werkt met generalisten die zowel de taken op het gebied van Wmo, Jeugdwet als Participatiewet doen, doen zich andere privacy-risico's voor dan bij een gemeente waarbij de dienstverlening georganiseerd wordt binnen de kolommen van de verschillende domeinen of specialismen.

De archetypen van de VNG/KING beschrijven vijf varianten waarin de mate van integratie ook een rol speelt.

- Archetype 1 transitieproof: hierbij wordt de dienstverlening en toegang tot voorzieningen per kolom georganiseerd. Er is geen integratie van taken. De gedachte van 1 gezin, 1 plan, 1 regisseur wordt op korte termijn niet gerealiseerd.
- Archetype 2 totaal integraal: vanaf eerste contact integrale beoordeling door één medewerker voor de verschillende domeinen. Er wordt één toegang gecreëerd tot het sociale domein. Dit kan door middel van wijkteams, maar ook op centraal of ander niveau.
- Archetype 3 geclusterd integraal: geclusterde toegang, veelal door Wmo en jeugd te combineren en het W&I-loket in stand te laten. Maar andere clusteringen zijn mogelijk.
- Archetype 4 integraal in tweede instantie: hierin vindt het eerste contact plaats via een van de kolommen. Indien er sprake blijkt te zijn van bredere problematiek volgt doorverwijzing naar een wijkteam vooral gericht op multi problematiek.
- Het vijfde archetype 'geclusterd integraal anders' is vooral bijzonder vanwege de uitbesteding. De specifieke risico's met betrekking tot uitbesteding zijn reeds behandeld in paragraaf 3.1.

Afhankelijk van de mate van integraliteit doen zich risico's voor die te maken hebben met de inrichting van het werkproces, en risico's die te maken hebben met de bevoegdheden en toegang van medewerkers tot gegevens. In deze paragraaf wordt met name ingegaan op de risico's die te maken hebben met de bevoegdheden van medewerkers en de toegang van medewerkers tot persoonsgegevens.

3.2.1 Archetype transitieproof

De dienstverlening in dit archetype wordt georganiseerd via de kolommen. Medewerkers hebben in principe slechts toegang tot persoonsgegevens van de kolom waarvoor zij werken. Persoonsgegevens worden verwerkt

binnen de kolommen volgens de regels binnen dat specifieke domein en er is geen sprake van planvorming op een hoger niveau.

Risico's

- Bij dit archetype zijn er geen extra privacy-risico's ten opzichte van de huidige situatie.
- Door de verkokerde manier van werken bestaat het risico dat de gemeente (latente) multi-probleemsituaties minder snel op het spoor zal komen en door een minder integrale aanpak niet tot de optimale ondersteuning komt. Dit is een risico zowel vanuit hulp- als vanuit kostenperspectief.

Aanbevelingen

- Besteed in het werkproces binnen de kolommen en de training van medewerkers aandacht aan het herkennen van meervoudige problematiek en organiseer een procedure om daarmee om te gaan. Anders gezegd: draag zorg voor een adequate aanpak bij multi-problematiek, bijvoorbeeld door aan dacht te besteden aan archetype 4.

3.2.2 Archetypen met verschillende maten van integraliteit

Bij de archetypen 2 t/m 4 zijn er organisatieonderdelen actief die als taak hebben om indien nodig integrale dienstverlening te bieden. Deze benadering sluit aan bij de doelstellingen van de decentralisaties. Een van de achtergronden van de decentralisaties is dat gemeenten beter in staat zijn om waar nodig tot een integrale aanpak problemen van burgers te komen.

Inherent aan een integrale werkwijze is dat medewerkers op enig moment in het proces een afweging moeten maken ten aanzien van de aard van de problematiek waar zij mee te maken hebben. Gaat het om een enkelvoudige vraag of spelen er meer problemen? Kan de betrokkene het allemaal zelf goed aan, of speelt er wellicht zelfredzaamheidsproblematiek. Gaat het om deze ene persoon, of is er sprake van gezinsproblematiek? In de kabinetsvisie *Zorgvuldig en bewust*, worden dit type afwegingen aangeduid als triage. Voor het maken van deze afwegingen is verwerking van persoonsgegevens noodzakelijk. In eerste instantie op basis van informatie die de burger zelf geeft. En afhankelijk van de situatie op basis van gegevens uit bestanden of van andere professionals. Omdat op voorhand niet duidelijk is wat de probleemsituatie is, is ook vooraf niet aan te geven welke persoonsgegevens noodzakelijk zijn om te verwerken. Dit stelt eisen aan de wijze waarop gemeenten afwegingen maken ten aanzien van gegevensgebruik in hun werkprocessen. Op de verschillende manieren waarop gemeenten dat doen wordt nader ingegaan in Hoofdstuk 4 'Werkprocessen en triage'.

Bovenstaande impliceert ook dat de medewerkers bij een integrale aanpak toegang hebben tot gegevens uit verschillende domeinen. Als de gemeente geen extra maatregelen neemt met betrekking tot autorisaties, dan bestaat deze brede toegang tot gegevens ook in situaties dat de medewerker een 'enkelvoudige vraag' of de vraag van een zelfredzame burger behandelt.

Daarnaast hebben de medewerkers van deze teams te maken met verschillende juridische regimes binnen de verschillende domeinen, ook op het gebied van gegevensverwerking. In het jeugddomein geldt bijvoorbeeld dat werkzaamheden door specifieke gekwalificeerde medewerkers uitgevoerd dienen te worden.

Risico's

Op basis van bovenstaande kunnen zich bij horizontale integratie de volgende risico's voordoen:

- De bevoegdheden van de medewerkers met betrekking tot de taken en de daarvoor noodzakelijke gegevensverwerking zijn niet allemaal voldoende juridisch geborgd in bijvoorbeeld een mandaatregeling (risico type B).
- Een medewerker gaat vanuit een integrale visie breder gegevens gebruiken (bijvoorbeeld inzien of vastleggen) dan in een concreet geval noodzakelijk is gezien de ondersteuningsvraag van de burger en de aard van de problematiek (risico type A3).

Aanbevelingen

a. Maak een nauwkeurige analyse van de taken en werkzaamheden die aan de wijkteams toebedeeld worden en de bevoegdheden die zij toebedeeld moeten krijgen om deze ook uit te mogen voeren. Houdt bij de inrichting van werkprocessen en systemen rekening met de verschillende regels die kunnen gelden ten aanzien van de gegevensverwerking in specifieke domeinen.

b. Richt de toegang tot gegevens zo in dat een medewerker bewust aan moet geven tot welke gegevens van een cliënt hij toegang wil hebben op basis van de specifiek problematiek van die cliënt. Analyseer regelmatig hoe medewerkers hiermee omgaan, bijvoorbeeld op basis van log-gegevens en neem aanvullende maatregelen als medewerkers structureel meer gegevens inzien dan noodzakelijk. Hetzelfde geldt voor het verzamelen en vastleggen van gegevens.

3.3 Verticale integratie van taken

Bij verticale integratie van taken gaat het om de vraag in hoeverre een medewerker meerdere stappen in het proces voor zijn of haar rekening neemt. Gemeenten maken hierin verschillende keuzen. Sommige gemeenten hanteren een strikte scheiding tussen intake, behoeftenbepaling en planvorming, besluitvorming, uitvoering en regie. Andere gemeenten hanteren het principe van 'wie wikt, beschikt' en zien het liefste dat 'het ondersteuningsplan' ook meteen de aanvraag en het besluit voor een voorziening is. Daarnaast organiseren sommige gemeenten ook een deel van de lichte hulpverlening in hetzelfde team dat het onderzoek doet en het ondersteuningsplan opstelt. Belangrijke aspecten die spelen bij verticale integratie van taken zijn de verschillende juridische regimes die samenhangen met de taken en rollen die medewerkers hebben in het proces en de overdracht van informatie tussen afdelingen en medewerkers. We onderscheiden hierbij een aantal hoofdvarianten van verticale integratie.

- Minimale verticale integratie van taken
- Verticale integratie van intake, onderzoek en besluitvorming
- Maximale verticale integratie van taken (inclusief delen van de hulpverlening en regie)

3.3.1 Minimale verticale integratie van taken

Bij 'minimale integratie van taken' zijn de verschillende fasen in het proces duidelijk gescheiden en worden door verschillende medewerkers en verschillende afdelingen gedaan. De eerste intake gebeurt veelal aan een loket, de behoeftebepaling van de klant en indien nodig, het opstellen van het ondersteuningsplan gebeuren door een medewerker van een inhoudelijk team. De aanvragen voor voorzieningen die op basis van het plan noodzakelijk zijn, worden afgehandeld door een medewerker van de back office, die soms ook nog een procesmatige of inhoudelijke toets doet. De uitvoering van de hulpverlening of de levering van maatwerkvoorzieningen gebeurt door gecontracteerde zorgverleners. Indien er sprake is van regie door de gemeente in de fase van de uitvoering van het plan gebeurt dit door een aparte regisseur. De praktijk laat zien dat de regierol vaak toebedeeld wordt aan de medewerker die betrokken geweest is bij het opstellen van het plan.

Door de scheiding in taken, vindt er bij elke overgang ook een overdracht plaats van persoonsgegevens tussen medewerkers en/of afdelingen. In sommige gevallen komen die gegevens ook in een ander systeem terecht, waarin soms andere regimes gehanteerd worden ten aanzien van privacy en de toegang tot gegevens door medewerkers. Een belangrijk aspect is hier dat bij de overdrachtsmomenten tussen de verschillende fasen van het proces aandacht wordt besteed aan de vraag welke informatie dan noodzakelijk is om over te dragen. Het maakt vanuit privacy-optiek een groot verschil of een medewerker het hele ondersteuningsplan en onderliggende informatie doorstuurt naar de afdeling die de aanvraag moet behandelen, of alleen de informatie doorgeeft die noodzakelijk is voor het nemen van een besluit over de toe te kennen voorziening.

<u>Risico's</u>

- Er worden meer persoonsgegevens overgedragen naar een andere afdeling die betrokken is bij het dienstverleningsproces dan noodzakelijk is voor de taak die de betreffende ontvangende afdeling heeft. Hierdoor wordt de privacy van betrokken burgers onnodig geschonden (risico type A3).
- Bij de overdracht van persoonsgegevens komen deze terecht in een omgeving en een systeem waarin een ander, minder strikt regime, gehanteerd wordt ten aanzien van toegankelijkheid en beveiliging van gegevens. Hierdoor wordt de privacy van betrokken burgers minder goed beschermd (risico type A3 en B).

<u>Aanbevelingen</u>

- Maak een analyse van de gegevens die noodzakelijk zijn voor de taak van de afdeling waaraan gegevens worden overgedragen. En richt het proces zo in dat zo min mogelijk gegevens overgedragen hoeven te worden.

- Breng de opeenvolgende omgevingen en systemen waarin persoonsgegevens terecht komen in kaart, en neem maatregelen om de privacy en informatieveiligheid in de hele keten (van systemen) te borgen.

3.3.2 Verticale integratie van intake, onderzoek en besluitvorming

Gemeenten die deze variant hanteren gaan uit van het adagium 'wie wikt, beschikt'. De intake vindt veelal nog wel aan het loket plaats. De behoeftebepaling van de klant, en het opstellen van het ondersteuningsplan gebeuren door een medewerker van een inhoudelijk team. Het feit dat een medewerker samen met de cliënt tot de conclusie komt dat een bepaalde voorziening noodzakelijk is, geldt tevens als beslissing op die aanvraag. Vaak wordt uit efficiëncy-overwegingen het uiteindelijke besluit nog wel in de back office genomen, maar dan meer als administratieve handeling. In sommige gevallen vindt er in de back office nog een technische toets plaats,bijvoorbeeld bij woningaanpassingen. Voor de uitvoering van de hulpverlening of levering van maatwerkvoorzieningen en regie door de gemeente in de fase van de uitvoering van het plan geldt hetzelfde als bij de hiervoor beschreven variant.

Door de verticale integratie van taken, hoeft er in principe minder overdracht van persoonsgegevens plaats te vinden naar andere afdelingen dan bij minimale verticale integratie. Persoonsgegevens gaan door minder handen en door minder systemen, waardoor de privacy-risico's beperkter zijn dan bij die variant. Als er vanuit gegaan wordt dat de inhoudelijke beoordeling in de planfase is gedaan, zou de gegevensoverdracht naar de back office voor het nemen van beslissingen beperkt moeten kunnen blijven.

<u>Risico's</u>

- Het risico is dat een gemeenten ondanks de verticale integratie van taken, haar proces toch zo inricht dat de medewerker die de inhoudelijke beoordeling doet toch een heel plan of dossier doorstuurt naar de back office. De reden daarvoor is dat de inhoudelijke overwegingen dan reeds beschikbaar zijn bij een eventueel bezwaar of beroep. In dat geval worden de privacy-voordelen van deze variant teniet gedaan en doen de privacyrisico's genoemd bij 'minimale verticale integratie' zich alsnog voor.

3.3.3 'Maximale' integratie van taken

In deze variant is er één medewerker die het hele proces doet, van intake tot en met de besluitvorming over aanvragen, en deze medewerker doet ook delen van lichtere hulpverlening en regie. Ook hier wordt het uiteindelijke besluit vaak (formeel) in de back office genomen.

Door de verticale integratie van taken komen medewerkers in verschillende fasen van het proces in verschillende rollen terecht. Die rol verschuift in de loop van het proces grofweg van 'consulent', naar planmaker, naar beoordelaar, naar regisseur en hulpverlener. Dit vraagt aandacht voor de juridische vormgeving, toegang tot gegevens, en vooral het rolbewustzijn van medewerkers.

Vanuit de dienstverleningsgedachte is het positief dat een burger gedurende het hele proces met dezelfde medewerker te maken heeft. Ook hoeft in deze variant minder overdracht van gegevens plaats te vinden tussen afdelingen of tussen de gemeente en instellingen. Desalniettemin doen zich een aantal privacy-risico's voor.

<u>Risico's</u>

- Medewerkers hebben toegang tot gegevens en onderdelen van het dossier, waar zij uit hoofde van de taak en rol die zij op dat moment vervullen geen toegang meer toe zouden mogen hebben. Dit speelt met name bij de rolveranderaar van planmaker/beoordelaar naar hulpverlener (risico type A1 en A3).
- Bij vergaande vormen verticale integratie neemt het risico toe dat persoonsgegevens die idealiter gescheiden blijven vermengd raken en daardoor niet meer gescheiden kunnen worden ontsloten. Het kan hier bijvoorbeeld gaan om persoonsgegevens waarover de betreffende medewerker beschikt vanuit zijn rol als behandelaar en persoonsgegevens waarover hij of zij beschikt als beoordelaar. Vanuit privacyoverwegingen is het gewenst om dergelijke typen informatie te scheiden zodat ze ook gescheiden ontsloten kunnen worden. Dat laatste is van belang als er bijvoorbeeld sprake is van personele wisselingen op één van de rollen, of als collega's specifieke informatie uit het dossier moeten kunnen inzien maar niet het hele dossier (risico type A3 en B).

Aanbevelingen

- Creëer in de informatiesystemen de mogelijkheid om de toegang tot gegevens en onderdelen van het dossier zowel te baseren op betrokkenheid bij de cliënt als de taak en rol die de medewerker op dat moment heeft met betrekking tot de cliënt.
- Besteed in training van medewerkers aandacht aan het thema van rolwisselingen en maak zorgvuldige omgang hiermee onderdeel van het teamontwikkelproces.

4. Werkprocessen en triage

Algemene toelichting

In de kabinetsvisie 'Zorgvuldig en bewust' stelt het kabinet dat gemeenten de privacy van burgers kunnen borgen in hun dienstverleningsprocessen door 'het inrichten van een zorgvuldig proces van triage waarin de stapsgewijze afwegingen ten aanzien van gegevensverwerking een plaats hebben. Privacy wordt op die manier onderdeel van de kwaliteit van het dienstverleningsproces en de professionaliteit van de medewerker.'

Voor het standaardwerkproces van gemeenten in het sociaal domein hanteert KING de fasering zoals beschreven in deel I:

- Klantcontact en intake
- Behoeftebepaling en planvorming
- Besluitvorming
- Uitvoering en levering
- Regievoering

.

Een aantal aspecten springen eruit die van belang zijn met betrekking tot het borgen van de privacy:

1. De omgang met gegevens bij de triage in de fasen van intake, behoeftebepaling en planvorming, en besluitvorming.
2. De omgang met gegevens bij signalering. Signalering heeft betrekking op de situatie waarin de gemeente signalen ontvangt van professionals of mensen uit de omgeving van een persoon.
3. De positie en organisatie van het casus-overleg.
4. De omgang met toestemming in het proces.
5. De routering van politiemeldingen.
6. De gegevensuitwisseling tussen de gemeente en zorgverleners en aanbieders in de uitvoeringsfase ten behoeve van de levering van maatwerkvoorzieningen en regie, en ten behoeve van financiële declaraties. Hieronder valt ook de uitwisseling van gegevens in het kader van de jeugdzorg in de situatie dat instellingen het besluit nemen om jeugdhulp te gaan verlenen en de gemeente financieel verantwoordelijk is.

4.1 Omgang met gegevens bij triage

Triage is het proces van verhelderen, routeren en escaleren van vragen en casussen. Door middel van triage bepaalt een medewerker of er sprake is van een enkelvoudige of meervoudige vraag, dan wel complexe (multiprobleem) casuïstiek, en welke mate van gegevensverwerking daarbij hoort. Bij een eenvoudige en enkelvoudige vraag is de gegevensverwerking beperkt terwijl er bij een complexere vraag wellicht meer partijen betrokken zijn er dus meer gegevens verwerkt (en eventueel uitgewisseld) worden.

In de werkprocessen van de gemeenten in het sociaal domein, zijn grofweg drie triagemomenten te herkennen. Deze staan beschreven in de handreiking 'Triagekader en instrument' van KING/VNG van oktober 2014. Daarin wordt ook geschetst hoe gemeenten op een verantwoorde manier om kunnen gaan met gegevens in het kader van triage.

Het eerste triagemoment heeft betrekking op vraagverheldering als een burger zich meldt bij de gemeente met een vraag. Hier maakt een medewerker de inschatting of de betrokkene voldoende geholpen is met het verstrekken van informatie of doorverwezen moet worden naar een medewerker WMO, Jeugd, Werk en Inkomen, of verwezen dient te worden naar een wijkteam gericht op bijvoorbeeld multi problematiek.

Het tweede triagemoment vindt plaats tijdens de fase van behoeftebepaling en planvorming. Hier maakt de betrokken medewerker op basis van gesprekken en informatieverzameling in samenspraak met betrokkene(n), een inschatting of er sprake is van enkelvoudige en relatief eenvoudig op te lossen problematiek, of dat de hulpvraag niet meer eenvoudig kan worden afgehandeld maar er echt sprake is van een meervoudige of complexe vraag die een integrale aanpak en vormen van regie noodzakelijk maken.

Het derde triagemoment heeft betrekking op escalatie. Deze afweging vindt plaats als sprake lijkt te zijn van zware problematiek of weigerachtigheid om mee te werken aan hulpverlening terwijl de situatie zeer ernstig is. Hier vindt de afweging plaats of escalatie naar een gespecialiseerd team (interventieteam) of veiligheidshuis en eventueel een dwang-en-drangkader of bemoeizorg noodzakelijk is. Hierbij speelt ook de afweging of het noodzakelijk is om gegevens buiten medeweten van de cliënt om verwerken.

In deze paragraaf gaan we in op de keuzes die gemeenten kunnen maken ten aanzien van de omgang met gegevens in het triageproces. Daarnaast zoomen we apart in op de omgang met gegevens rond casus-overleggen en escalatie.

4.1.1 Impliciete en expliciete triage

Alle gemeenten maken afwegingen ten aanzien van de aard van de problematiek en doen daarmee aan triage. Zij het dat de afwegingsmomenten in het werkproces nog niet altijd expliciet zijn benoemd en dat de afweging ten aanzien van de bij een bepaalde fase binnen de triage noodzakelijke gegevensverwerking niet altijd expliciet en transparant wordt gemaakt.
Gemeenten die dat wel doen bepalen per fase wat de vervolgstappen zijn, benoemen daarbij concrete de gegevens die dan noodzakelijk zijn om te verwerken en nemen de burger mee in die afweging. Op die manier worden de afwegingen ten aanzien van de noodzaak van gegevensverwerking bewust voor de medewerker, transparant voor de burger en verifieerbaar en evalueerbaar voor zowel de organisatie als de burger. Dat laatste is van belang met het oog op verantwoording en het 'leren om steeds betere afwegingen te maken'.

<u>Risico's</u>

- Gemeenten die de triagemomenten en de afwegingen ten aanzien van noodzaak van te verwerken gegevens niet expliciet inbouwen en benoemen in hun werkprocessen zijn niet transparant naar de burger en lopen een groot risico dat zij meer gegevens verwerken dan noodzakelijk is voor de taakuitvoering. Zij zijn ook niet in staat om achteraf verantwoording af te leggen over de omgang met gegevens en te leren om steeds beter te worden in het maken van afwegingen ten aanzien van gegevensgebruik (risico type A3 en B).
- Deze gemeenten lopen ook het risico dat partners niet willen meewerken aan gegevensverstrekking in situaties dat dit wel noodzakelijk en ook aanvaardbaar is, omdat ze niet in staat zijn om voldoende concreet of precies aan te geven wat doel en noodzaak zijn van de gegevensverwerking in de concrete casus (risico type A1, A3 en B). Hiermee kunnen hulprisico's ontstaan voor de betrokkene.

<u>Aanbevelingen</u>

- Benoem de triagemomenten in het werkproces, koppel daaraan een bewuste afweging ten aanzien van de gegevens die noodzakelijk zijn om vast te leggen en welke gegevens die verzameld zijn, doorgegeven moeten worden naar de volgende fase in het proces. Maak daarbij bijvoorbeeld gebruik van het triagekader en instrument van VNG/KING.[2] Leg de afwegingen bij een concrete hulpvraag vast, zodat die transparant, expliciet en verifieerbaar zijn.
- Hanteer daarbij de principes van 'dataminimalisatie', need-to-know in plaats van nice to know, en bekijk wanneer volstaan kan worden met 'dat'-informatie en wanneer zogeheten 'wat'-informatie noodzakelijk is.
- Stuur er als management op dat medewerkers deze afwegingen ook zorgvuldig en bewust maken.
- Organiseer het leren om dit typen afwegingen beter onder de knie te krijgen. Bijvoorbeeld door op geaggregeerd niveau informatie te verzamelen over de breedte van uitvraag in relatie tot problematieken. Daarmee wordt duidelijk welke soorten gegevens in de praktijk bij de verschillende

[2] https://www.visd.nl/sites/visd/files/Triagekader-en-instrument-privacy-oktober-2014.pdf

triagemomenten gebruikt worden en kan verder richting gegeven worden aan welke gegevens in welke fase noodzakelijk zijn. Ook kunnen geanonimiseerde casussen geëvalueerd worden op dit aspect. Daarmee kan bezien worden of de principes van dataminimalisatie, need-to-know in plaats van nice-to-know, en zoveel mogelijk gebruik van datgegevens in een specifieke situaties ook voldoende uit de verf komen.

4.1.2 Omgang met persoonsgegevens: De burger aan het stuur versus de gemeente aan het stuur

In de omgang met de burger en de gevolgen daarvan voor het verzamelen en verwerken van gegevens tijdens het dienstverleningsproces schetsen we hier drie modelmatige benaderingen.

De eerste is de *burger aan het stuur*. Hier kiest de gemeente ervoor om zolang mogelijk in het proces uitsluitend te werken op basis van informatie die de burger verstrekt. Sommigen ontwikkelen hiervoor een zelfassessment of quick scan op basis waarvan de burger zelf kan bepalen welke vervolgstappen hij of zij wil zetten. Bijvoorbeeld nadere informatie inwinnen, aankloppen bij een algemene voorziening, een aanvraag indienen voor een maatwerkvoorziening, of een gesprek met een medewerker.

Pas bij een aanvraag of een gesprek met een medewerker komt nadere gegevensverwerking in beeld. Bijvoorbeeld om de aanvraag te kunnen toetsen, of als tijdens het gesprek duidelijk wordt dat het nodig is een aantal zaken verder uit te zoeken op basis van gegevens van de gemeente, of in samenspraak met andere hulpverleners. Er vindt minimale dossiervorming plaats in de gemeentelijke systemen. Deze blijft bij voorkeur beperkt tot 'dat-gegevens' en bij aanvragen voor een maatwerkvoorziening, de noodzakelijke aanvraaggegevens. Alle andere gegevens blijven als uitgangspunt bij de burger zelf. Deze zit aan het stuur en beheert in die zin het eigen plan en dossier. Ook als er sprake is van zelfredzaamheidsproblematiek. Alleen als er sprake is van zware problematiek kan meer dossiervorming plaats vinden bij de gemeente.

<u>Risico's</u>

- Deze benadering kent weinig risico's vanuit privacyperspectief.
- Deze benadering kent wel hulprisico's. Doordat de gemeente zich terughoudend opstelt is de kans groter dat (latente) multi-problematiek die schuil gaat achter een schijnbaar eenvoudige hulpvraag of signaal langer buiten beeld blijft en noodzakelijke ondersteuning later op gang komt.

<u>Aanbevelingen</u>

- Om de kans dat het genoemde zorgrisico zich voordoet te verminderen, kunnen gemeenten typen hulpvragen identificeren waarvan bekend is dat ze vaak samenhangen met andere problematieken. Bij dergelijke hulpvragen kan dan middels een quick scan op basis van een beperkt aantal vragen aan de burger een inschatting gemaakt worden of er inderdaad andere problematieken spelen. Een dergelijke quick scan is in ontwikkeling bij VNG/KING.

De tweede benadering *Gemeente aan het stuur* zit aan de andere kant van het spectrum. Bij deze benadering wordt ervan uitgegaan dat een gemeente een integraal klantbeeld wil construeren op basis van gegevens die bij de gemeente zelf beschikbaar zijn en gegevens waartoe de gemeente toegang heeft (bijvoorbeeld SUWI). Gemeenten die hiervoor kiezen willen in kaart brengen welke voorzieningen al worden verstrekt aan betrokkene of aan het huishouden van betrokkene. En of er andere hulpverleners betrokken zijn of niet. Het beeld wordt meestal bepaald op basis van zogeheten 'dat-gegevens'. Op basis van dit beeld bepaalt de gemeente of het nodig is dat een medewerker een gesprek aangaat of dat bijvoorbeeld een aanvraag direct in behandeling kan worden genomen.
In deze benadering kunnen veel persoonsgegevens vastgelegd worden tijdens het proces ten behoeve van een integraal klantbeeld. Als bijvoorbeeld de zelfredzaamheidsmatrix gebruikt wordt als leidraad voor een 'keukentafelgesprek' worden alle velden van de matrix doorgenomen en de gewisselde informatie wordt vastgelegd.

Aan deze benadering liggen verschillende redenen ten grondslag. De eerste is zorginhoudelijk: (potentieel) meervoudige en complexe problematiek snel kunnen identificeren. De tweede is goede dienstverlening: betrokkene mag verwachten dat de gemeente weet welke diensten al worden verleend, en dat een medewerker of vervanger die op gesprek komt de informatie al op een rij heeft zodat de burger minder hoeft uit te leggen. De derde is efficiëncy en kostenbeheersing: Door de enkelvoudige vragen 'af te vangen' en zoveel

mogelijk digitaal af te handelen, kan de inzet van 'relatief dure' medewerkers van een integraal team worden beperkt tot de situaties dat het echt nodig is. Daarmee wordt ook onnodige belasting van burgers met keukentafelgesprekken voorkomen. Als laatste speelt het argument van fraudebestrijding.

Risico's

- Deze benadering draagt een groot risico in zich dat er bovenmatig en buitenproportioneel persoonsgegevens worden vastgelegd, omdat de afweging ten aanzien van noodzaak, proportionaliteit en subsidiariteit minimaal is. De gegevensverwerking is niet toegespitst op een concrete hulpvraag, maar vloeit eerder voort uit een voorgestane meer algemene werkwijze. Er worden in die zin persoonsgegevens a priori verwerkt die mogelijk niet relevant en noodzakelijk zijn voor de problematiek en het risico is groot dat veel persoonsgegevens terecht komen in gemeentelijke systemen. De gegevens worden dan niet zozeer vastgelegd omdat ze uiteindelijke noodzakelijk zijn voor de concrete hulpvraag, maar omdat ze in het kader van de voorgestane werkwijze nu eenmaal verzameld zijn (risico type A1 en A3).

Aanbevelingen

- Deze benadering is niet voldoende in overeenstemming met de regelgeving. Gemeenten die deze werkwijze overwegen zullen bij de intake en ook in de rest van het proces, de triagemomenten moeten benoemen en daarin steeds de afweging moeten maken welke gegevens noodzakelijk zijn, gezien de hulpvraag die de burger stelt. Anders gezegd: de hulpvraag dient centraler te staan bij de afwegingen welke gegevens wel of niet vastgelegd moeten worden.

Een werkwijze die tussen beide benaderingen in ligt is die van *De hulpvraag is leidend*. Bij het eerste contact vindt een beperkte intake plaats om te bepalen of het noodzakelijk is iemand door te verwijzen voor een gesprek naar een medewerker. De medewerker zal op basis van de hulpvraag en zijn professionele kennis bepalen welke thema's noodzakelijk zijn om te verkennen met betrokkene, en of het noodzakelijk is bepaalde informatie al vooraf te checken.

Deze werkwijze gaat uit van de professionele kennis van de medewerker met betrekking tot samenhangen tussen problematieken en de noodzaak voor samenhangende aanpak. Mede op basis daarvan maakt de medewerker afwegingen omtrent te verkennen thema's en bijbehorende gegevensverwerking ook als de burger er niet direct zelf mee komt.

Risico's

- Het privacy-risico wordt in hoge mate bepaald door de wijze waarop de gemeente erop stuurt dat medewerkers de zorgvuldige afweging ten aanzien van gegevensgebruik ook daadwerkelijk maken. Het risico bestaat dat medewerkers structureel meer gegevens uitvragen en bewerken dan noodzakelijk is en er daarbij geen correctiemechanismen zijn (risico type A3 en B).

Aanbevelingen

De aanbevelingen voor deze variant zijn dezelfde als bij par. 4.1.1

4.1.3 Escalatie

Het triagemoment rond escalatie vraagt van gemeenten extra aandacht. Bij uitzondering zal een medewerker namens de gemeente, ondanks dat betrokkene dat niet wil, toch verdere actie willen ondernemen en in dat kader ook gegevens willen verwerken. Dat is mogelijk als de professional na zorgvuldige afweging tot de conclusie komt dat het niet ondernemen van verdere actie een situatie oplevert die ontoelaatbaar is gezien de taak van de gemeente op het gebied van hulp of veiligheid. Het gaat dan bijvoorbeeld om situaties die gevaar op kunnen leveren voor de gezondheid of de veiligheid van betrokkene en/of zijn omgeving.

Vanuit privacy gezien betekent de laatste een zware inbreuk op de persoonlijke levenssfeer van mensen. De gemeente bemoeit zich nadrukkelijk met het dagelijks leven van de burger in een situatie waarbij de burger daar in meer of minder mate niet mee instemt. Zo'n beslissing vraagt dan ook om extra waarborgen om zorgvuldigheid te garanderen. De procedures die gemeenten hiervoor hanteren zijn divers. We beschrijven hieronder de risico's die bestaan bij gebrekkige procedures in algemene zin.

Risico's

- Gebrek aan duidelijke procedures voor deze inbreuk op de privacy van betrokkene kan leiden tot onzekerheid en kwetsbaarheid van professionals. Hierdoor neemt het risico van verkeerde beslissingen toe. Hieraan zit zowel een privacy als een hulprisico. Het privacy-risico is dat gegevens worden verwerkt en uitgewisseld tegen de wil van betrokkene terwijl hier onvoldoende gronden voor zijn. Het hulprisico is dat er geen gegevens worden verwerkt of uitgewisseld, terwijl dit vanuit de taak en verantwoordelijkheid van de gemeente wel noodzakelijk was geweest (risico A3 en B).
- In specifieke gevallen is niet duidelijk en verifieerbaar waarom gegevens worden verwerkt of uitgewisseld tegen de wil van betrokkene. Dit maakt de situatie ook achteraf niet transparant voor betrokkene. In het geval betrokkene hiertegen bezwaar maakt, is de gemeente kwetsbaar en mogelijk aansprakelijk (risico A3 en B).
- Het is niet duidelijk hoe vaak en op welke gronden gegevens worden verwerkt tegen de wil van betrokkene of zonder deze daarin te kennen. Daardoor is bijvoorbeeld niet duidelijk of en in welke mate drang en dwang nodig zijn en wat de beweegredenen zijn. Er is daarbij dan veelal onvoldoende feitelijke onderbouwing voor bijvoorbeeld een wenst tot aanvullende regelgeving die gegevensverwerking in dergelijke situaties faciliteert. Daarnaast is verantwoording door het College van B&W aan de Raad over deze ingrijpende beslissingen ten aanzien van de privacy van burgers niet mogelijk (risico type B).

<u>Aanbevelingen</u>

- De aanbevelingen hier zijn dezelfde als in par. 4.1.1. Echter omdat het hier om een gegevensverwerkingen gaat tegen de wil van betrokkene of buiten diens medeweten, vraagt deze beslissing om extra zorgvuldigheid. Het verdient daarom aanbeveling de procedure hiervoor apart uit te werken, ook ten aanzien van de rechten van de cliënt.
- Overweeg daarbij bijvoorbeeld om bij dit type beslissingen altijd het “4-ogen” principe te hanteren. Bijvoorbeeld door een teamleider te betrekken of om een expert in de organisatie aan te wijzen met kennis van het type problematiek en privacywetgeving.

4.2 Signalering: Meldingen door derden

Signalering heeft betrekking op de situatie waarin de gemeente signalen ontvangt van professionals of mensen uit de omgeving van een persoon. Gemeenten zullen hiervoor een proces willen inrichten dat er globaal als volgt uitziet: bij binnenkomst van signalen vindt er een eerste triage plaats naar ernst van de situatie op basis van informatie van de signaalgever. Bij crisis volgt direct handelen. Als er geen spoed is wordt meer tijd genomen om het signaal te onderzoeken. In overleg met signaalgever en degene waarover gemeld is wordt bepaald of vervolgacties nodig zijn of niet, en of doorverwijzing door bijvoorbeeld een wijkteam of AMHK nodig is.

Bij het inrichten van het proces rond de omgang met signalen spelen een aantal specifieke privacyaspecten een rol:

- Aspecten met betrekking tot de rechten van degene waarover gemeld wordt.
- De registratie van signalen en het bewaren en vernietigen van signalen.

Met betrekking tot de rechten van degene waarover gemeld wordt geldt het uitgangspunt: ‘van uitstel mag geen afstel’ komen.. Burgers dienen ook bij ‘uitstel’ zo spoedig mogelijk geïnformeerd worden dat er een melding over hem of haar is gedaan en de aard van de melding Dit tenzij er gegronde redenen zijn om dat niet te doen (in de zin van veiligheid). En betrokkene moet gewezen worden op zijn of haar rechten.

Met betrekking tot de registratie, het bewaren en vernietigen van signalen doen zich dilemma’s voor. Niet gegronde signalen dienen vernietigd te worden. Echter soms is een signaal wel gegrond, maar is één enkel signaal nog geen reden om tot actie over te gaan en is er pas echt reden om in actie te komen als binnen afzienbare tijd nieuwe en meerdere signalen over een burger of gezin binnen komen. Hier doet zich een spanningsveld voor ten aanzien van borging van de privacy en de taak van de gemeente om probleemsituaties in een vroeg stadium te signaleren dan wel te onderkennen en preventieve actie te ondernemen

<u>Risico’s</u>

- Een risico is dat een gemeente alle signalen registreert en bewaart. Het signaal blijft in het systeem beschikbaar terwijl het ongegrond was. Hierdoor wordt de registratie onrechtmatig, wordt de privacy van betrokkene geschonden en loopt deze het risico dat een signaal hem of haar blijft achtervolgen (risico type A1 en A3).
- Omgekeerd bestaat het risico dat een gemeente alle signalen die niet meteen tot een vervolgactie leiden verwijdert uit het systeem, waardoor aan vervolgsignalen niet de juiste betekenis toegekend kan worden en gevaarlijke situaties ontstaan voor betrokkenen en/of hun omgeving.Er zijn thans geen eenduidige handvatten of specifieke wettelijke voorzieningen het vastleggen van signalen in vooral situaties met signalen die niet meteen tot een specifieke vervolgactie leiden (risico type A3 en B).

Aanbevelingen

- Maak bewuste afwegingen met betrekking tot het bewaren van signalen, bijvoorbeeld in de categorieën: 'vernietigen', 'actie ondernemen', 'voorlopig bewaren, na x maanden opnieuw bezien'. Bouw in het systeem in dat een medewerker na de x aantal maanden opnieuw een expliciete afweging moet maken. Maak de afwegingen verifieerbaar en transparant.
- Stel de betrokkene altijd in kennis van het feit dat een melding over hem of haar wordt geregistreerd, tenzij er zwaarwegende overwegingen zijn om dat niet te doen. Maak ook deze afweging expliciet en verifieerbaar.
- Organiseer het leren om steeds betere afwegingen te kunnen maken. Bijvoorbeeld door managementinformatie te verzamelen die zichtbaar maakt binnen hoeveel tijd bij bepaalde meldingen vervolgsignalen binnen komen en in hoeveel procent van die gevallen er ook iets aan de hand bleek te zijn. Gebruik deze inzichten om regelmatig terug te blikken en zo te leren om betere afwegingen te maken.

4.3 Casusoverleg

Een belangrijk onderdeel van het werkproces bij wijkteams is het multidisciplinair casusoverleg. Bij vermoeden van multi-problematiek of als multi-problematiek is vastgesteld, kan een casusoverleg noodzakelijk zijn om te komen tot een adequate aanpak en afstemming tussen de verschillende betrokken hulpverleners. Op die manier geven gemeenten invulling aan het kabinetsbeleid van één gezin, één plan, één regisseur.

We onderscheiden hier twee typen multidisciplinair casusoverleg:

- *Institutioneel casusoverleg*: Bespreking van casussen in een periodiek overleg met vaste vertegenwoordigers van instellingen. Tijdens het overleg passeren meerdere casussen de revue, met als doel om te komen tot inhoudelijke aanpak, en routering van casussen.
- *Individueel maatwerkoverleg*: Bespreking met noodzakelijke derden (hulpverleners van verschillende instanties, eventueel mantelzorgers) en betrokkene(n) gezamenlijk, om tot een samenhangende analyse en aanpak te komen rond een individuele casus.

Naast bespreking van casussen in bovenstaande multidisciplinaire overleggen, worden casussen ook vaak besproken binnen het wijkteam. Dergelijke besprekingen dienen onder andere de volgende doelen:

- Bespreking binnen het team om te komen tot 'een goede match' tussen expertise van medewerkers en hulpvraag van betrokkene(n).
- Bespreking met collega's bij wijze van 'collegiale consultatie' om te komen tot een betere beoordeling en aanpak van individuele casussen.
- Bespreking van casussen met als doel om van elkaar te leren en een gemeenschappelijke aanpak te ontwikkelen.

Risico's

Afhankelijk van het type casusoverleg doen de volgende risico's zich in meerdere of mindere mate voor:

- Gebrek aan transparantie: de betrokkene heeft geen zicht op wie er allemaal kennis nemen van zijn of haar casus (risico type B).
- Er worden meer persoonsgegevens ingebracht in het overleg dan noodzakelijk is voor het doel van de bespreking (risico type A3).
- Persoonsgegevens worden gedeeld met meer teamleden of derden dan noodzakelijk is voor het doel van de bespreking (risico type A3).

- Persoonsgegevens komen terecht in teamverslagen of aanwezigen leggen persoonsgegevens vast in eigen dossiers of systemen van hun moederorganisaties, terwijl dit niet noodzakelijk is (risico type A1 en A3).

Aanbevelingen

- De verschillende doelen van de bespreking van een casus, en de verschillende settings waarin deze besproken worden vragen ook om andere afwegingen ten aanzien van de gegevensverwerking. Door bij de inrichting en organisatie van het overleg hier rekening mee te houden kan de gemeente invulling geven aan de voorwaarden voor gegevensverwerking 'op maat'. Afwegingen die hierbij een rol spelen betrekking hebben op:
    - Doel en noodzaak om de casus te bespreken in een casusoverleg.
    - Anonimisering van gegevens.
    - Rol en betrokkenheid van degene(n) om wie het gaat.
    - Beperken van de kring waarin de casus besproken wordt, bijvoorbeeld tot uitsluitend betrokkenen bij de ondersteuning, of uitsluitend collega's met noodzakelijke expertise
    - Het bepalen van de persoonsgegevens die strikt noodzakelijk zijn in het kader van de bespreking.
    - Wat wordt vastgelegd over een bespreking, wie legt het vast, waar wordt dit vastgelegd en hoe lang het wordt bewaard.

4.4 De omgang met toestemming

Veel gemeenten maken in hun werkproces gebruik van een toestemmingsverklaring. Daarin wordt de burger gevraagd om toestemming te geven voor het opvragen gegevens uit gemeentelijke bestanden en bij derden, indien de gemeente dit noodzakelijk acht. Het gebruik van toestemming kan daarbij veelal gezien worden als een soort noodgreep: "de privacy-wetgeving is ingewikkeld, dus laten we maar toestemming vragen, dan zit het wel goed." De gedachte is dat daarmee de toestemming van de betrokken kan dienen als grondslag voor eventuele gegevensverwerking in de zin van de Wbp. Dit is niet het geval.. Voor de verwerking van persoonsgegevens in het kader van haar taken in het sociaal domein zal voor de gemeente in het algemeen niet de toestemming, maar de wettelijke verplichting, of de goede vervulling van een publiekrechtelijke taak de correcte grondslag uit de Wbp moeten zijn. Weliswaar is in sommige gevallen toestemming nodig om geheimhoudingsverplichten te kunnen doorbreken, maar ook in die gevallen dient de gegevensverwerking noodzakelijk te zijn voor de goede taakuitvoering door de ontvanger. Het feit dat iemand toestemming geeft aan een verstrekker om een geheimhoudingsplicht te doorbreken, zegt immers nog niets over de reden waarom en de noodzaak dat de ontvanger die gegevens ook echt nodig heeft.

Bij toestemmingsverklaringen zijn er verschillende varianten. De toestemmingsverklaringen kunnen een algemeen karakter hebben. Ze spreken dan over gegevenscategorieën of instanties waarbij gegevens opgevraagd mogen worden, waarbij de concrete doelen waarvoor de gegevens nodig zijn niet gespecificeerd worden. Soms worden specifieke gegevens opgevraagd aan de hand van een checklist bijvoorbeeld de zelfredzaamheidsmatrix. In andere gevallen wordt, uitgaande van de situatie, hulpvraag en fase in het triage-proces, toestemming voor gegevensverzameling gevraagd op een moment dat duidelijk is welke gegevens nodig zijn voor het behandelen van de hulpvraag en de daarbij behorende dienstverlening.

Er is ook sprake van begripsverwarring. Daar waar gemeenten zeggen te werken met toestemming bedoelen ze vaak dat ze werken 'in samenspraak met de betrokkene'. Het gaat dan niet zo zeer om de juridische vorm van toestemming voor gegevensverwerking, maar veel meer om de transparantie richting betrokke(n). Bij transparantie ligt de nadruk op het feit dat de burger weet en begrijpt welke stappen de gemeente wil ondernemen om zijn of haar vraag om ondersteuning te kunnen beantwoorden, waarom die stappen noodzakelijk zijn en welke gegevens daarvoor noodzakelijk zijn om te verwerken.

Risico's

De wijze waarop gemeenten omgaan met toestemming en het gebruik van 'algemene tostemmingsverklaringen' voor het verwerken van persoonsgegevens is zeer problematisch.

- Door toestemming te kiezen als maakt zij de uitvoering van haar taken onnodig afhankelijk van toestemming. Als de gemeente 'toestemming' gebruikt als grondslag is er namelijk ook een kans dat

de betrokkene deze toestemming niet verleent, of intrekt, hetgeen de basis onder de gegvensverwerking vandaan zou trekken, terwijl de basis of noodzaak voor dienstverlening wel blijft bestaan (risico type A2).

- Het Cbp heeft er in dit verband meerdere malen op gewezen dat het gebruik van toestemming als grondslag voor het verwerken van persoonsgegeven bij de uitvoering van gemeentelijke publiekrechtelijke taken problematisch is, omdat er een afhankelijkheidsrelatie bestaat tussen gemeente en betrokkene en de toestemming daarmee vaak niet in vrijheid kan worden gegevens (risico type A2).
- Bij het gebruik van een algemene toestemmingsverklaring gaat de gemeente voorbij aan de afwegingen ten aanzien van noodzaak, subsidiariteit en proportionaliteit.. De Wbp eist dat toestemming voor het verwerken van bepaalde gegevens uitsluitend gevraagd kan worden, nadat eerst is vastgesteld dat de verwerking van die gegevens noodzakelijk, subsidiair en proportioneel is. Door het gebruik van algemene toestemmingsverklaringen lopen gemeenten het risico dat de gegevensverwerking niet rechtmatig is (risico type A1 en A2).
- Het gebruik van een algemene toestemmingsverklaring creëert een situatie die niet transparant is voor de burger. Eenmaal getekend, heeft de burger geen zicht meer op wanneer persoonsgegevens worden opgevraagd en met welk doel (risico type B).

Aanbevelingen

- Maak de beweging van 'werken met toestemming' naar 'transparantie' en 'werken in samenspraak met'. Neem daarbij hetgeen beschreven is bij triage in par. 4.1 als basis om die transparantie naar betrokkene(n) te borgen. Reserveer 'toestemming' in de juridische zin, voor die gegevens waarvoor dat een wettelijk vereiste is. In de regel gegevens waarop een geheimhoudingsplicht rust, zoals medische gegevens of waarvoor specifieke wettelijke bepalingen van toepassing zijn.
- Daar waar toestemming een wettelijk vereiste is, is het van belang dat eerst voor betrokkene duidelijk is om welk gegeven het gaat, met welk doel de gemeente het gegeven wil verwerken, en waarom dat noodzakelijk is. Oftewel: de vraag om toestemming in verband met gegevensverwerking moet in die gevallen specifiek en gemotiveerd zijn. Dus niet: 'wij willen medische gegevens bij uw huisarts opvragen'. Maar: 'wij overwegen deze dagbesteding te bieden. Zijn er eventueel medisch relevante zaken waarmee wij dan rekening moeten houden, of kunnen we daarvoor zo nodig contact opnemen met uw huisarts?'

4.5 Gegevensuitwisseling tussen gemeente en hulpverleners in de uitvoeringsfase en bij financiële verantwoording

In de uitvoeringsfase zal er opnieuw sprake zijn van gegevensuitwisseling, in dit geval tussen de gemeente en hulpverleners. In deze paragraaf gaan we in op drie categorieën:

1. Gegevensuitwisseling tussen gemeente en hulpverlener of maatwerkaanbieder ten behoeve van de opdrachtverstrekking en declaratie van te verlenen hulp, of van een maatwerkvoorziening;
2. De gegevensverwerking ten behoeve van de regie op hulp in de situatie dat een integrale aanpak noodzakelijk is;
3. De gegevensverwerking in het kader van de Jeugdwet in de situatie waarbij een ander dan de gemeente, bijvoorbeeld een huisarts of gecertificeerde instelling) verwijst naar jeugdhulp waarvoor de gemeente financieel verantwoordelijk is.

4.5.1 Gegevensuitwisseling tussen de gemeente en de hulpverlener of maatwerkaanbieder ten behoeve van de opdrachtverstrekking en declaratie van te verlenen van zorg of een maatwerkvoorziening

Voor deze situatie zijn gemeenten in samenwerking met VNG en het ministerie van VWS bijvoorbeeld bezig met het inrichten van een gestandaardiseerd berichtenverkeer voor de Wmo. Dit voorziet erin dat de berichten gedefinieerd worden en een infrastructuur wordt ingericht.

Risico's

- De privacy-risico's die zich voor kunnen doen bij deze gestandaardiseerde berichtenstromen vallen buiten de scope van deze PIA.
- Één risico willen wij hier specifiek noemen. In veel gevallen zullen hulpverleners en aanbieders in hun facturen melding moeten maken van de persoon aan wie een voorziening is verstrekt en om welke voorziening het gaat. Zo kan de financiële afdeling bijvoorbeeld de rechtmatigheid van de factuur controleren. Hiermee ontstaat een risico dat er een (te) grote hoeveelheid gevoelige persoonsgegevens terecht komt in de financiële administraties van gemeenten. Hiermee doelen we niet zozeer op de inhoud van de declaraties, maar vooral op de wijze waarop gemeenten die inhoud zelf vastleggen en opslaan in de gemeentelijke (financiële) systemen. Hierbij hebben we in het achterhoofd dat financiële systemen niet altijd zodanig afgeschermd zijn als bij inhoudelijke systemen of systemen van wijkteams het geval is. Anders gezegd: door het vastleggen van inhoudelijke gegevens over hulp in financiële systemen, bestaat het risico dat deze gegevens als het ware (onbedoeld) 'weglekken' naar personen of gemeentelijke afdelingen waarvoor deze inhoudelijke gegevens bepaald niet bedoeld zijn (risico type A1, A3 en B).

Aanbevelingen

- Onderzoek hoe de gemeentelijke gegevensverwerking (de financiële systemen) die nodig is voor inzicht in verplichtingen, betaling en controle van facturen zodanig vorm gegeven kan worden dat deze met een minimum aan persoonsgegevens kan plaats vinden en (onbedoeld) 'weglekken' van inhoudelijke gegevens voorkomen wordt.

4.5.2 De gegevensverwerking ten behoeve van de regie op zorg bij een integrale aanpak

Het kabinetsbeleid vraagt van gemeenten om regie te voeren op de ondersteuning in situaties dat dit noodzakelijk is: één gezin, één plan, één regisseur. Om die regie te kunnen voeren zullen gemeenten en betrokken hulpverleners informatie moeten uitwisselen. Gemeenten maken hierin keuzen in de niveaus van informatie van de hulpverleners (de uitvoerders) waarover zij met het oog op regie willen beschikken. Grofweg is het een keuze tussen regievoering op basis van een plan en gegevensuitwisseling tussen gemeente en aanbieder met uitsluitend 'dat-gegevens' , of regievoering op basis van een dossier waarin ook inhoudelijke gegevens aangaande casus en uitvoering staan..

In het document 'Startnotitie Gegevensuitwisseling en Privacybescherming; één gezin, één plan, één regisseur' maken KING en VNG een duidelijk onderscheid tussen het plan op basis waarvan de gemeente regie voert en inhoudelijke dossiers. Als uitgangspunt wordt gehanteerd dat het plan op basis waarvan de gemeente regie voert in beginsel géén informatie over de achtergrond van de problematiek, inhoudelijke overwegingen vanuit de verschillende disciplines of hulpverleners of inhoudelijke behandelgegevens bevat. Deze informatie dient in de eigen dossiers van de verschillende hulpverleners te blijven[3]. VNG/KING definiëren in dit document de volgende set gegevens op basis waarvan gemeenten regie kunnen voeren:

- Personalia van het betrokken persoon/gezin
- Contactgegevens van de regisseur
- Afgesproken activiteiten, met per activiteit:
    - aard en (algemene) omschrijving van de activiteit,
    - begin en einddatum,
    - uitvoerende organisatie, gegevens van uitvoerder / contactpersoon,
    - is de activiteit afgerond,
    - Eventueel toelichtende opmerkingen over de activiteit of de voortgang.

Risico's

- Gemeenten die kiezen voor regie op basis van inhoudelijke dossiers lopen een groot risico dat zij meer gegevens wensen en vragen van hulpverleners en maatwerkaanbieders dan noodzakelijk en toegestaan is. Zij zullen daarin vaak te maken krijgen met beperkingen die aan hulpverleners zijn opgelegd met betrekking tot gegevensverstrekking vanwege bijvoorbeeld een beroepsgeheim. Kortom: gemeenten lopen het risico dat 'overvraagd' wordt en dat geheimhoudingsbepalingen (onnodig) onder druk komen te staan (risico type A1 en A3).

[3] Startnotitie Gegevensuitwisseling en Privacybescherming versie 1.5, 29 juli 2013, Den Haag

Aanbevelingen

- Sluit aan met betrekking tot de regie-informatie aan bij de gegevensset uit de startnotitie van KING/VNG.

4.5.3 Gegevensverwerking in het kader van de Jeugdwet in de situatie waarbij een jeugdhulpaanbieder hulp verleend op basis van een verwijzing door anderen dan de gemeente, waarvoor de gemeente financieel verantwoordelijk is

In de Jeugdwet is vastgelegd dat bijvoorbeeld huisartsen jeugdigen kunnen doorverwijzen naar jeugdhulp, waarna de betreffende instelling na een intake kan besluiten om jeugdhulp te gaan verlenen. De gemeente is verantwoordelijk voor de kosten van deze hulpverlening. Daarbij kan het van belang zijn voor de betreffende jeugdhulpaanbieder om gegevens uit te wisselen met de gemeente als er al verschillende trajecten bij het gezin van de jeugdige lopen en een integrale aanpak noodzakelijk wordt geacht.

In dit kader zijn er verschillende soorten gegevensuitwisseling te onderscheiden. De eerste is de administratieve melding van de instelling aan de gemeente dat jeugdhulp verleend zal worden aan een jeugdige en zijn of haar gezin. Dit zal in veel gevallen een melding zijn aan de afdeling die de contracten beheert of een financiële afdeling. Een tweede gegevensuitwisseling kan betrekking hebben op de inhoud van de te verlenen zorg, waarin de instelling contact zoekt met de gemeente (wijkteam) om af te stemmen over lopende trajecten vanuit de gemeente.

De routering en inhoud van deze berichtenstromen is nog niet uitgekristalliseerd. Gemeenten maken hierover afspraken in hun inkoopcontracten, of leggen vast dat hierover nog nadere afspraken gemaakt moeten worden.

Risico's

- Het risico bestaat dat er onnodig veel persoonsgegevens in de financiële of contractbeheeradministratie van de gemeente terecht komen. In veel gevallen zullen beveiliging van en toegang tot administratieve gegevens anders geregeld zijn, dan bij een team dat zich inhoudelijk met zorg bezig houdt. Er ontstaat dus tevens een risico dat meer mensen dan nodig toegang hebben tot deze gevoelige gegevens (risico type A1, A3 en B).
- Bij de gegevensverwerking die betrekking heeft op de afstemming tussen hulptrajecten bestaat het risico dat er meer inhoudelijke informatie uitgewisseld wordt dan strikt noodzakelijk is (risico type A3).

Aanbevelingen

- Maak afspraken tussen zorgverlener en gemeente over de inhoud van deze inhoudelijke meldingen. Sluit daarvoor aan bij hetgeen hiervoor gezegd is over regie – 'dat-gegevens' in plaats van 'wat-gegevens', en bij de aandachtspunten beschreven in par. 4.1 onder triage.

5 Inrichting van informatiesystemen, registratie, toegang, bewaren en vernietigen van gegevens

Algemene toelichting

De wijze waarop gemeenten hun informatiesystemen inrichten heeft potentieel grote impact op de risico's ten aanzien van de privacy van burgers. In dit onderdeel wordt gekeken naar verschillende keuzen die gemeenten maken bij de inrichting van die informatievoorziening. Hierbij komen de volgende aspecten aan de orde:

1. De mate van integratie en scheiding van dossiers.
2. De mate van integratie en scheiding in informatieniveaus.
3. De wijze waarop de toegang tot persoonsgegevens is georganiseerd
4. Het bewaren en vernietigen van persoonsgegevens

5.1 De mate van integratie en scheiding van dossiers

Bij de integratie van dossiers gaat het met name om de vraag hoe gemeenten hun ICT-systeem inrichten. Hierin is een hoofdindeling te maken tussen drie varianten:

- Volledig gescheiden domeindossiers.
- Koppelbare domeindossiers: Hierin is het mogelijk om bijvoorbeeld via een regiemodule, dossiers van dezelfde burger uit verschillende domeinen aan elkaar te koppelen.
- Volledig geïntegreerde domeindossiers: Hierbij bestaat er één integraal burgerdossier voor het hele sociale domein.

Specifieke aandacht vraagt in dit verband de omgang met wat wel gezinsdossiers[4] genoemd wordt. Een opvatting in de praktijk lijkt te zijn dat het kabinetsbeleid van één gezin, één plan, één regisseur tevens suggereert dat er sprake zou kunnen zijn van één integraal gezinsdossier. Dit achten we onjuist en ook een misvatting. Er kan sprake zijn van een hulpvraag of multi problematiek waardoor een het nodig is ok ook een dossier op gezinsniveau te hebben en inzicht te hebben in de samenstelling van het gezin.Echter dat in bepaalde situaties een dergelijk dossier noodzakelijk is, wil nog niet zeggen dat een algemene praktijk waarbij dossiers van gezinsleden standaard worden samengevoegd aangewezen of mogelijk is op basis vabn de wetgeving.

5.1.1 Volledig gescheiden domeindossiers

In deze variant is het niet mogelijk om dossiers van dezelfde burger uit verschillende domeinen geautomatiseerd aan elkaar te relateren. Gemeenten in deze situatie zitten vaak in het archetype 'Transitieproof'. Voor situaties waarin een integrale aanpak en vormen van regie noodzakelijk zijn maken zij gebruik van een regiemodule die los staat van de andere systemen, of ze geven dit vorm vanuit één van de domeinsystemen. Daar waar informatie uit andere domeinen nodig is, moeten zij bijvoorbeeld inloggen op het systeem van het desbetreffende domein en de noodzakelijke gegevens handmatig verwerken.

<u>Risico's</u>
In deze variant lijken de privacyrisico's op het eerste gezicht beperkt. Dat hoeft echter niet zo te zijn.

- Daar waar sprake is van een integrale aanpak, zullen medewerkers gegevens – al dan niet via email, en 'knippen en plakken' – overhevelen naar het domeinoverstijgende. Daarmee is niet alleen de kans op fouten groot, maar ontstaat ook het risico dat het zorgvuldig beheer van persoonsgegevens moeilijk wordt omdat deze op verschillende systemen zijn opgeslagen. Daarnaast is er een groter risico dan bij de andere varianten dat medewerkers uit gemaksoverwegingen bovenmatig gegevens over te hevelen (risico type A3).
- Bij veel domeinspecifieke systemen is er sprake van brede autorisaties op basis van functies. Alle medewerkers van een bepaalde afdeling, bijvoorbeeld het Wmo-loket hebben dan toegang tot alle klantdossiers van de afdeling. Hierdoor is het risico dat mensen onrechtmatig kennis nemen van dossiers groot (risico type A3 en B).

<u>Aanbevelingen</u>
- Besteed in training van medewerkers aandacht aan het gedrag ten aanzien van gegevens.
- Stuur er als management op dat medewerkers hooguit 'dat-gegevens' opnemen in een domein-overstijgend dossier, en geen 'wat-gegevens'.
- Overweeg om binnen de domeinspecifieke afdelingen middels het autorisatiebeleid de toegang tot persoonsgegevens meer te compartimenteren.

5.1.2 Koppelbare domeindossiers

In deze variant is het mogelijk om dossiers van dezelfde burger uit verschillende domeinen aan elkaar te koppelen Dit is technisch te realiseren met een regiemodule. Medewerkers hebben de keuze om indien de situatie dat vraagt, meerdere domeinen of leefgebieden aan te vinken in het kader van de behandeling van een specifieke hulpvraag en de daarbij behorende dienstverlening . Vervolgens krijgen ze indien ze daartoe

[4] Waar hier gesproken wordt van gezin, kan ook gelezen worden huishouden, of in het geval van gebroken gezinnen of jongerengroepen, 'de relevante groep'

geautoriseerd zijn, toegang tot gedefinieerde sets met persoonsgegevens in dat domein of leefgebied. Deze wijze van inrichting van het ICT-systeem faciliteert het triageproces zoals beschreven in paragraaf 4.1. Zij legt de verantwoordelijkheid bij de professional neer en maakt maatwerk mogelijk.

Risico's

- In deze variant is het gedrag van de medewerker een de belangrijkste factor. Het risico op schending van de privacy wordt bepaald door de kwaliteit en professionaliteit van de medewerkers, en de wijze waarop het management stuurt op een zorgvuldige omgang met persoonsgegevens (risico type A3).
- Met betrekking tot de toegang tot gegevens kan zich hier hetzelfde risico voordoen als genoemd bij volledig gescheiden dossiers.

Aanbevelingen

- Deze variant vraagt om controlemechanismen om misbruik snel te onderkennen. Een medewerker die bijvoorbeeld altijd alle leefgebieden aan vinkt, doet waarschijnlijk iets niet goed en is wellicht in overtreding wegens ongeoorloofd inzien van persoonsgegevens. Een medewerker die altijd alleen één leefgebied aan vinkt is wellicht te voorzichtig, of is niet alert op multiproblematiek.
- Met betrekking tot toegang tot gegevens is dezelfde als bij volledig gescheiden dossiers van toepassing.

5.1.3 Volledig geïntegreerde dossiers / gezinsdossiers

Deze variant past bij het streven naar een integraal klantbeeld onder alle omstandigheden en kan zich zelfs uitstrekken tot gezinsdossiers. Er is voor zover mogelijk, één integraal burgerdossier voor het hele sociale domein, en soms voor het gehele gezin. Medewerkers hebben geen, of slechts zeer beperkte mogelijkheden om een maatwerkomgeving te creëren tot de gegevens die ze nodig hebben en scheiding aan te brengen tussen dossiers van gezinsleden. Hetgeen overigens niet wil zeggen dat ze ook altijd alle gegevens zullen willen inzien.

Risico's

- Deze variant draagt grote risico's in zich ten aanzien van de privacy in zich ten opzichte van de andere twee varianten, omdat de afweging ten aanzien van noodzaak, subsidiariteit en proportionaliteit voor de toegang tot gegevens niet wordt gemaakt. Indien een burger een Wmo-voorziening krijgt, en ook over een bijstandsuitkering beschikt zou dit automatisch in hetzelfde dossier zichtbaar worden, ook als er geen sprake is van samenhang in problematiek. Indien er sprake is van een integraaal gezinsdossier zou dit ook gelden voor voorzieningen van andere gezinsleden. Daarmee voldoet deze wijze van dossiervoering niet aan de vereisten van regelgeving over het verwerken van persoonsgegevens en is er door één overkoepelend en omvattend dossier sprake van een te grote bemoeienis met het dagelijkse leven van de burger (risico type A1).

Aanbevelingen

- Stap van deze variant af en ontwikkel in de richting van 'koppelbare dossiers' zowel met betrekking tot de domeinen, als met betrekking tot de gezinsleden. Bij koppelbare dossiers blijven de dossiers van gezinsleden gescheiden, maar is het mogelijk om, indien de situatie dat vraagt, bij individuele dossiers aan te geven welke personen tot het gezin behoren. Voor de overkoepelende gezinsproblematiek die alle leden van het gezin aangaat is er soms wel de mogelijkheid om een gezinsdossier te maken. Het in stand houden van individuele dossiers is ook relevant onder andere met het oog op inzage en correctie-recht van personen. Indien een jongere inzage wil in zijn of haar dossier en dit is niet gescheiden van het dossier van de ouders, wordt de privacy van ouders wellicht geschonden, en krijgt deze wellicht toegang tot informatie die ook vanuit zorgoogpunt niet gewenst is.

5.2 De mate van integratie en scheiding in informatieniveaus

Bij de integratie en scheiding van informatieniveaus gaat het om de vraag in hoeverre verschillende typen informatie gescheiden worden opgeslagen en kunnen worden ontsloten. Naarmate de inrichting van het systeem hier meer mogelijkheden toe biedt is het mogelijk om de toegang tot informatie mee te laten lopen

met de rollen die een medewerker heeft in het werkproces. Waarbij er per definitie opgepast moet worden voor een te grote mate van fragmentatie.

In dit verband wordt gekeken naar de volgende mogelijke indelingen:

1. Scheiding van dat- en wat-informatie
2. Scheiding van informatieniveaus voor de verschillende fasen van het werkproces

5.2.1 Scheiding van wat en dat informatie

Bij de scheiding van dat- en wat informatie gaat het erom in hoeverre het mogelijk is voor een medewerker om eerst inzicht te krijgen in 'dat-gegevens' om vervolgens pas te beslissen of het nodig is om ook toegang te krijgen tot de wat-gegevens. Hierbij staan 'dat-gegevens' voor gegevens die aangeven dàt er sprake is van een bepaalde voorziening, bijvoorbeeld een Wmo-voorziening, en 'wat-gegevens' voor gegevens die informatie geven wat er om welke voorziening het gaat, of de meer inhoudelijke informatie over en problematiek.

Risico's

- Gemeenten die niet de mogelijkheid hebben om 'dat- en wat-gegevens' gescheiden te benaderen lopen een hoog risico dat medewerkers onnodig inzage hebben in inhoudelijke persoonlijke gegevens van burgers dan gemeenten waar dit onderscheid wel mogelijk is (risico type A1 en A3).

Suggestie

- De mogelijkheid om dat- en wat-gegevens apart te kunnen ontsluiten is van groot belang voor de borging van de privacy. Gemeenten moeten overwegen hun systemen aan te passen om deze mogelijkheid te creëren.

5.2.2 Scheiding van informatieniveaus voor de verschillende fasen van het werkproces

Voor het standaardwerkproces van gemeenten in het sociaal domein hanteert KING de fasering zoals beschreven in deel 1:

- Klantcontact en intake
- Behoeftebepaling en planvorming
- Besluitvorming
- Uitvoering en levering
- Regievoering

In hoofdstuk 3 hebben in paragraaf 3.3, verticale integratie van taken aangegeven dat de rollen van medewerkers van de gemeente gaandeweg het proces kunnen verschuiven, bijvoorbeeld van diagnosesteller en planmaker naar beslisser en regisseur. Hierbij kan het ook zo zijn dat in de verschillende fasen een andere medewerker de rol invult.

Met de verschillende rollen in het werkproces hangt ook samen dat de noodzakelijke toegang tot gegevens kan verschillen. Niet alle informatie die nodig is voor het maken van de diagnose en de planvorming hoeft door naar de beslisser, of is noodzakelijk voor het voeren van regie. Naarmate een gemeente het mogelijk maakt om gegevens langs deze lijnen in te richten, informatie op maat te ontsluiten voor de fase van het werkproces, des te beter de privacy kan worden geborgd. Dit kan met name van belang zijn in situaties waarbij de opeenvolgende rollen ingevuld worden door andere medewerkers.

Risico's

- Gemeenten waar het niet mogelijk is om de toegang tot persoonsgegevens af te stemmen op de rol van de betreffende medewerker lopen een verhoogd risico dat bij overdracht van een cliënt naar een volgende fase de collega die de cliënt overneemt onnodig veel persoonsgegevens in kan zien (risico type A3).

Aanbevelingen

- Pas de inrichting van het systeem zodanig aan dat toegang tot gegevens afgestemd kan worden op de taak en rol die een medewerker vervult in het proces.

5.3 De wijze waarop de toegang tot persoonsgegevens is georganiseerd

In deze paragraaf gaan we in op de vraag wie toegang hebben tot de gegevens van een burger. In dit verband zijn er ook gemeenten die experimenteren met het beheer van eigen dossiers door burgers zelf. Deze ontwikkeling laten we hier buiten beschouwing.

We kijken in dit verband naar drie veelvoorkomende autorisatieniveaus:

- Autorisatie op basis van functie
- Autorisatie op teamniveau
- Autorisatie op basis van betrokkenheid

5.3.1 Autorisatie op basis van functie

Bij autorisatie op basis van functie hebben alle medewerkers met een bepaalde functie toegang tot de voor die functie relevante persoonsgegevens van alle burgers. Deze variant is gebruikelijk bij afdelingen waar 'productie wordt gedraaid', en mensen makkelijk dossiers van elkaar moeten kunnen overnemen. Bij veel afdelingen sociale zaken is autorisatie op dat niveau ook geregeld. Hetzelfde geldt voor bijvoorbeeld ambtenaren van de burgerlijke stand. Iedere ambtenaar van de burgerlijke stand moet daarbij de akte kunnen maken (en de daarvoor benodigde gegevens en eventuele eerdere akten kunnen raadplegen) die in een bepaald geval nodig is.

Risico's

- In deze variant hebben veel mensen toegang tot persoonsgegevens van cliënten waar zij geen betrokkenheid bij hebben. Dit draagt het risico in zich dat mensen onrechtmatig kennis nemen van dossiers (risico type A1 en A3).

Aanbevelingen

- Stap tenminste over naar autorisaties op teamniveau en overweeg om over te stappen naar autoriusaties op basis van betrokkenheid.
- Maak gebruik van logging-systematieken die signalen afgeven wanneer mensen persoonsgegevens inzien van cliënten waar zij niet bij betrokken zijn. Evalueer deze signalen regelmatig. Tref sancties als blijkt dat inzagen inderdaad onrechtmatig waren.

5.3.2 Autorisatie op teamniveau

Bij autorisatie op teamniveau hebben de leden van een specifiek team, bijvoorbeeld een wijkteaml team, toegang tot de dossiers van elkaars cliënten. Het onderscheid met de autorisatie op functie is dat de schaal meestal kleiner is. Veel gemeenten met wijkteams lijken voor deze variant te kiezen, warbij een team ca. 10 leden kent. De achtergrond van deze autorisatie ligt dan in het feit dat teamleden verschillende aandachtsgebieden hebben en door gemeenschappelijke toegang elkaar makkelijk kunnen interviseren, en dat men makkelijk voor elkaar moet kunnen inspringen bij ziekte en verlof. Ook speelt hier dat bij wijkteams de schaal dusdanig beperkt is dat iedereen elkaars cliënten toch wel min of meer kent.

Risico's

- Hier speelt hetzelfde risico als bij autorisatie op basis van functie, zij het in (sterk) verminderde mate (risico type A3) .

Aanbevelingen

- Maak gebruik van logging-systematieken die signalen afgeven wanneer mensen persoonsgegevens inzien van cliënten waar zij niet bij betrokken zijn. Evalueer deze signalen regelmatig. Tref sancties als blijkt dat inzagen inderdaad onrechtmatig waren.
- Overweeg om over te stappen naar autorisaties op basis van betrokkenheid.

5.3.3 Autorisatie op basis van betrokkenheid

Bij autorisatie op basis van betrokkenheid heeft elke medewerker alleen toegang tot de persoonsgegevens van zijn of haar eigen cliënten. Gemeenten die hiervoor kiezen doen dit voornamelijk uit privacyoverwegingen. Door de toegang tot gegevens te koppelen aan individuele medewerkers beperken ze het risico van onrechtmatig inzien van gegevens.

Risico's

- De risico's uit de andere twee varianten zijn bij deze variant geminimaliseerd.
- Er kan zich wel een hulprisico voordoen. Namelijk dat bij plotselinge afwezigheid van een van de medewerkers collega's niet bij gegevens kunnen terwijl dit wel noodzakelijk is. Bijvoorbeeld bij crisissituaties.

Aanbevelingen

- Overweeg de volgende oplossing die ook wel bekend staat als 'Breaking the Glass' In een concrete uitwerking krijgen medewerkers die toegang zoeken tot het dossier van de cliënt van een collega een mededeling dat ze niet geautoriseerd zijn en slechts toegang krijgen na het invullen van de reden waarom ze toegang willen hebben. Dit wordt gelogd en er gaat een signaal naar de teamleider of aangewezen teamlid. Deze werkwijze maakt het mogelijk om in specifieke situaties toch toegang aan andere medewerkers te verlenen en dit tegelijkertijd te monitoren en controleren. Deze werkwijze is gebaseerd op procedures die in de medische sector gebruikt worden als er bijvoorbeeld sprake is van vervanging, van weekenddienst of bij bezoek van een huisartsenpost.

5.4 Bewaren en vernietigen van persoonsgegevens

Met betrekking tot het bewaren en vernietigen van persoonsgegevens kunnen zich dilemma's voordoen in de situaties waarin een casus (gedeeltelijk) wordt afgesloten. Bij multiprobleemsituaties speelt de dienstverlening zich af in meerdere domeinen, en is er daarnaast sprake van overkoepelende regie-informatie. Voor zover persoonsgegevens gesplitst zijn naar de verschillende domeinen, kan voor de bewaartermijnen in dat betreffende domein de geldende materiewetgeving leidend zijn. Echter voor de gegevens in het integrale plan, en de regie-informatie is dat minder duidelijk..

Risico's

- Gegevens worden langer bewaard dan wettelijk toegestaan is, en/of noodzakelijk is (risico type A1 en A3).
- Gegevens worden korter bewaard dan wettelijk wordt vereist (risico type A1).
- Gegevens worden vernietigd, terwijl het van belang is om de casus nog enige tijd te volgen met het oog op gevaar van hernieuwde problematiek of nieuwe hulpvragen.

Aanbevelingen

a. Breng zoveel mogelijk een scheiding aan tussen enerzijds domeinspecifieke gegevens die bijvoorbeeld opgeslagen kunnen (kunnen) worden in de back-office systemen van het betreffende domein, en anderzijds 'toegangs- of regie-informatie' die beschikbaar moet zijn in het systeem van de wijkteams. Op die manier wordt het mogelijk om voor de domeinspecifieke gegevens, nauwkeuriger de regels toe te passen van de betreffende domeinwetgeving.
b. Maak bij het afsluiten van een casus of een deel van de casus een afweging welke gegevens voor welke periode in het regiesysteem bewaard moeten worden met het oog op mogelijke vervolgvragen of terugval. Maak deze afweging expliciet en verifieerbaar. En bouw in het systeem in dat na verloop van die periode een nieuwe afweging gemaakt moet worden.

c. Sluit voor de maximumtermijn voor systemen voor wijkteams (toegang, triage en regie) aan bij de kabinetsvisie waarin voor dit soort situaties een maximumtermijn van 5 jaar genoemd, gebaseerd op de ervaringen van het programma 'Integrale aanpak'.
d. .

6. Transparantie en positie van de burger

Algemene toelichting
Transparantie over het gebruik van persoonsgegevens is een belangrijk onderdeel van het borgen van de privacy, zeker in de situatie waarin gemeenten meer dan voorheen persoonsgegevens met betrekking tot de zorg van burgers zullen verwerken. In het kader van deze rapportage hebben we met name gekeken naar de wijze waarop gemeenten vorm geven aan transparantie en de positie van de burger met betrekking tot gegevensverwerking en privacy tijdens het gemeentelijk dienstverleningsproces in het sociaal domein.

Hierbij komen met name twee aspecten in beeld:

1. De positie van de burger tijdens het dienstverleningsproces in relatie tot gegevensverwerking
2. Informatie aan de burger met betrekking tot zijn of haar rechten en plichten in het kader van de gegevensverwerking in het sociale domein.

6.1 De positie van de burger tijdens het dienstverleningsproces

Een belangrijke doelstelling van de decentralisaties is gericht op het versterken van de zelfredzaamheid van de burger. Hierbij passen termen als 'de burger in de eigen kracht zetten'. Onderdeel daarvan behoort te zijn dat de gemeente transparant is naar de burger over de gegevens zij wil verwerken, de noodzaak en het doel daarvan.

Risico's
- Het risico is dat gemeenten deze transparantie geen onderdeel maken van hun werkproces. De burger kan dan niet precies weten welke persoonsgegevens wanneer door wie waarvoor worden verwerkt, en kan daardoor ook niet effectief gebruik maken van zijn of haar rechten (risico type B).

Aanbevelingen
- Maak gebruik van de aanbevelingen gedaan in hoofdstuk 4 ten aanzien van triage en de afwegingen met betrekking tot gegevensverwerking. Betrek de burger actief bij deze afwegingen.

6.2 Informatie aan de burger met betrekking tot rechten en plichten

De privacywetgeving schrijft voor dat burgers geïnformeerd worden als de overheid persoonsgegevens van hen wil registreren en verwerken, en dat ze geïnformeerd worden over hun rechten en plichten. De kabinetsvisie 'Zorgvuldig en bewust' over Privacy in het sociaal domein benadrukt het belang van transparantie naar de burger en de noodzaak om de drempel naar uitoefening van zijn rechten laagdrempelig te maken. Juist in de huidige situatie waarin meer gegevens verwerkt gaan worden door gemeenten. De praktijk bij gemeenten aangaande het informeren van burgers op dit vlak varieert.

Risico's
- Burgers worden tijdens het dienstverleningsproces te weinig of niet geïnformeerd ten aanzien van hun rechten en plichten in het kader van gegevensverwerking (risico type B).
- Er zijn geen processen en procedures ingericht voor de situatie waarin een burger gebruik wil maken van zijn of haar rechten met betrekking tot bezwaar, inzage of correctie, waardoor deze rechten slechts met grote moeite geëffectueerd kunnen worden (risico type B).
- Medewerkers zijn niet op de hoogte van de rechten van burgers met betrekking tot privacy en gegevensverwerking, en de daarvoor ingerichte processen, waardoor deze slechts met grote moeite geëffectueerd kunnen worden (risico type B).

Aanbevelingen

- Maak de communicatie over de rechten van de cliënt met betrekking tot privacy en gegevensverwerking een expliciet onderdeel van het werkproces en besteed aandacht hieraan in training en bewustwording van medewerkers.
- Richt processen en procedures in, zodat burgers die gebruik willen maken van hun rechten laagdrempelig en snel geholpen kunnen worden.
- Monitor de wijze waarop in de praktijk invulling gegeven wordt aan de rechten van de burger met betrekking tot gegevensverwerking. Neem dit mee in de managementrapportages bijvoorbeeld door te rapporteren over het aantal bezwaarschriften, beslissingen om tegen de wil van betrokkenen gegevens te verwerken, verzoeken om inzage, correctie, gehonoreerde en afgewezen verzoeken en analyse van de redenen voor afwijkingen. Maak dit onderdeel van de verantwoording aan de raad over gegevensverwerking en privacy in het sociaal domein.
- Borg in contracten met samenwerkings- en contractpartners die taken uitvoeren namens de gemeente dat zij in de uitvoering van deze taken de burger actief informeren over rechten en plichten met betrekking tot privacy en gegevensverwerking en laat hen hierover rapporteren.
- Zorg voor actieve voorlichting aan burgers omtrent hun rechten ten aanzien van gegevensverwerking.

7. Kennis en bewustwording van medewerkers

Algemene toelichting

Uit de voorgaande hoofdstukken van deze rapportage is duidelijk geworden dat mate waarin burgers hun privacy geborgd weten in belangrijke mate bepaald wordt door de kwaliteit en de professionaliteit van de medewerkers en de wijze waarop gestuurd wordt door de organisatie op een zorgvuldige omgang met persoonsgegevens.

Op dit moment staan gemeenten aan het begin van de nieuwe werkwijzen en taken in het sociaal domein. Het ‘vak’ van wijkteammedewerker of medewerker ‘integraal team’ is nog relatief nieuw. Vaak komen de medewerkers in deze teams uit een van de specifieke domeinen Jeugd, Wmo, of Werk en Inkomen. Er zijn nog slechts beperkt professionele standaarden voor handen, ook met betrekking tot privacy en gegevensverwerking.

Risico’s

- Door gebrekkige kennis over privacy en gegevensverwerking in relatie tot het eigen werk, wordt de zorgvuldige omgang met persoonsgegevens onvoldoende intrinsiek onderdeel van de dagelijkse professionele praktijk. Daardoor is de kans groot dat onnodig of bovenmatig gegevens uitgevraagd en geregistreerd worden en/of dat er onvoldoende aandacht is voor de rechten van de burger. De burger loopt daarmee het risico dat zijn of haar privacy wordt geschonden. De gemeente loopt daarmee het risico dat gegevens onrechtmatig worden verwerkt (risico type A2 en A3).
- Omgekeerd kan het betekenen dat medewerkers zich teveel laten belemmeren in hun werk door onnodige angst de privacy-regels te schenden, waardoor probleemsituaties te laat of pas in een laat stadium zichtbaar worden en kunnen worden aangepakt (risico type A2).
- Door gebrek aan kennis in de organisatie over privacy en gegevensverwerking in relatie tot de dienstverlening in het sociaal domein, wordt de kwetsbaarheid van medewerkers vergroot. Bij complexe of zwaarwegende afwegingen ten aanzien van de omgang met gegevens, kunnen medewerkers bijvoorbeeld niet terug vallen op deskundige ondersteuning. Ook ontstaat er een risico dat op verschillende plaatsen in de organisatie verschillend wordt omgegaan met privacy-issues (risico type A3 en B).

Aanbevelingen

- Besteed in training en opleiding van medewerkers aandacht aan het thema privacy en gegevensverwerking en hoe medewerkers de privacy van hun cliënten kunnen borgen in de manier van werken.
- Overweeg om specifieke expertise te organiseren in de organisatie, om medewerkers te adviseren bij lastige afwegingen in het kader van privacy en gegevensverwerking.

8. Beleid voor Privacy en verwerking van persoonsgegevens in het Sociaal domein

Algemene toelichting

Het is gebruikelijk om een Privacy Impact Assessment en rapportage daarover te beginnen met het beleid ten aanzien van privacy. Wij hebben ervoor gekozen om dit het sluitstuk van de PIA te maken. De reden daarvoor is dat het opstellen van een overkoepelend privacy-beleid voor het sociaal domein nog niet gebruikelijk is bij gemeenten, waarbij de nadruk op dit moment op de transitie ligt. De nieuwe praktijk dient zich ook nog te ontwikkelen. En waar er geen beleid is, is het van belang een tweesporenbeleid te volgen: richting geven aan de praktijk in ontwikkeling zodat de materiële borging van de privacy al in gang wordt gezet, om vervolgens een en ander te borgen in een formeel door de Raad goedgekeurd beleid. De omgekeerde volgorde zou er slechts toe leiden dat de praktijk gaat zitten wachten tot er een keer beleid is.

Veel gemeenten zijn de afgelopen jaren wel gestart met een informatieveiligheidsbeleid, mede onder invloed van de resolutie die daartoe is aangenomen tijdens de Bijzondere Algemene Ledenvergadering van de VNG in november 2013, de oprichting van een Informatiebeveiligingsdienst bij KING en de Task Force bestuurlijke Informatieveiligheid Dienstverlening in opdracht van de minister van Binnenlandse Zaken.

In de kabinetsvisie 'Zorgvuldig en bewust' stelt het kabinet dat het College van B&W verantwoording moet afleggen aan de Raad hoe zij omgaat met gegevensverwerking en privacy. Om op een goede manier verantwoording af te kunnen leggen is een beleid op dit punt onontbeerlijk. Een dergelijk beleid kan tevens een overkoepelend kader bieden voor de thema's die in deze PIA-rapportage zijn besproken.

Risico's

- Bij gebrek aan beleid biedt de gemeente geen transparantie aan haar burgers over de vraag hoe zij in het algemeen denkt over privacy, hoe zij de privacy probeert te borgen en hoe zij daar op wil sturen. Hiermee ontstaat het risico van een toenemend wantrouwen in de overheid (risico type B).
- Zonder beleid is verantwoording afleggen aan, en controle door de gemeenteraad op de wijze waarop het College omgaat met privacy moeilijk. En daar waar de overheid geen verantwoording aflegt over har gedrag ten aanzien van de privacy van burgers neemt het risico op wantrouwen in diezelfde overheid toe (risico type B).
- Op verschillende plekken in de organisatie wordt verschillend met privacy omgegaan. Daardoor is er onduidelijkheid waar de privacyrisico's zitten, hoe het College hierop kan sturen, en ontstaat er rechtsongelijkheid voor de burger binnen eenzelfde gemeente (risico type A3 en B).
- Er is onvoldoende duidelijkheid wat men in contracten en convenanten met partners moet/wil afspreken ten aanzien van privacy en gegevensverwerking. Hierdoor ontstaat het risico dat noodzakelijke afspraken niet of onvoldoende worden gemaakt en de privacy van burgers niet adequaat is geborgd (risico type A3 en B).
- Zonder privacybeleid zijn er ook geen kaders voor training en bewustwording van medewerkers, en de wijze waarop de gemeente de burger in staat wil stellen om zijn of haar rechten met betrekking tot privacy en gegevensverwerking te effectueren. Hiermee is het risico groot dat privacy in de praktijk onvoldoende wordt geborgd, en gegevensverwerkingen onrechtmatig zijn (risico type B).

Aanbevelingen

- Begin zo snel mogelijk met het gestructureerd oppakken van de aanbevelingen in deze rapportage, met het oog op een zorgvuldige en bewuste praktijk.
- Ontwikkel indicatoren waaruit de zorgvuldige omgang met gegevens en de borging van de privacy blijkt. Denk hierbij aan klachten van burgers, verzoeken om inzage en correctie, en mate waarin die zijn gehonoreerd, aantal keren dat besloten is om tegen de wil van betrokkenen gegevens uit te wisselen, en controle op logging van gebruik van persoonsgegevens.
- Start in de loop van 2015 met het opstellen van een overkoepelend privacybeleid, tenminste voor het sociaal domein. Dit kan meer samenhang, eenduidigheid en transparantie brengen voor privacy en ook het lerend vermogen van de organisatie op dit punt vergroten.
- Laat het beleid vaststellen door de Raad en leg hierover verantwoording af aan de Raad.