gemeente Tynaarlo

pro facto

juridisch en bestuurskundig
onderzoek / advies / onderwijs

Rekenkameronderzoek gemeente Tynaarlo

Privacy in het sociaal domein: nice tot know or need to know?

Groningen, februari 2017

Heinrich Winter
Sylvia Huberts

ADRES
Pro Facto
Ossenmarkt 5
9712 NZ Groningen
EMAIL
profacto@pro-facto.nl
INTERNET
www.pro-facto.nl

rijksuniversiteit groningen

Inhoud

1

Inleiding

1.1 Aanleiding

Sinds de decentralisaties per 1 januari 2015 zijn de gemeentelijke taken binnen het sociaal domein fors uitgebreid. Niet alleen nieuwe taken op grond van de Wet maatschappelijke ondersteuning 2015 (Wmo 2015), maar ook de verantwoordelijkheid voor de uitvoering van de Jeugdwet per die datum, hebben voor een geheel andere uitvoeringspraktijk bij gemeenten gezorgd. Veel gemeenten zetten sociale (wijk)teams in om de zorg en ondersteuning van burgers zo effectief en efficiënt mogelijk te organiseren. De gemeente Tynaarlo kent ook drie van dergelijke teams (in Vries, Zuidlaren en Eelde-Paterswolde). De uitbreiding van de taken binnen het sociaal domein, in combinatie met het werken vanuit een sociaal team en het aangaan van samenwerkingsverbanden met aanzienlijk meer ketenpartners, leidt tot een forse toename van privacygevoelige gegevensdeling en -verwerking. Het betreft gegevens van uiteenlopende aard over zorgvragers, maar met het oog op het steeds belangrijker wordende sociaal netwerk, ook gegevens van personen rondom deze zorgvragers. De vraag is op welke wijze gegevensverwerking zich verhoudt tot de bescherming van de privacy van de doelgroepen binnen het sociaal domein.

Het belang van een goede gegevensuitwisseling en daarmee een meer efficiënte en effectieve dienstverlening moet altijd worden afgewogen tegen het (privacy)belang van een betrokkene.[1] Die afweging is vaak lastig en levert verschillende dilemma's op in de uitvoeringspraktijk. Een voorbeeld daarvan is de geïntegreerde probleemaanpak bij gezinnen (of personen) die meerdere problemen (financieel, gezondheid, werkloos) hebben. Om deze gezinnen zo efficiënt en effectief mogelijk te helpen worden gegevens gedeeld met meerdere organisaties. Het dilemma dat hierbij ontstaat is: welke gegevens mogen gedeeld worden met andere organisaties? De gegevens van de burger mogelijk namelijk niet verder worden verwerkt dan het doel waarvoor zij zijn verstrekt, als ze toereikend en ter zake dienend en niet bovenmatig zijn.[2] De gemeente zal de balans moeten vinden tussen de verwerking van gegevens ten behoeve van een goede dienstverlening aan de ene kant en de bescherming van de privacy van de burgers aan de andere kant. Integriteit van handelen is belangrijk in het kader van gegevensverwerking en de bescherming van de privacy. De integriteit van de overheid en haar functionarissen is belangrijk omdat zij een belangrijke en ingrijpende rol

[1] Deze tekst is deels ontleend aan een onderzoeksopzet van de Rekenkamercommissie van Amsterdam.
[2] Minister van Binnenlandse Zaken en Koninkrijkrelaties, Visiebrief digitale overheid 2017, 23 mei 2013.

spelen in het leven van burgers.[3] Vastgelegde procedures, protocollen en processen dragen bij aan het bevorderen van de integriteit.

1.2 Opdrachtomschrijving

De rekenkamercommissie van de gemeente Tynaarlo heeft Pro Facto in maart 2016 opdracht gegeven voor het uitvoeren van een rekenkameronderzoek naar de doeltreffendheid en de doelmatigheid van het beleid en de uitvoeringspraktijk rond privacy binnen het sociaal domein.

In dit rekenkameronderzoek staat de volgende centrale onderzoeksvraag centraal:

Zorgt het college van B&W er voldoende voor dat zich binnen het sociaal domein een praktijk ontwikkelt waarin een balans wordt gevonden tussen gegevensverwerking en de bescherming van privacy van de burger?

De doelstelling van het onderzoek is daarmee tweeledig. In de eerste plaats is het doel te komen tot een beschrijving van het beleid betreffende de privacy in het sociaal domein en van de afspraken die hierover zijn gemaakt tussen de gemeente en ketenpartners. In de tweede plaats wordt vervolgens gekeken naar de vraag óf en de wijze waarop volgens deze afspraken wordt gehandeld. Hierbij wordt eveneens ingegaan op de problemen die zich hierbij voordoen. Van belang is dat enkel is gekeken naar de taken die de gemeente heeft op grond van de Jeugdwet en de Wet maatschappelijke ondersteuning 2015 (Wmo 2015).

De centrale onderzoeksvraag mondt uit in een viertal thema's en bijbehorende deelvragen.

Thema 1: Privacybeleid en de toepassing daarvan binnen het sociaal domein

1. Welke visie heeft het college van B&W op de balans tussen gegevensverwerking en de bescherming van de privacy binnen het sociaal domein?
2. In welke mate is binnen de gemeente Tynaarlo beleid vastgelegd over de bescherming van de privacy binnen het sociaal domein? Voldoet dit beleid aan wet- en regelgeving?
3. Wordt uitvoering gegeven aan het opgestelde beleid? Zo nee, waarom niet?
4. In hoeverre wordt binnen de sociaal teams en door betrokken ketenpartners voldoende integer gehandeld? En zijn betrokkenen voldoende integriteitsbewust?
5. Welke hiaten vertoont het beleid rondom privacy binnen het sociaal domein? En worden deze ook in de praktijk opgemerkt?
6. Welke toekomstige ontwikkelingen zijn van belang voor het te (her)formuleren beleid?

Thema 2: Gegevensverwerking en privacybescherming

7. Welke risico's vallen aan te wijzen als het gaat om gegevensverwerking binnen het sociaal domein en de bescherming van de privacy?
8. Heeft de gemeente deze risico's en eventueel daarop te nemen maatregelen voldoende in kaart gebracht?
9. Welke afspraken heeft de gemeente met ketenpartners gemaakt wat betreft privacy? Geldt er bijvoorbeeld een privacy protocol en geldt dat voor alle ketenpartners?

[3] Bureau Integriteitsbevordering Openbare Sector: https://www.integriteitsoverheid.nl/over-bios/wat-is-integriteit/

Zijn de verantwoordelijkheden wat betreft de borging van de privacy voldoende duidelijk? Ook in die gevallen waarin eventueel sprake is van mandaat?
10. Welke maatregelen worden wat betreft privacy binnen het sociaal domein toegepast en dragen deze voldoende bij aan een balans tussen gegevensverwerking en de bescherming van de privacy? Zijn er ten aanzien van bijvoorbeeld het administratieve proces voldoende waarborgen ingebouwd?
11. Welke toekomstige ontwikkelingen zijn van toepassing wat betreft door de gemeente lopen risico's en eventueel te nemen maatregelen?

Thema 3: De rol van de gemeenteraad

12. Welke sturingsmogelijkheden en –instrumenten zet de raad in de praktijk in om zijn controlerende en kaderstellende rol aangaande het privacybeleid in te vullen?
13. Welke knelpunten worden door de raad ervaren als het gaat om sturing en controle op het privacybeleid binnen het sociaal domein?
14. Wordt de raad voldoende door het college in de gelegenheid gesteld om te sturen en te controleren?
15. Is de raad tevreden over de praktijk wat betreft de wijze waarop aan bescherming van de privacy wordt gedaan? Zo nee, waarom niet?
16. Welke toekomstige ontwikkelingen zijn van belang wat betreft de kaderstellende en controlerende rol van de raad?

Thema 4: Conclusies en aanbevelingen

17. Kan het huidige privacybeleid als doeltreffend en doelmatig worden beschouwd?
18. Wat zijn de leerpunten voor verbetering van het privacybeleid binnen het sociaal domein?
19. Welke stappen kunnen worden gezet om te komen tot een betere balans tussen gegevensverwerking en de bescherming van de privacy?
20. Welke eventuele lessen kunnen worden getrokken wat betreft de kaderstellende en controlerende rol van de raad?
21. Welke toekomstige ontwikkelingen dienen nauwlettend in de gaten te worden gehouden, zodat het college van B&W en de raad hierop een lokale visie ontwikkelen?

1.3 Aanpak

Het onderzoek is uitgevoerd in de periode van april 2016 tot en met oktober 2016 en kende de volgende onderzoeksactiviteiten:

- Startbijeenkomst
- Documentstudie
- Interviews
- Groepsgesprek met de raad
- Voortgangsbijeenkomsten met de rekenkamercommissie

1.4 Deze rapportage

In hoofdstuk 2 van deze rapportage wordt allereerst het wettelijk kader rondom privacyregelgeving geschetst. Aan bod komt voorts de visie van het college van B&W, alsmede de vraag naar de wijze waarop privacybelangen binnen het beleid aandacht hebben gekregen.

Beoordeeld wordt in hoeverre het gemeentelijke beleid aan de wettelijke kaders voldoet. In dit hoofdstuk wordt ook gewezen op toekomstige ontwikkelingen, waaronder de komst van een Europese privacyverordening, die van belang kunnen zijn voor te ontwikkelen beleid.

Hoofdstuk 3 beschrijft de wijze waarop gegevensverwerking in de praktijk plaatsvindt en of uitvoering wordt gegeven aan het beleid, alsmede de verhouding tussen de risico's van gegevensverwerking en de binnen de gemeente Tynaarlo gehanteerde waarborgen. Hiertoe zal ook aandacht worden geschonken aan de met ketenpartners gemaakte afspraken en de vraag naar naleving van die afspraken.

De rol van de gemeenteraad komt aan bod in hoofdstuk 4. Gekeken wordt naar de formele rol die de gemeenteraad heeft ten aanzien van privacybeleid binnen het sociaal domein en hoe deze in de praktijk wordt ingevuld.

Tot slot volgen conclusies en aanbevelingen in hoofdstuk 5.

1.5 Tot slot

De taakuitbreiding binnen het sociaal domein bracht voor gemeenten verschillende nieuwe en ingrijpende uitdagingen met zich mee. Met de uitbreiding van de Wmo 2015 en de Jeugdwet kwamen privacy vragen nog indringender op het bordje van de gemeente terecht. Het is niet vreemd dat niet meteen alles goed ging. Onderzoek van de Autoriteit Persoonsgegevens bracht aan het licht dat binnen een steekproef van gemeenten het merendeel van de onderzochte gemeenten tekortkomingen vertoonde op dit punt. Het is niet moeilijk bij een willekeurige gemeente te wijzen naar wat er aan schort. De insteek van dit rekenkameronderzoek was dan ook niet om de vinger op de zere plek te leggen en zout in de wonden te wrijven. De ambitie van onderzoekers en rekenkamercommissie was te beschrijven hoe het zit met privacy in het sociaal domein, in beleid, in de praktijk en bij de sturing, om vervolgens adviezen te kunnen doen die leiden tot verbetering. Het gaat daarbij eerder om een gezamenlijke zoektocht naar oplossingen, dan om toezicht en controle.

2

Het privacybeleid

2.1 Inleiding

Dit hoofdstuk gaat in op de vraag of en in hoeverre de gemeente Tynaarlo, met het oog op de binnen het sociaal domein uit te voeren taken, privacybeleid heeft vastgelegd en of daaraan uitvoering wordt gegeven. Met andere woorden: neemt de gemeente zijn verantwoordelijkheid op het gebied van de bescherming van de privacy? In dit verband wordt allereerst het wettelijk kader rondom het verwerken van gegevens geschetst, opdat beoordeeld kan worden in hoeverre het gemeentelijke beleid daaraan voldoet.

2.2 Kabinetsvisie en wettelijk kader

2.2.1. Inleiding

In deze paragraaf wordt stilgestaan bij de Kabinetsvisie op gegevensverwerking binnen het sociaal domein en het wettelijk kader betrekking hebbende op het verwerken en verstrekken van persoonsgegevens.

2.2.2. Kabinetsvisie Zorgvuldig en Bewust

In het kader van gegevensverwerking in het sociaal domein is allereerst de Kabinetsvisie 'Zorgvuldig en Bewust' van belang.[4] Hieruit blijkt dat de wijze van gegevensverwerking is neergelegd in algemene regelgeving over het verwerken van persoonsgegevens en dat de sectorwetgeving (waarmee onder andere de Wet maatschappelijke ondersteuning 2015 en de Jeugdwet worden bedoeld) aanvullende regelgeving bevat.

Uit de Kabinetsvisie blijkt dat een van de uitgangspunten van de decentralisatiewetten de betrokkenheid van de burger en zijn omgeving bij het tot stand komen van ondersteuning in het sociaal domein betreft. Dit betekent dat de ondersteuning en de daarvoor noodzakelijke gegevensverwerking in de regel in samenspraak met de betrokkene(n) zou moeten plaatsvinden. De overheid heeft de plicht om terughoudend te werk te gaan met de uitvraag en registratie van persoonsgegevens. Zij is dan gehouden aan de in de Wet bescherming persoonsgegevens (hierna: de Wbp) neergelegde criteria van noodzaak, subsidiariteit en proportionaliteit.

[4] Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Zorgvuldig en Bewust: Gegevensverwerking en Privacy in een gedecentraliseerd sociaal domein, 1 mei 2014.

Ten aanzien van gegevensverwerking wordt in de Kabinetsvisie uitgegaan van de volgende algemene uitgangspunten:

1. De Wbp is leidend;
2. Hergebruik van gestandaardiseerde gegevens voor standaardprocessen en voorzieningen moet geregeld zijn in de betreffende sectorale wet- en regelgeving, op basis van wederkerigheid;
3. Richting geven aan een lerende praktijk;
4. De ruimte voor gegevensverwerking en uitvraag moet zijn ingebed in een zorgvuldig triageproces om bovenmatige en onnodige gegevensdeling en uitvraag te voorkomen;
5. Versterking van de positie van de burger;
6. Het college van B&W is verantwoordelijk voor de zorgvuldigheid van gegevensverwerking die door of namens de gemeente plaatsvindt. Zij stelt eisen aan beveiliging en borging van de privacy. Het college is voor de wijze waarop het hieraan invulling geeft verantwoording verschuldigd aan de raad.

Het laatste kernpunt beoogt om de afspraken die gemeenten maken over gegevensverwerking en privacy transparant te maken en onderdeel van het lokale democratische proces. Voor zover de gemeente haar taken in samenwerking uitvoert, is het college ervoor verantwoordelijk dat gegevensverwerking is ingebed in een zorgvuldig proces van triage en dat hierover afspraken met samenwerkingspartners worden gemaakt. Cliëntorganisaties kunnen hierbij een adviserende rol invullen. Door het college van B&W verantwoording af te laten leggen aan de raad ontstaat zicht op de uitvoeringspraktijk en wordt deze zichtbaar, controleerbaar en evalueerbaar.[5]

2.2.3. Wet bescherming persoonsgegevens

De Wbp vormt de wettelijke basis voor gegevensverwerking en -verstrekking in het algemeen. Uitgangspunt van de Wbp is dat gegevens *zorgvuldig* moeten worden verwerkt en dat zo precies mogelijk wordt omschreven *welke gegevens* worden verwerkt en met *welk doel* dat gebeurt.

Grondslagen voor verwerking
Op grond van het bepaalde in artikel 8 van de Wbp geldt dat persoonsgegevens slechts mogen worden verwerkt indien aan één van de zes in dat artikel genoemde grondslagen wordt voldaan. Deze grondslagen zijn:

- De ondubbelzinnige toestemming van de betrokkene;
- In het kader van de uitvoering van een overeenkomst;
- In geval van het nakomen van een wettelijke verplichting;
- Ter vrijwaring van een vitaal belang van de betrokkene;
- Voor een goede vervulling van een publiekrechtelijke taak;
- Ter behartiging van het gerechtvaardigde belang van de verantwoordelijke.[6]

Onderzoek Autoriteit Persoonsgegevens: de rol van toestemming
De Autoriteit Persoonsgegevens (AP) heeft begin 2016 onder 41 gemeenten onderzoek gedaan naar hoe zij toestemming gebruiken bij de verwerking van persoonsgegevens in het sociaal domein. Ook is onderzocht hoe de gemeenten hun burgers informeren over de verwerking van hun gegevens.
Grondslag verwerken van gegevens: de rol van toestemming

[5] Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Zorgvuldig en Bewust: Gegevensverwerking en Privacy in een gedecentraliseerd sociaal domein, 1 mei 2014, p. 5.
[6] Wet bescherming persoonsgegevens, artikel 6 t/m 24.

Uit het onderzoek blijkt dat geen van de 41 gemeenten duidelijk heeft bepaald wat de rol van toestemming bij het verwerken van persoonsgegevens kan of moet zijn. Volgens de AP kunnen gemeenten problemen bij het bepalen van grondslagen voor de verwerking van persoonsgegevens in het sociaal domein niet vermijden door toestemming aan de betrokkenen te vragen voor de verwerking van persoonsgegevens.[7] Vooral niet als gemeenten die toestemming vragen in situaties waarin de betrokkenen afhankelijk zijn van de gemeente voor hun hulp, zoals de intake/toegangsverlening. Betrokkenen kunnen daarbij immers niet in vrijheid toestemming geven en een 'onvrije' toestemming vormt geen grondslag. Volgens de AP mogen gemeenten alleen persoonsgegevens verwerken als zij zich kunnen baseren op een van de andere grondslagen uit artikel 8 van de Wet bescherming persoonsgegevens. Concluderend stelt de AP dat toestemming vaak geen grondslag voor gegevensverwerking vormt, omdat er vanwege de afhankelijkheidsrelatie tussen betrokkene en de verantwoordelijke geen vrijheid is om toestemming te weigeren.

Overzicht
Gemeenten zouden volgens de AP een overzicht nodig hebben van de doelen, grondslagen en persoonsgegevens in het sociaal domein, omdat zij geen duidelijk beeld hebben van welke gegevens zij in het sociaal domein mogen verwerken. Dit overzicht zou onder meer noodzakelijk zijn om de taken in het sociaal domein te onderkennen die niet wettelijk geregeld zijn. Zonder een dergelijk overzicht kunnen gemeenten hun inwoners bovendien niet goed informeren, terwijl dat op grond van de Wbp wel vereist is.

Verenigbaar met doeleinden
Uitgangspunt van de Wbp is dat persoonsgegevens niet verder worden verwerkt dan op een wijze die verenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9 Wbp). Bij de beoordeling daarvan dient in elk geval het volgende in acht te worden genomen:

- de verwantschap met het doel van verzamelen;
- de aard van de gegevens;
- de gevolgen van een verstrekking;
- de wijze waarop de gegevens zijn verkregen;
- de mate waarin wordt voorzien in passende waarborgen.

Bovendien geldt dat persoonsgegevens slechts mogen worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, *toereikend*, *ter zake dienend* en *niet bovenmatig* zijn (artikel 11 Wbp).

Verwerking bijzondere persoonsgegevens
Op grond van de wet geldt dat het in beginsel verboden is om bijzondere persoonsgegevens – gegevens zoals iemands godsdienst of levensovertuiging, politieke gezindheid of omtrent iemands *gezondheid* – te verwerken (artikel 16 Wbp). Artikel 21 van de Wbp bevat uitzonderingen op het verbod om persoonsgegevens betreffende iemands gezondheid te verwerken.

Tabel 1. Uitzonderingen artikel 21 Wbp

Het verbod om persoonsgegevens betreffende iemands gezondheid te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt door: a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is;

[7] Autoriteit Persoonsgegevens, Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming, april 2016.

d. een reclasseringsinstelling, een bijzondere reclasseringsambtenaar, de raad voor de kinderbescherming of de gecertificeerde instelling, bedoeld in artikel 1.1 van de Jeugdwet, en de rechtspersoon, bedoeld in artikel 256, eerste lid, of artikel 302, tweede lid, van Boek 1 van het Burgerlijk Wetboek, voor zover dat noodzakelijk is voor de uitvoering van de hun wettelijk opgedragen taken;
f. bestuursorganen, pensioenfondsen, werkgevers of instellingen die te hunnen behoeve werkzaam zijn voor zover dat noodzakelijk is voor: 1. een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene.

Wet meldplicht datalekken
Met ingang van 1 januari 2016 is een wijziging van de Wet bescherming persoonsgegevens in werking getreden, waardoor een meldplicht voor datalekken geldt. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken, datalekken moeten melden aan de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene (de persoon van wie de persoonsgegevens zijn gelekt). De meldplicht geldt in geval van voorgedane beveiligingsincidenten. Beveiligingsincidenten zijn bijvoorbeeld het kwijtraken van een USB-stick, de diefstal van een laptop of een inbraak door een hacker. Er is volgens de wet sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van persoonsgegevens niet valt uit te sluiten. Bij zwakke plekken in de beveiliging wordt gesproken over een beveiligingslek en niet van een datalek.[8] De Autoriteit Persoonsgegevens kan met de inwerkintreding van de wet een bestuurlijke boete opleggen aan overtreders van privacyregels.[9]

2.2.4. Wet maatschappelijke ondersteuning 2015

Naast de regels uit de Wbp bevatten de Wmo 2015 en de Jeugdwet eigen regels rondom gegevensverwerking. In deze paragraaf volgt allereerst een overzicht van de belangrijkste bepalingen uit het hoofdstuk Gegevensverwerking van de Wmo 2015.[10]

Noodzakelijkheid
Uitgangspunt van de Wmo 2015 is dat *gegevensverwerking noodzakelijk* dient te zijn voor de beoordeling van de behoefte aan ondersteuning in de zelfredzaamheid en participatie. Dit geldt ook voor zover het gegevens omtrent het sociale netwerk van de cliënt of de mantelzorger betreft. Laatstgenoemde gegevens moeten zijn verkregen in het kader van het onderzoek respectievelijk van de mantelzorger/de cliënt zelf. Het noodzakelijkheidsprincipe geldt ook indien gegevens door een aanbieder worden verwerkt (artikel 5.1.2 Wmo 2015).[11]

Voor het *verstrekken* van persoonsgegevens geldt dat het college enkel die gegevens verstrekt die zijn verkregen in het kader van het onderzoek, of waarvoor de betrokkene zijn *ondubbelzinnige toestemming* heeft verleend (artikel 5.2.1 Wmo 2015). Voor verstrekking van gegevens aan een aanbieder, het CAK, de SVB of toezichthoudende ambtenaren (en vice versa), geldt ook dat dit plaatsvindt op basis van het noodzakelijkheidscriterium.

[8] Meldplicht datalekken Wet bescherming persoonsgegevens: Beleidsregels Wet meldplicht datalekken.
[9] https://www.rijksoverheid.nl/actueel/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht
[10] Wet maatschappelijke ondersteuning 2015, hoofdstuk 5.
[11] De wet bevat daarnaast ook bepalingen ten aanzien van gegevensverwerking door het CAK, de SVB en toezichthoudende ambtenaren. Op deze bepalingen wordt niet ingegaan, nu deze voor dit onderzoek niet van belang worden geacht.

Ondubbelzinnige toestemming
Als het gaat om het verkrijgen van informatie die binnen andere afdelingen bekend is, wegens aan het college opgedragen taken op grond van de Jeugdwet, de Participatiewet en de Wet gemeentelijke schuldhulpverlening, is daarvoor de *ondubbelzinnige toestemming* van de betrokkene vereist (artikel 5.1.1, vierde lid, Wmo 2015). Dit geldt ook voor zover de gegevens zijn verkregen van een zorgverzekeraar of een zorgaanbieder als bedoeld in de Zorgverzekeringswet en *noodzakelijk* zijn voor de beoordeling van het verzoek om ondersteuning.

Huiselijk geweld en kindermishandeling
Logischerwijs geldt in situaties waarbij sprake is van huiselijk geweld of kindermishandeling, of een redelijkerwijs vermoeden dat daarvan sprake is, dat het Advies en Meldpunt Huiselijk Geweld en Kindermishandeling (hierna: het AMHK) bevoegd is om zonder toestemming van de betrokkene persoonsgegevens te verwerken (artikel 5.1.6, tweede lid, Wmo 2015).[12]

In paragraaf 5.3 van de wet zijn tenslotte bepalingen opgenomen omtrent het bewaren van gegevens en de rechten van betrokkene, waaronder inzage in de bescheiden waarover bijvoorbeeld het college en aanbieders beschikken, het recht om gegevens te laten corrigeren en het recht op vernietiging van persoonsgegevens. Daarnaast schrijft de wet voor dat bij het verstrekken van persoonsgegevens het Burgerservicenummer (BSN) van een persoon wordt gebruikt.

2.2.5. Jeugdwet

Ook de Jeugdwet kent eigen regels voor wat betreft gegevensverwerking.[13]

Noodzakelijkheid
Verwerking van gegevens van een jeugdige of zijn ouders mag op grond van de wet plaatsvinden, voor zover dat *noodzakelijk* is voor:

a. de toeleiding naar, advisering over, bepaling van of het inzetten van een voorziening op het gebied van de jeugdhulp;
b. het doen van een verzoek tot onderzoek bij de raad voor de kinderbescherming of de uitvoering van kinderbeschermingsmaatregelen of jeugdreclassering;
c. de bekostiging van preventie, jeugdhulp, kinderbeschermingsmaatregelen, jeugdreclassering of werkzaamheden inzake gesloten uithuisplaatsing;
d. het verrichten van controle of fraude-onderzoek (artikel 7.4.0, eerste lid, Jeugdwet).

Als dat van belang is voor de uitvoering van voornoemde werkzaamheden wordt van jeugdhulpaanbieders, aanbieders van preventie, gecertificeerde instellingen, de raad voor de kinderbescherming en gekwalificeerde gedragswetenschappers verwacht om *kosteloos* tot *verstrekking* van de van belang zijnde persoonsgegevens van een jeugdige of zijn ouders, waaronder het BSN en andere bijzondere persoonsgegevens als bedoeld in de Wbp, over te gaan (artikel 7.4.0, tweede lid, Jeugdwet). Bij ministeriële regeling wordt bepaald op welke wijze gegevens, bedoeld in het eerste en tweede lid, worden verwerkt en in geval van het eerste lid, onder c. en d., tot welke gegevens de verplichting zich ten hoogste uitstrekt.

[12] Sinds 1 januari 2015 zijn het Steunpunt Huiselijk Geweld en het Advies en Meldpunt Kindermishandeling samen gegaan. De nieuwe naam is Veilig Thuis. De wettekst spreekt echter nog over AMHK. Indien in dit rapport wordt verwezen naar huidige (beleids)documenten is de in die documenten gehanteerde naam ongewijzigd overgenomen.
[13] Jeugdwet, hoofdstuk 7.

Gaat het om verwerking van gegevens die zien op de financiering van jeugdhulp – dit betreft bijvoorbeeld het verstrekken van een persoonsgebonden budget– dan geldt ook dat dit geschiedt voor zover dat in dat verband *noodzakelijk* is (artikel 8.4.2, eerste lid, Jeugdwet).

Regeling Jeugdwet
Voor het verwerken van persoonsgegevens omtrent de facturatie van de in te zetten jeugdhulp is paragraaf 6 van de Regeling Jeugdwet bepalend. De Regeling bepaalt welke persoonsgegevens van de jeugdige bij de declaratie van verleende diensten mogen worden verstrekt en voor welke doelen de gemeenten deze gegevens mogen verwerken. De ministeriële regel bevat daarnaast regels over de controle van declaraties, het betalen daarvan, het verrichten van materiële controle en het doen van fraudeonderzoek. In Bijlage 1a, behorende bij de Regeling, is voorts een voorbeeld van een privacyverklaring opgenomen die gebruikt kan worden in geval van hulpverleners die gespecialiseerde geestelijke gezondheidszorg (GGZ) aan jeugdigen verlenen. Hiermee kan worden bewerkstelligd dat de met betrekking tot de patiënt gestelde diagnose niet op het declaratieformulier hoeft te worden vermeld.

Dossieropbouw
De wet bepaalt ten aanzien van de jeugdhulpverlener dat deze een dossier inricht met betrekking tot de verlening van jeugdhulp. Hierin mogen aantekeningen worden bijgehouden omtrent de geconstateerde opgroei- en opvoedingsproblemen, psychische problemen en stoornissen en de te diens aanzien uitgevoerde verrichtingen, alsmede andere stukken die zodanige gegevens bevatten, voor zover dit voor een goede hulpverlening aan de betrokkene *noodzakelijk* is (artikel 7.3.8, eerste lid, Jeugdwet). In het tweede lid van voornoemd artikel is opgenomen dat de jeugdhulpverlener desgevraagd een door de betrokkene afgegeven verklaring met betrekking tot de in het dossier opgenomen stukken aan het dossier toevoegt.

Verder bevat hoofdstuk 7 van de Jeugdwet bepalingen omtrent het bewaren van persoonsgegevens en de rechten van betrokkenen zoals het recht op vernietiging van persoonsgegevens en het recht op inzage in het dossier. Op grond van het bepaalde in artikel 7.2.1 van de Jeugdwet gebruiken de gecertificeerde instelling, de jeugdhulpaanbieder, de raad voor de kinderbescherming en het college het BSN van een jeugdige in verband met het verwerken van persoonsgegevens.

2.3 Gemeentelijke visie

2.3.1. Inleiding

In deze paragraaf wordt de visie van de raad en het college van B&W op de balans tussen gegevensverwerking en de bescherming van de privacy binnen het sociaal domein belicht. De paragraaf geeft weer in welke mate binnen de gemeente Tynaarlo beleid is vastgelegd over de bescherming van de privacy en of dit beleid voldoet aan wet- en regelgeving. Tevens wordt aangegeven of het beleid eventuele hiaten vertoont.

2.3.2. Beleidsnota's

Opvallend is dat de visie van het college voor wat betreft de privacy binnen het sociaal domein niet zonder meer vindbaar is. Het onderwerp privacy komt echter wel als onderdeel van overkoepelende beleidsnotities, of meer uitvoeringsgerichte documenten, zoals de Beleidsregels Wmo 2015, naar voren. Door gesprekspartners is aangegeven dat er bewust voor is gekozen privacy in werkprocessen te verankeren, vanwege de vele voor 1 januari 2015 te

treffen voorbereidingen en het ontbreken van voldoende tijd voor afzonderlijk privacybeleid.

Er zijn twee beleidsnota's bekend, te weten de notitie 'Toegang sociaal domein', afkomstig van het college en de 'Kadernota Jeugd 2015-2016', afkomstig van de gemeenteraad.

In eerstgenoemde notitie blijkt dat het college belang hecht aan privacy en informatiebeveiliging.[14] Het college geeft hierover aan dat zowel organisatorische en technische beveiliging van belang is. Hieruit blijkt verder dat convenanten verkokerend zouden werken en op basis van toestemming van de burgers erg kwetsbaar zijn. Het uitwisselen van informatie zou echter veel voordelen opleveren en hiertoe zou een helder afwegingskader geformuleerd moeten worden. Uit de Kadernota Jeugd blijkt dat een privacyprotocol zal worden ontwikkeld voor het hele sociale domein.[15] Dit protocol zou ervoor moeten zorgen dat zich een praktijk ontwikkelt waarin de juiste balans wordt gevonden tussen ruimte voor professionals om noodzakelijke informatie te delen met het oog op een optimale ondersteuning van de betrokken burgers, en de borging van de privacy.
Van het bestaan van een privacy protocol is – ten tijde van de uitvoering van dit onderzoek – niet gebleken.

2.3.3. Beleidsregels Wmo 2015

Voor wat betreft de uitvoering van de Wet maatschappelijke ondersteuning 2015 (Wmo 2015), is in de 'Beleidsregels Wmo 2015' (hierna: de beleidsregels) een volledig hoofdstuk gewijd aan de bevoegdheden die het college heeft als het gaat om het verwerken en verstrekken van persoonsgegevens.[16] In deze beleidsregels wordt verwezen naar de vereisten uit de Wet bescherming persoonsgegevens en de bepalingen zoals opgenomen in hoofdstuk 5 van de Wmo 2015.

Transparant en noodzakelijkheid
Kenmerkende begrippen voor gegevensverwerking zijn de begrippen *transparant* en *noodzakelijkheid*. Het college dient transparant te zijn over het proces richting de betrokken inwoner en het moet voor de inwoner duidelijk zijn *door wie* en welke gegevens *met welk doel* worden verwerkt. Uit de beleidsregels blijkt dat het college enkel bevoegd is tot het verwerken van persoonsgegevens van de betrokkene voor zover die *noodzakelijk* zijn voor de uitvoering van de taken met betrekking tot de Wmo 2015. Dit geldt eveneens voor persoonsgegevens van de echtgenoot, ouders, inwonende kinderen en andere huisgenoten, voor zover dat *noodzakelijk* is om te bepalen welke hulp zij de betrokken inwoner kunnen bieden. Hetzelfde uitgangspunt geldt voor de vaststelling van te verlenen (of mogelijk te verlenen) hulp door mantelzorgers en anderen uit het sociale netwerk.

Noodzakelijkheid
Voor het verwerken van gegevens, is de invulling van het begrip *noodzakelijk* cruciaal. Afhankelijk van de situatie, moet het College over bepaalde gegevens beschikken en moeten deze verwerkt worden. Het College moet altijd in staat zijn te kunnen redeneren waarom bepaalde gegevens worden verwerkt en vastgelegd: waarom dit noodzakelijk is voor de uitvoering van de Wmo 2015.[17]

[14] College van B&W, Notitie Toegang Sociaal domein, december 2013, p. 17.
[15] Gemeenteraad Tynaarlo, Kadernota Jeugd 2015-2016, 'Groeien naar de toekomst', oktober 2014, p. 29.
[16] Beleidsregels Wmo 2015, hoofdstuk 8.
[17] Beleidsregels Wmo 2015, p. 25.

*Ondubbelzinnige toestemming*Als het – in het kader van uitvoering van de Wmo 2015 – gaat om het verwerken van gegevens die het college ten behoeve van de uitvoering van taken vanuit de Jeugdwet, de Participatiewet of de Wet gemeentelijke schuldhulpverlening heeft verkregen, is door het college aangesloten bij de eis van door de inwoner (expliciete schriftelijke) verleende *ondubbelzinnige toestemming*. Dit geldt ook voor zover het college gegevens wenst te verwerken die verkregen zijn van een zorgverzekeraar of een zorg-/ondersteuningsaanbieder. Bovendien dient het college ook in die gevallen wederom te kunnen aangeven waarom verwerking van deze gegevens noodzakelijk is voor de uitvoering van de Wmo 2015.

Ondubbelzinnige toestemming
Vanuit de Wmo 2015 heeft het college de plicht om de problematiek van de betrokken inwoner in het sociale domein in onderlinge samenhang in kaart te brengen en te bevorderen dat de dienstverlening zo goed mogelijk op elkaar is afgestemd. Problemen op grond van de Participatiewet (werkloosheid) kunnen bijvoorbeeld samenhangen met participatieproblemen in het kader van de Wmo 2015 (problemen bij de zelfredzaamheid en participatie). Daarnaast kan het ook van belang zijn om de zorg die deze inwoner op grond van de Zorgverzekeringswet ontvangt, af te stemmen op de ondersteuning die hij of zij in aansluiting of in aanvulling daarop nodig heeft vanuit de Wmo 2015. Omdat deze gegevens oorspronkelijk voor een ander doel zijn verwerkt, kan het College deze gegevens enkel verweken voor de uitvoering van de Wmo 2015 als de inwoner zijn of haar toestemming heeft gegeven.[18]

Verstrekken van persoonsgegevens
Indien het om door het college *verstrekken* van persoonsgegevens gaat, verwijzen de beleidsregels naar de wettekst. Dit geldt ook voor door zorg- en ondersteuningsaanbieders, het CAK, de SVB en toezichthouders te ververweken gegevens. Het college mag voorts gegevens aan deze organisaties verstrekken indien dat *noodzakelijk* is voor door die organisaties uit te voeren taken. Dit geldt ook in geval van gegevensverstrekking aan zorgverzekeraars en wederom enkel met toestemming van de betrokken inwoner.

AMHK binnen de gemeente
Uit de beleidsregels blijkt dat derden, zoals medewerkers van een Sociaal Team, inlichtingen kunnen verschaffen aan het AMHK, indien die beroepshalve beschikken over inlichtingen die noodzakelijk kunnen worden geacht om een situatie van kindermishandeling te beëindigen of een redelijk vermoeden van kindersmishandeling te onderzoeken. In die gevallen is geen toestemming vereist van de inwoner die het betreft en kan het – indien nodig – met doorbreking van de plicht tot geheimhouding op grond van een wettelijk voorschrift of op grond van hun ambt of beroep. In de beleidsregels wordt dit aangeduid als ‘meldrecht’. De medewerker beschikt hiertoe over beoordelingsvrijheid.

Rechten en plichten inwoners en afhankelijkheidsrelatie
De beleidsregels gaan ook in op de rechten en plichten die inwoners hebben in het kader van de verwerking en verstrekking van persoonsgegevens. Inwoners hebben onder omstandigheden de mogelijkheid om toestemming voor het verwerken en verstrekken van gegevens te weigeren. Een gevolg daarvan zal echter zijn dat het college niet in staat is te komen tot een integraal aanbod voor de ondersteuning. Dit kan – zo is opgenomen in de beleidsregels – betekenen dat de Wmo voorziening niet goed of minder goed afgestemd zal zijn op andere voorzieningen die de betrokken inwoner eventueel ontvangt.

[18] Beleidsregels Wmo 2015, p. 26.

Uit de beleidsregels volgt verder dat als het college niet kan vaststellen of er reden is de betrokken inwoner met een maatschappelijke voorziening te ondersteunen, dat het college een negatief besluit kan nemen over de aanvraag. Voorts blijkt dat de betrokken inwoner met de mogelijkheid om al dan niet toestemming te verlenen, zelf in staat wordt gesteld een afweging te maken of hij of zij de gegevensverwerking of -verstrekking in verhouding vindt staan tot de benodigde ondersteuning.

Moment van toestemming
De beleidsregels geven aan dat het college meteen bij de melding aan de inwoner duidelijk zal moeten maken dat – indien dat noodzakelijk is voor de uitvoering van de Wmo 2015 – gegevens worden opgehaald, verstrekt en verwerkt, conform de wet- en regelgeving die van toepassing is. Omdat het onderzoek meteen na de melding volgt, is het dan ook van belang de inwoner op het moment van de melding te informeren en dat hij/zij op dat moment zijn/haar toestemming geeft.

2.3.4. Gegevensverwerking Jeugdhulp

Met de invoering van de Jeugdwet zijn gemeenten verantwoordelijk voor de preventie, jeugdhulp en de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering. Logisch gevolg hiervan is dat gemeenten het aantal zorgpartners waarmee zij samenwerken hebben zien toenemen en dat daarbij sprake is van andersoortige zorgpartners dan voorheen het geval was. In het kader van de uitvoering van de Jeugdwet vinden onder andere contacten plaats met het schoolmaatschappelijk werk, instellingen voor kinder- en jeugdpsychiatrie, alsook met de Raad voor de kinderbescherming. Gegevenswerking vindt onder meer plaats in het kader van preventie, de in te zetten jeugdhulp, alsmede in verband met facturering. De vraag luidt in hoeverre binnen de gemeente Tynaarlo privacybeleid is ontwikkeld ten aanzien van gegevensverwerking aangaande de uitvoering van de Jeugdwet.

Plan van aanpak voorliggend veld: de Leertuin
Ten behoeve van de uitvoering van de Jeugdwet hebben de gemeenten in Noord-Midden Drenthe een zogeheten 'Plan van aanpak voorliggend veld' opgesteld.[19] Het plan van aanpak beoogt de ondersteuning zo dicht mogelijk bij ouders en kind te brengen, door het versterken van de plaatsen waar ouders, kinderen en jeugdigen zijn. In het plan van aanpak wordt gesproken over een activiteitenplanning, en hierbij is ook privacy een van de thema's. Als gewenst resultaat wordt gesproken over het hanteren van een eenduidig privacy reglement.

Gegevens delen in het belang van het kind
Uit het plan van aanpak volgt dat gegevens in het belang van het kind gedeeld mogen worden en dat dit ook zou kunnen betekenen dat gegevens gedeeld worden tegen de zin van de ouders in. Aangegeven wordt dat betrokken organisaties en hulpverleners in de diverse samenwerkingsverbanden verschillende opvattingen zouden hebben over het mogen delen van informatie. Ieder samenwerkingsverband zou doorgaans een eigen convenant met bijbehorende privacy afspraken hanteren, en voor iedere groep hulpverlener zou tegelijkertijd een andere interpretatie inzake privacy gelden. In dit verband wordt dan ook gewezen op de in Brabant, Friesland en Groningen al ontwikkelde Leertuin Zorg en Veiligheid (hierna: de Leertuin) die als doel heeft te komen tot eenduidige interpretatie van de wet- en regelgeving en een ontschotte informatie uitwisseling.

Leertuin Zorg en Veiligheid
De Leertuin Zorg en Veiligheid zou leiden tot afgestemde zorg en – indien nodig – justitiële interventies; één handelswijze voor alle partijen en samenwerkingsverbanden, dus niet

[19] Regio Noord-Midden Drenthe, Plan van aanpak voorliggend veld, juni 2014.

alleen voor veiligheidshuizen, maar ook voor CJG's, sociale teams, bemoeizorg, ZAT's (zorgadviesteams) in het onderwijs, huiselijk geweld, buurtnetwerken etc. Zodoende zou niemand zelf het 'privacy-wiel' hoeven uit te vinden. Middels bijbehorend stappenplan zou het mogelijk zijn om binnen de wettelijke kaders eenzelfde verantwoorde afweging inzake gegevensuitwisseling te realiseren.

Actiepunten betreffende het thema privacy, zo blijkt uit het plan van aanpak, betreft het doen van onderzoek naar de vraag of een Leertuin Zorg en Veiligheid ook binnen de gemeenten in Noord-Midden Drenthe gewenst is, welke kosten daaraan zijn verbonden, op welke schaal dit georganiseerd dient te worden en of er alternatieven zijn. Bovendien wordt aangegeven dat de wens bestaat dit 3d-breed te organiseren, maar dat de vraag is hoe dat vormgegeven kan worden.

In andere documenten, zoals de brief van het college van B&W gericht aan de PvdA raadsfractie d.d. 19 augustus 2015, wordt door het college eveneens verwezen naar de te ontwikkelen Leertuin. Volgens het college worden gegevens uitgewisseld om hulp en/of ondersteuning aan een gezin op elkaar af te stemmen en gebeurt dit altijd met toestemming van het gezin of de jeugdige.[20] In de brief maakt het college voorts nadrukkelijk gewag van het feit dat zowel de gemeente, maar ook andere betrokken partners, zich dienen te houden aan de opgestelde wetgeving rond privacy en dat in geval van overtreding door medewerkers eventuele sancties op grond van de CAR/UWO worden getroffen. Verder blijkt uit de brief dat een Security Officer is belast met de naleving van de privacy.

Het college van B&W over de Leertuin
De Leertuin is erop gericht hoe je als verschillende organisaties/professionals omgaat met privacy en gezamenlijk tot een protocol kunt komen waarbij privacy wordt gerespecteerd maar niet belemmerend werkt. Uitgangspunt binnen de jeugdhulp is dat de betrokken medewerkers vanuit hun professie weten om te gaan met de privacy van de cliënt en deze respecteren. Daarbij kan het in het belang van de veiligheid van het kind soms noodzakelijk zijn daarvan af te wijken. De professional zou dan in staat zijn dat te motiveren.

2.4 Toekomstige ontwikkelingen voor te (her)formuleren beleid

Algemene Verordening Gegevensbescherming
Op 14 april 2016 heeft het Europees Parlement ingestemd met de Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van verwerking van die gegevens (Verordening 2016/679, de Algemene Verordening Gegevensbescherming, hierna: de AVG). De AVG is van toepassing vanaf 25 mei 2018 en heeft rechtstreekse werking.

De AVG ziet op versterking en uitbreiding van privacy rechten, en dezelfde, stevige bevoegdheden voor alle Europese privacy toezichthouders, meer verantwoordelijkheden voor organisaties en is rechtstreeks van toepassing in alle lidstaten. Als de AVG van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de Verordening bijvoorbeeld nadruk gelegd op de verantwoordelijkheid van organisaties om zelf de wet na te leven en om te kunnen aantonen dat zij zich aan de wet moeten houden. Er gaat een documentatieplicht gelden, wat inhoudt dat organisaties moeten aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG

[20] College van Burgemeester en Wethouders gemeente Tynaarlo, Antwoordbrief aan de PvdA raadsfractie inzake privacy, 19 augustus 2015.

te voldoen. Verder mogen boetes worden opgelegd voor elke inbreuk op de verordening, en organisaties worden verplicht om een Privacy Impact Assessment (PIA) uit te voeren, zodat zij inzicht krijgen in de risico's van het verwerken van persoonsgegevens en als gevolg daarop gepaste maatregelen kunnen nemen. Voorts worden overheidsorganisaties verplicht gesteld om een functionaris voor gegevensbescherming aan te wijzen die onder andere toeziet op de naleving van de AVG.

De AVG biedt organisaties verder ook hulp bij het naleven van de wet. Zo bevat deze modelbepalingen voor de relatie tussen de verantwoordelijke en de verwerker en voor doorgifte van persoonsgegevens. De AVG bevat ook een artikel over toestemming. Hierin staat wat de voorwaarden zijn om geldige toestemming te krijgen van mensen om hun persoonsgegevens te verwerken. Ook voor de verwerking van bijzondere persoonsgegevens, zoals gegevens omtrent iemands gezondheid, schrijft de AVG voor wanneer een organisatie daartoe bevoegd is.

2.5 Conclusie

De Kabinetsvisie Zorgvuldig en Bewust, alsmede de regels uit de Wbp, de Wmo 2015 en de Jeugdwet zijn bepalend voor de wijze waarop gemeenten gegevens mogen verwerken. Uit de Kabinetsvisie blijkt dat van overheidsorganisaties ten aanzien van gegevensdeling wordt verwacht terughoudend te werk te gaan. Bovendien wordt verwezen naar de eisen van de Wbp en de sectorale wetgeving. Uit deze wetgeving volgt dat het bij het verwerken en verstrekken van persoonsgegevens gaat om de vraag in hoeverre dit noodzakelijk is voor de uit te voeren taak. In beginsel geldt een verbod op het verwerken van gegevens omtrent iemands gezondheid. In artikel 21 van de Wbp zijn hierop uitzonderingen geformuleerd en in de sectorale wetgeving wordt, wat betreft gegevens aangaande iemands gezondheid, gewezen op het noodzakelijkheidsprincipe.

Hoewel in de Nota Toegang sociaal domein en de Kadernota Jeugd enige aandacht aan privacy wordt geschonken, is dat onvoldoende om te kunnen spreken van een duidelijke visie van het college op gegevensverwerking binnen het sociaal domein.

De Beleidsregels Wmo 2015 bevatten wél uitvoerige bepalingen over de wijze waarop gegevens mogen worden verwerkt en verstrekt en deze sluiten aan bij de wettekst van de Wmo 2015. Kernbegrippen van gegevensverwerking betreft noodzakelijkheid en transparantie. Opvallend is dat de beleidsregels ervan uitgaan dat het door burgers weigeren van het verstrekken van gegevens kan leiden tot een negatief besluit over de gewenste ondersteuning. De beleidsregels schrijven dan ook voor om burgers vanaf het moment van de melding meteen om toestemming voor het verwerken en verstrekken van gegevens te vragen, maar van een daadwerkelijke vrije toestemming is dan geen sprake. Deze werkwijze benadrukt de afhankelijkheidsrelatie tussen kwetsbare burgers en de gemeente. De Autoriteit Persoonsgegevens heeft naar aanleiding van onderzoek echter geconcludeerd dat toestemming geen grondslag voor gegevensverwerking vormt, omdat er vanwege de afhankelijkheidsrelatie tussen betrokkene en de verantwoordelijke geen vrijheid is om toestemming te weigeren.

Voor wat betreft de uitvoering van de Jeugdwet wordt in verschillende documenten verwezen naar de zogeheten Leertuin Zorg en Veiligheid. De Leertuin zou moeten leiden tot één handelswijze voor alle partijen en samenwerkingsverbanden, zodat niemand zelf het 'priva-

cy-wiel' zou hoeven uit te vinden. De wens was om de Leertuin 3d breed vorm te geven, maar uit de documentstudie blijkt niet dat dit is gebeurd.

Sinds 1 januari 2016 geldt op grond van de Wet meldplicht datalekken dat beveiligingsincidenten waarbij persoonsgegevens verloren zijn gegaan, of als niet valt uit te sluiten dat sprake is van onrechtmatige verwerking van persoonsgegevens, gemeld behoren te worden bij de Autoriteit Persoonsgegevens.

Op 25 mei 2018 treedt de Europese Algemene Verordening Gegevensbescherming in werking. Deze Verordening ziet op de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens. De Verordening heeft rechtstreekse werking, wat betekent dat ook gemeenten aan de in de Verordening opgenomen bepalingen gebonden zijn. Op grond van de Verordening gaat een documentatieplicht gelden, worden organisaties verplicht om een Privacy Impact Assessment te verrichten, en wordt het verplicht om een functionaris gegevensbescherming aan te stellen. De Verordening bevat nadrukkelijke bepalingen over het verkrijgen van toestemming en het verwerken van bijzondere persoonsgegevens, zoals gegevens omtrent iemands gezondheid. Er kunnen bovendien boetes opgelegd worden voor overtreding van de Verordening.

Op grond van zowel de huidige wetgeving als de in 2018 in werking tredende Algemene Verordening Gegevensbescherming wordt steeds meer van overheden verwacht als het gaat om gegevensverwerking. Dit vraagt ook om kennisverbreding en gedragsverandering van de bij deze overheden werkzame medewerkers. De onderzoekers achten het van belang dat de gemeente Tynaarlo zijn medewerkers op voornoemde veranderingen voorbereidt.

3

Gegevensverwerking en privacybescherming

3.1 Inleiding

In dit hoofdstuk wordt ingegaan op de verhouding tussen gegevensverwerking en de bescherming van de privacy in de praktijk. Allereerst wordt antwoord gegeven op de vraag of in de praktijk uitvoering wordt gegeven aan het vastgelegde privacybeleid. Daarnaast wordt aangegeven welke risico's bestaan wat betreft de verwerking van gegevens en of deze binnen de gemeente Tynaarlo voldoende in kaart zijn gebracht. Ook is beoordeeld of het college voldoende maatregelen heeft genomen om te bevorderen dat er binnen het sociaal domein voldoende balans is tussen gegevensverwerking en de bescherming van de privacy. In dit kader is dan ook onderzocht welke afspraken gelden tussen de gemeente en ketenpartners en of hiernaar wordt gehandeld. Tenslotte is gekeken of burgers voldoende worden geïnformeerd over de bescherming van hun privacy.

3.2 Uitvoering geven aan privacybeleid

3.2.1. Inleiding

Onderstaande paragraaf geeft antwoord op de vraag hoe gegevensverwerking in het sociaal domein binnen de gemeente Tynaarlo plaatsvindt. Hierbij is niet alleen onderzocht hoe medewerkers van de gemeenten hiermee omgaan, maar gekeken is ook naar de wijze waarop zorgaanbieders dit doen. De vraag luidt of hierbij voldoende integer wordt gehandeld en of betrokkenen voldoende integriteitsbewust zijn.

3.2.2. Bekendheid met het beleid

Om het beleid op het gebied van gegevensverwerking te kunnen naleven, is het van belang daarmee bekend te zijn. Door gesprekspartners is verschillend geantwoord op de vraag in hoeverre binnen de gemeente privacybeleid is vastgelegd.

De meeste gesprekspartners verwijzen naar de Leertuin en de in dat verband gevolgde informatiebijeenkomsten. Deze bijeenkomsten zijn gevolgd door zowel de leden van de Sociaal Teams als door de leden van het Toegangsteam Jeugd. Gesprekspartners geven aan de

informatie over de Leertuin als naslagwerk te zien en als zodanig te gebruiken wanneer privacyvraagstukken zich in de praktijk voordoen. Enkele gesprekspartners zeggen dat de kennis omtrent de Leertuin niet volledig up to date is. Anderen wijzen op het zogeheten – voor zorgverleners al langer bekende – juridisch Zwitsers Zakmes. Ook is regelmatig gewezen op de Beleidsregels Wmo 2015. En een enkeling verwijst voor regelgeving omtrent gegevensverwerking naar de wettekst van de Wmo.

Daarnaast verwijzen sommige gesprekspartners naar de binnen hun beroepsgroep geldende beroepscodes en een enkeling benadrukt de afgelegde ambtseed. Bovendien is aangegeven dat medewerkers die afkomstig zijn van verschillende organisaties, mogelijk ook hun eigen gedragsregels hanteren. Een aantal personen dat al langer in dienst is van de gemeente, heeft aangegeven dat de op de gemeentepagina gepubliceerde gedragsregels bepalend zijn voor zorgvuldige gegevensverwerking. Wat tijdens de gevoerde gesprekken ook naar voren is gekomen, is dat betrokkenen regelmatig op basis van een combinatie van gevoel, ervaring en professionele integriteit handelen. Ervaren medewerkers (zowel op het gebied van de Wmo als op het gebied van de voormalige Wet op de Jeugdzorg) geven immers aan dat privacy altijd een onderdeel van het werk is geweest en dat zij op basis daarvan weten hoe te handelen.

Geen van de gesprekspartners verwijst naar hetgeen de Wbp voorschrijft.

Regelmatig is gezegd dat de werkwijze rondom privacy niet volledig concreet is vastgelegd. Dit terwijl dit met het oog op eenduidig werken, alsmede in geval van het in dienst treden van nieuwe medewerkers, door de meeste gesprekspartners wel als nuttig wordt beschouwd.[21]

Zorgaanbieders verwijzen voor met de gemeente gemaakte afspraken over privacy doorgaans naar de met de gemeente afgesloten zorgcontracten, die, volgens hen, bepalingen over de in acht te nemen privacyregels bevatten. Vanuit een enkele zorgaanbieder is aangegeven dat deze niet bekend is met de privacyregels van de gemeente. Wel zouden er algemene werkwijzen en protocollen zijn die zorgaanbieders hanteren. Een bepaalde zorgaanbieder ontwikkelt een eigen visie/werkwijze. In de met zorgaanbieders gevoerde gesprekken is regelmatig aangegeven dat binnen de organisatie een eigen handboek geldt waarnaar wordt verwezen in geval van privacyvraagstukken.

Op de vraag of op juiste wijze uitvoering wordt gegeven aan het beleid wordt in onderstaande paragrafen – aan de hand van verschillende bij gegevensverwerking behorende onderdelen – antwoord gegeven.

3.2.3. Toestemming: gebruik van toestemmingsfomulieren?

Door de meeste gesprekspartners is aangegeven dat het door de cliënt/burger verlenen van toestemming belangrijk is voor het al dan niet mogen verwerken en verstrekken van persoonsgegevens. De cliënt dient immers te begrijpen waarom gegevens worden gevraagd en voor hem of haar moet duidelijk zijn dat in zijn of haar belang wordt gehandeld. Het verkrijgen van toestemming valt of staat volgens de meeste gesprekspartners dan ook met goede argumentatie.

[21] Binnen het Toegangsteam Jeugd wordt gewerkt aan een visie rondom privacy. De binnen het team werkzame medewerkers maken soms nog gebruik van de regels die binnen verschillende organisaties golden. Dit betekent voor hen dat de oorspronkelijke regels – van voor de transitie – feitelijk nog gelden.

Opvallend is dat gesprekspartners niet op de hoogte zeggen te zijn van de juridische grondslag die voor het verwerken van persoonsgegevens geldt. Er bestaat ook geen eenduidig beeld omtrent het al dan niet gebruiken van toestemmingsformulieren in geval dat informatie bij derden (zoals een behandelaar of de huisarts) dient te worden opgevraagd. Sommige gesprekspartners hanteren wel een zogeheten toestemmingsformulier, terwijl anderen zeggen dat een dergelijk formulier niet bestaat. Regelmatig wordt zelfs mondeling om toestemming gevraagd, waarover is aangegeven dat die vervolgens niet altijd schriftelijk wordt vastgelegd. De gesprekspartners zijn zich allen bewust van het feit dat zij bijvoorbeeld niet zelfstandig een behandeld arts mogen bellen met het verzoek om informatie. Een enkele keer is daarover opgemerkt dat het efficiëntie bevorderend zou zijn om de cliënt zelf informatie via bijvoorbeeld de behandelend arts aan te laten dragen.

Enkele gesprekspartners hebben aangegeven dat de bedoeling van onder andere de sociaal teams is om zo laagdrempelig mogelijk zorg te verlenen, maar dat sommige regels daaraan in de weg zouden staan. Het gebruik van een toestemmingsverklaring zou bijvoorbeeld haaks staan op het (snel) zorg willen verlenen. Door raadsleden is het belang van schriftelijke toestemmingsformulieren echter onderschreven.

Toestemming bij dementerende ouderen
Een medewerker van een Sociaal Team: “Als je bijvoorbeeld toestemming nodig hebt in een situatie waarin sprake is van een dementerende oudere, dan vraag ik meestal mondeling om toestemming, maar bij dementerende ouderen kom je niet altijd tot een gesprek. Dan gaat toestemming via de naaste omgeving, zoals familieleden, maar zij willen niet altijd meteen tekenen, omdat zij soms huiverig zijn waarvoor getekend wordt. Dit is in het kader van de Leertuin nogal tegenstrijdig.”

In het kader van uitvoering van de Jeugdwet is door gesprekspartners aangegeven dat men voorheen gewend was – dat wil zeggen voor de inwerkingtreding van de Jeugdwet – ouders voor alles om toestemming te vragen. Dit gebeurt nu nog steeds. Aangegeven wordt dat gegevens worden gedeeld en met welke reden. Indien gegevens afkomstig van bijvoorbeeld een leerkracht van de school benodigd zijn, wordt hiervoor ook altijd eerst toestemming gevraagd. Ouders worden vervolgens gevraagd om het verslag, dat na het ontvangen van de informatie wordt opgesteld, voor akkoord te tekenen. Vanaf de leeftijd van 16 jaar dient de jeugdige voorts ook altijd zelf toestemming te geven.

Toestemming in crisissituaties
Vrijwel alle gesprekspartners geven aan dat er situaties zijn waarbij direct handelen van levensbelang is en dat men dan niet toekomt aan het vragen van toestemming. In het dossier wordt dan melding gemaakt van de reden waarom de privacyregels niet in acht zijn genomen.

Een medewerker van een Sociaal Team aan het woord
“In crisissituaties heb je geen tijd om alles uit te leggen op het gebied van privacy regels. Daar kom je dus niet aan toe. Je moet ingrijpen in het kader van de veiligheid en gezondheid van de cliënt. We nemen dan ook meteen contact op met andere instanties. Veiligheid gaat in die gevallen voor.”

Afhankelijkheidsrelatie
In het kader van gegevensverwerking in het sociaal domein is het van belang in hoeverre het weigeren van het delen van gegevens invloed heeft op de beoordeling van de hulpvraag en de uiteindelijke inzet van ondersteuning/jeugdhulp. Ondersteuningsbehoevenden zijn voor

de inzet daarvan in zekere zin afhankelijk van de gemeentelijke organisatie, wat maakt dat de toestemming mogelijk niet altijd vanuit vrije wil wordt gegeven. Zie ook het in het vorige hoofdstuk vermelde onderzoek van de Autoriteit Persoonsgegevens hierover. De meeste gesprekspartners geven aan dat vrij snel aan de cliënt duidelijk gemaakt dient te worden waarom bepaalde informatie moet worden gedeeld. Dit zou het vertrouwen dat de cliënt in de gemeente heeft ten goede komen met als gevolg dat toestemming niet snel geweigerd wordt. Enkele gesprekspartners geven aan dat de cliënt direct bij de melding dient te tekenen voor onderzoek. Dit betekent vervolgens dat hij of zij aan het verstrekken van gegevens dient mee te werken, zodat het proces van melding tot de daadwerkelijke inzet van ondersteuning zorgvuldig kan worden afgerond. De meeste gesprekspartners geven aan dat het van belang is dat de gegevens op het moment van de aanvraag volledig en correct zijn. Als dat niet het geval is, dan kan een aanvraag niet in behandeling worden genomen.

Sommige gesprekspartners geven aan in bovenstaande situatie een oplossing te zien in het inschakelen van een extern (advies)bureau. Ter bevordering van de transparantie van het proces worden de aan de extern adviseur te stellen vragen eventueel gezamenlijk – dus met behulp van de cliënt/de ouders – opgesteld. Het adviesbureau brengt vervolgens advies uit, dat volgens de gesprekspartners altijd nog door de cliënt/de ouders kan worden geblokkeerd. Anderen geven aan met problemen rondom het toestemmingsvereiste naar een jurist van de afdeling Wmo, of de centrale juridische afdeling van gemeente te gaan. Door sommige gesprekspartners is aangegeven dat ook de klachtencoördinator ingeschakeld zou kunnen worden, in geval dat een situatie ‘lastig kan worden’.

Binnen de uitvoering van de Jeugdwet gaat het opvragen van stukken doorgaans via de ouders en op basis van vrijwilligheid. Aan ouders wordt aangegeven welke stukken voor de beoordeling van de hulpvraag vereist zijn en hierbij wordt nadrukkelijk aangegeven voor welk doel die gegevens worden opgevraagd. Bij het niet verkrijgen van de benodigde informatie en afhankelijk van de soort hulpvraag, de ernst van de problematiek en de mate van (on)veiligheid van de situatie, bezint men zich op de te nemen vervolgstappen. Dat kan bijvoorbeeld het afsluiten van het dossier zijn, het stoppen van de hulpverlening, het formuleren van nieuwe doelen met betrokkenen, het doorzetten van de melding naar Veilig Thuis, of de Raad voor de kinderbescherming.

Regelmatig is door gesprekspartners opgemerkt dat cliënten het doorgaans niet erg vinden dat gegevens gedeeld en verwerkt worden, mits dat in hun belang is en ten behoeve is van de zorg die zij wensen. Medewerkers leggen mondeling uit hoe de regels rondom privacy werken, hiervoor bestaat namelijk geen informatiefolder.

Gegevensverwerking ten behoeve van de inzet van jeugdhulp
Een jeugdconsulent aan het woord: “Wij voeren veel gesprekken met ouders en kinderen en we weten dat voor gegevensverwerking toestemming vereist is. Een kind moet vanaf zijn 16e ook zelf toestemming geven. Stel dat een van de ouders belt, dan moet die ouder de andere ouder op de hoogte stellen. Als je belt naar school, dan stel je daarvan ook de ouders op de hoogte. Of als een moeder met mij wil afstemmen over een indicatie, dan wil ik dat wel afstemmen met alle partijen. Het gaat dus altijd om openheid.”

3.2.4. Noodzakelijkheid

In veruit de meeste gesprekken is aangegeven dat bij het verwerken en verstrekken van persoonsgegevens gehandeld wordt op basis van noodzakelijkheid. Een veel gehoord uitgangspunt in deze is: ‘nice to know, or need to know’. Op basis van dit principe zijn de ge-

sprekspartners van mening dat ook altijd zeer gerichte vragen aan bijvoorbeeld partners, het sociale netwerk, mantelzorgers, scholen, huisartsen, of betrokken behandelaars worden gesteld.

Andere gesprekspartners geven aan dat per situatie zorgvuldig gekeken dient te worden naar de belangen die spelen. Op basis daarvan maken zij een afweging of gegevens al dan niet gedeeld mogen worden. Ook hierover is wederom aangegeven dat een en ander soms plaatsvindt op basis van gevoel, ervaring en professionele integriteit. Gesprekspartners hebben aangegeven bij het bepalen van de noodzakelijkheid en het formuleren van de juiste vragen geen moeilijkheden te ondervinden, omdat zij op basis van ervaring vaak weten welke informatie benodigd is.

Nice to know, or need to know
Een medewerker van het Jeugdteam aan het woord: “Het kan voorkomen dat ouders angstig zijn voor het delen van gegevens en niet zonder meer toestemming geven. Je wilt een breed beeld krijgen van de situatie waarin het kind zich bevindt en dus moet je goed uitleggen waarom gegevens noodzakelijk zijn. Het gaat dan om zowel de situatie thuis, als op school. Je bakent de vraagstelling aan bijvoorbeeld de leerkracht ook goed af. Je hoeft ook weer niet te veel te horen en de vraag is altijd: Is it nice to know, or need to know?”

3.2.5. Eenduidigheid

De meeste gesprekspartners geven aan dat op dezelfde wijze door betrokkenen wordt gewerkt als het gaat om het hanteren van de privacyregels. Dit geldt ook voor de sociaal teams. Ter borging van het op eenduidige wijze werken wordt door gesprekspartners verwezen naar de binnen de gemeente werkzame juristen aan wie vragen rondom het privacyrecht gesteld kunnen worden. Daarnaast is aangegeven dat gezamenlijke studiemiddagen, waarbij medewerkers elkaar op de hoogte kunnen stellen van de laatste ontwikkelingen, hieraan bijdragen. In teams en in breder verband is voorts regelmatig sprake van casus- of projectteamoverleg waarbij gezamenlijk gezocht kan worden naar het hanteren van juiste methoden en werkwijzen.

Sommige gesprekspartners hebben aangegeven dat getwijfeld wordt of conform de privacy regels wordt gewerkt. Zorgen zijn bijvoorbeeld geuit over het feit dat niet alles vastligt en daarmee het risico bestaat dat gegevensverwerking op verschillende wijzen plaatsvindt. Ook het feit dat op de gemeentelijke website geen duidelijke verwijzing naar de privacyregels of een folder bestaat, kan betekenen dat burgers niet op dezelfde wijze worden geïnformeerd. Anderen geven daarover aan dat het aantal door burgers gestelde vragen over de privacy enorm meevalt en dat uitleg omtrent de regelgeving zelfden problemen oplevert.

Volgens gesprekspartners zit de valkuil in het feit dat de aandacht verslapt en het onderwerp privacy niet op regelmatige basis gezamenlijk wordt besproken. Aangegeven is dat behoefte bestaat aan een stappenplan of een compact handboek. Dit ook met het oog op het inwerken van nieuwe en/of tijdelijke medewerkers.

Over de wijze waarop informatie wordt gedeeld geven sommige gesprekspartners aan dat vanuit de Leertuin is aangegeven dat dit per e-mail kan plaatsvinden. Andere gesprekspartners zeggen dat dit enkel schriftelijk mag. Ook is niet vastgelegd hoe gegevens door cliënten zelf kunnen en mogen worden aangeleverd. Door enkele medewerkers is aangegeven dat het efficiënt en praktisch zou zijn als cliënten gegevens gewoon per e-mail delen. Bovendien zouden gegevens onder de ogen van daartoe onbevoegden kunnen komen, als cliënten gegevens per post zouden aanleveren.

3.3 Risico's gegevensverwerking

De vraag luidt welke risico's er bestaan als het gaat om gegevensverwerking en de bescherming van de privacy en of deze risico's voldoende in kaart zijn gebracht. Als het gaat om de risico's van gegevensverwerking, dan zijn deze volgens de onderzoekers als volgt te categoriseren:

- **Risico's wegens het niet op uniforme wijze verwerken van gegevens (het niet hanteren van protocollen en stappenplannen)**

Een uniforme wijze van gegevensverwerking komt tot stand door bijvoorbeeld het gebruik van protocollen en werkprocessen. Door een ieder die binnen het sociaal domein te maken heeft met gegevensverwerking op dezelfde wijze laten werken, wordt voorkomen dat gegevensverwerking op talloze manieren en naar eigen inzicht plaatsvindt. Als dat laatste het geval is, wordt meer risico gelopen op bovenmatige, juridisch niet toelaatbare (niet noodzakelijke) verwerking van gegevens. Bovendien kan in verband met het ontbreken van duidelijke richtlijnen niet gecontroleerd worden in hoeverre conform wet- en regelgeving wordt gewerkt. In dit kader is tevens van belang of bevoegdheden en verantwoordelijkheden zijn vastgelegd, opdat medewerkers weten wat van hen wordt verwacht. Een uniforme werkwijze ziet voorts ook op de voorlichting van burgers.

- **Risico's wegens verkeerd gebruik van juridische grondslagen en eigen invulling van normen**

Zoals gebleken bevatten de Wbp en de zogeheten sectorwetgeving diverse grondslagen op basis waarvan gegevens verwerkt kunnen worden. Indien gegevensverwerking in de praktijk niet conform deze grondslagen, of niet eenduidig, plaatsvindt, bestaat ook het gevaar op bovenmatige of juridisch niet toelaatbare gegevensverwerking.

- **Risico's ten aanzien van systeemtechnische beveiliging, zoals het niet gebruiken van beveiligde systemen (waaronder portals ten behoeve van gegevensoverdracht), het niet hanteren van autorisaties, gegevensbeveiliging (waaronder het bewaren van dossiers) en het niet inbouwen van waarborgen ten aanzien van het administratieve proces**

Ten aanzien van de taken binnen het sociaal domein is sprake van betrokkenheid van diverse, zowel interne als externe, professionals. Voor gegevensverwerking wordt gebruik gemaakt van diverse systemen. Van belang is dat deze systemen juist zijn ingericht en door een ieder op juiste wijze worden gehanteerd. Met het hanteren van autorisaties ten aanzien van die systemen wordt voorkomen dat dossiers en daarbij behorende documenten voor een ieder inzichtelijk zijn. Ook is het van belang dat dossiers in de te gebruiken systemen op dezelfde wijze worden bewaard. Onder dit onderdeel valt ook het maken van waarborgen ten aanzien van het administratieve proces, opdat medewerkers van de administratie enkel die gegevens zien die noodzakelijk zijn voor de uitvoering van hun (administratieve) taken.

- **Risico's wegens het door ketenpartners onjuist omgaan met de privacyrechten van burgers**

Uitvoering van de taken behorende tot het sociaal domein vindt door diverse ketenpartners plaats. Het is van belang dat ook deze ketenpartners weten hoe met gegevens dient te worden omgegaan en dat dit conform de regelgeving gebeurt.

3.4 Waarborgen

3.4.1. Inleiding

De vraag luidt of sprake is van in de uitvoeringspraktijk ingebedde en gehanteerde waarborgen ter bescherming van het recht op privacy. Dit ter bevordering van voldoende balans tussen gegevensverwerking en de bescherming van de privacy. In onderstaande paragrafen wordt, aan de hand van de in de vorige paragrafen door de onderzoekers geconstateerde risico's van gegevensverwerking, antwoord gegeven op deze vraag.

3.4.2. Uniforme wijze van gegevensverwerking

Om een uniforme wijze van gegevensverwerking te bewerkstelligen, ter voorkoming van het naar eigen inzicht verwerken van gegevens, geldt voor interne medewerkers, waaronder ook de leden van de sociaal teams, dat in ieder geval de Beleidsregels Wmo 2015 en de Leertuin bepalend zijn. Hoewel geen sprake is van stappenplannen of gestandaardiseerde protocollen, bevatten de beleidsregels en de Leertuin enig houvast. Bovendien is in de gevoerde gesprekken gebleken dat zowel de leden van de sociaal teams, als het Toegangsteam Jeugd de bijeenkomsten over de Leertuin hebben gevolgd.

Als het gaat om gegevensverwerking zijn geen verdere werkprocessen, of verantwoordelijkheden en bevoegdheden vastgelegd. Opvallend is dat vanuit het college niet is voorgeschreven om te werken met bijvoorbeeld gestandaardiseerde formulieren.[22] Leden van een sociaal team hebben gewezen op de situatie waarin ten aanzien van een dementerende burger ad hoc een toestemmingsformulier is opgesteld. Ook is onvoldoende zicht op hoe door medewerkers mag worden gehandeld, in geval dat informatie reeds binnen de gemeente bekend is. In hoeverre de wijze van vraagstelling (in geval van huisbezoeken of vraagstelling aan derden) op uniforme wijze plaatsvindt, zowel als het gaat om de Wmo 2015 als de Jeugdwet, valt ook geen antwoord te geven. Verder ontbreekt voorlichtingsmateriaal dat gebruikt kan worden richting burgers.

Het staat niet vast dat gegevensverwerking door alle betrokkenen op dezelfde wijze gebeurt. Voor vragen omtrent gegevensverwerking is door gesprekspartners regelmatig verwezen naar de juridisch medewerkers van Team Mens en Maatschappij (waaronder ook de jurist bezwaar en beroep). De privacyregels zouden mogelijk op uniforme wijze worden gehanteerd, indien alle betrokkenen deze collega's raadplegen bij vraagstukken omtrent de privacy. Maar er valt niet met duidelijkheid te zeggen dat iedereen een beroep op deze medewerkers doet. Het volgen van de Leertuin biedt ook geen garanties dat door een ieder op dezelfde wijze gewerkt wordt, dit blijkt uit door gesprekspartners gegeven antwoorden omtrent het privacybeleid. Ook het feit dat tot de sociaal teams en het Toegangsteam Jeugd enkele nieuwe medewerkers zijn gaan behoren, maakt dat niet iedereen de deze Leertuin kent. Bovendien wordt in de Beleidsregels Wmo 2015 niet verwezen naar de Leertuin, omdat daarover op het moment van het vaststellen van de beleidsregels nog weinig bekend was.

3.4.3. Gebruik van grondslagen

In de Beleidsregels Wmo 2015 wordt nadrukkelijk gesproken van termen als 'noodzakelijkheid', 'het doel waarmee gegevens worden verwerkt' en 'ondubbelzinnige toestemming'.

[22] Behalve voor zover dat gestandaardiseerde gespreksverslagen en meldingsformulieren betreft.

Hiermee lijkt het college in elk geval waarborgen te hebben ingebouwd voor het zorgvuldig verwerken en verstrekken van persoonsgegevens.

Opvallend is echter dat het begrip noodzakelijkheid niet nader is uitgewerkt of is afgebakend door daaraan verwante begrippen zoals subsidiariteit (is het delen van de informatie écht noodzakelijk en de minst ingrijpende maatregel?) en proportionaliteit (is het delen van al deze informatie noodzakelijk? Staan de maatregel en het doel met elkaar in verhouding?). Deze begrippen komen bijvoorbeeld wel tot uiting in het Zwitsers Zakmes dat door enkele medewerkers wordt gebruikt. Ook de doelmatigheid ontbreekt in de vastgelegde beleidsdocumenten.

Een medewerker administratie over informatieverstrekking
"Als bijvoorbeeld een zus vragen stelt over haar broer aan wie een Pgb is verstrekt, dan heb ik toestemming van de cliënt nodig om die vragen te beantwoorden. Die toestemming wordt vervolgens schriftelijk toegestuurd en als een handtekening ontbreekt dient die te worden nagestuurd., Dat is de wijze waarop wij handelen. Je weet immers nooit zeker of degene die belt wel de persoon is die deze zegt te zijn. Stel dat het zou gaan om een mantelzorger die informatie vraagt, dan wordt die informatie ook niet zonder meer gegeven."

3.4.4. Systeemtechnische beveiliging

In het kader van dit onderdeel zijn documenten bestudeerd die zien op informatiebeveiliging.

Informatiebeveiligingsbeleid
Als overkoepelende visie ten aanzien van informatiebeveiliging kent de gemeente Tynaarlo het zogeheten 'Informatiebeveiligingsbeleid Tynaarlo' (hierna: het Informatiebeveiligingsbeleid) waaruit beleidsuitgangspunten over informatiebeveiliging blijken.[23] Uit het Informatiebeveiligingsbeleid volgt dat passende technische en organisatorische maatregelen zullen worden getroffen om gemeentelijke informatie te beschermen en te waarborgen dat de gemeente voldoet aan wet- en regelgeving. Naast technologische beveiliging, wordt ook over het belang van bewustwording bij de organisatie, het management en de medewerker gesproken.

Visie
De komende jaren zal de gemeente Tynaarlo de aandacht besteden die nodig is voor het borgen van de veiligheid van informatie en het verder professionaliseren van de IB-functie in de organisatie. Hierbij werken we zoveel mogelijk samen met de gemeenten Aa en Hunze, Assen en Noordenveld. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.[24]

Uit het Informatiebeveiligingsbeleid blijkt dat de Informatiebeveiligingsfunctionaris/Security Officer (SO) de organisatie vanuit een onafhankelijke positie ondersteunt bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en het rapporteren daarover.

[23] Gemeente Tynaarlo, Informatiebeveiligingsbeleid, Beleidsuitgangspunten over informatiebeveiliging, Vries, april 2015.
[24] Gemeente Tynaarlo, Informatiebeveiligingsbeleid, Beleidsuitgangspunten over informatiebeveiliging, Vries, april 2015, p. 5.

Regels en verantwoordelijkheden voor het beveiligingsbeleid worden vastgelegd en vastgesteld en alle medewerkers worden getraind in het gebruik van beveiligingsprocedures. Verder zou iedere medewerker, zowel vast als tijdelijk, intern of extern, verplicht zijn waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Informatiebeveiligingsbeleid ziet niet op privacy in het sociaal domein
Het Informatiebeveiligingsbeleid ziet op algemene uitgangspunten die gelden voor de gehele gemeentelijke organisatie.[25] Het beleid bevat echter geen uitgangspunten omtrent gegevensverwerking/privacy binnen het sociaal domein. Uit het gesprek met de Security Officer is gebleken dat onlangs een jurist is aangetrokken die wat betreft gegevensverwerking binnen het sociaal domein als aanspreekpunt zal fungeren (de functionaris gegevensbescherming). Hij zal onder andere in kaart brengen welke persoonsgegevens binnen het sociaal domein worden verwerkt of dit op juiste wijze gebeurt. Verder zal deze functionaris de (eventueel) overeengekomen bewerkersovereenkomsten[26] in kaart brengen om zodoende bewustwording te creëren. Er dient volgens de Security Officer veel meer aandacht te zijn voor kennis, houding en gedrag van betrokkenen binnen het sociaal domein. Dit is tevens van belang in het kader van de Wet meldplicht datalekken.

Aeolus Back
Ten aanzien van de uitvoering van de taken binnen het sociaal domein wordt gebruik gemaakt van het systeem Aeolus Back (hierna: Aeolus). Aeolus betreft zogeheten software ten behoeve van de decentralisaties. In Aeolus worden alle documenten, zoals meldingsformulieren, gespreksverslagen en beschikkingen, die in het kader van de uitvoering van de taken binnen het sociaal domein worden opgesteld, opgeslagen. Sommige gesprekspartners geven aan dat dit ook geldt voor aantekeningen en telefoonnotities. Uit gesprekken met leden van de sociaal teams blijkt dat alleen nog door maatschappelijk werkers gebruik gemaakt wordt van fysieke dossiers en dat die in een afgesloten kast worden bewaard.

Autorisaties
Aeolus is een zogeheten webbased programma, wat betekent dat het ook thuis kan worden gebruikt. Volgens gesprekspartners vergrendelt het systeem wanneer de gebruiker een periode niet actief is geweest. Uit het document 'Gebruikers en rechten Aeolus Back', volgen autorisaties per medewerker. De leden van de sociaal teams hebben aangegeven dat Aeolus van voldoende schotten is voorzien en dat persoonlijke documenten voldoende kunnen worden afgeschermd. Het systeem maakt het mogelijk zaken als 'privacygevoelig' aan te duiden. De leden van de sociaal teams geven aan onderling elkaars dossiers in te kunnen zien, maar alleen binnen het eigen team. Er bestaat geen toegang tot bij andere sociaal teams in behandeling zijnde dossiers. Het feit dat niet iedereen alle gegevens kan inzien, zou in sommige gevallen zelfs een soepele uitvoering bemoeilijken.

Administratie
Voor wat betreft administratieve handelingen, die verricht worden ten aanzien van de taken binnen het sociaal domein, blijkt dat gegevens inzake persoonsgebonden budgetten (Pgb's) en betalingen door de administratief medewerkers zelf worden ingevoerd in Aeolus. Medewerkers van de administratie hebben naar eigen zeggen inzicht in de genomen beschikkin-

[25] Uit bijlage 2 van het Informatiebeveiligingsbeleid blijken enkele doelstellingen/beheersmaatregelen ten aanzien van het gebruik van ICT-voorzieningen en het inzien van informatie/gegevens. Bijlage 3 spreekt over de beveiliging van personeel. De afdeling zou regelmatig moeten spreken over dit onderwerp en in werkoverleggen zou periodiek aandacht geschonken moeten worden aan informatieveiligheid.
[26] Een overeenkomst waarin wordt vastgelegd hoe met privacygevoelige informatie omgegaan dient te worden.

gen, want dat zou noodzakelijk zijn om de facturen te kunnen controleren. Vanuit de administratie is aangegeven dat het berichtenverkeer met externe partijen via een zogeheten portal gaat. Het gaat dan om betalingen, maar ook om het uitwisselen van gegevens met de SVB. Op deze wijze komen er bijvoorbeeld geen documenten in mailboxen terecht. Verder is gewezen op het door de accountant ontvangen van gegevens van cliënten, maar dat deze een beroepscode heeft waaraan hij zich dient te houden. Gegevensuitwisseling met de account gaat overigens per e-mail.

De gesprekspartners hebben aangegeven dat Aeolus wat betreft de administratief medewerkers voldoende autorisaties bevat. Dit blijkt ook uit het document 'Gebruikers en rechten Aeolus Back'.

3.4.5. Met ketenpartners gemaakte afspraken en nakoming daarvan

Ten behoeve van de uitvoering van de taken binnen het sociaal domein wordt veel samengewerkt met diverse ketenpartners. Van belang is welke afspraken het college met ketenpartners heeft gemaakt en of de verantwoordelijkheden wat betreft de borging van de bescherming van privacy voldoende duidelijk zijn. Het antwoord op de vraag welke afspraken met ketenpartners zijn gemaakt blijkt niet eenvoudig vindbaar. Door gesprekspartners is aangegeven dat er een protocol geldt voor wat betreft borging van de privacy. Ook raadsleden hebben aangegeven dat een dergelijk protocol zou bestaan.

Zoals eerder aangegeven, zie paragraaf 3.2.2, verwijzen zorgaanbieders als het gaat over regels aangaande privacy doorgaans naar de overeengekomen zorgcontracten.

In het kader van dit onderzoek is een viertal met zorgaanbieders afgesloten overeenkomsten bestudeerd. Dit betreft:

- de 'Overeenkomst specialistische begeleiding zintuiglijke beperking' (dat een van de VNG afkomstige modelovereenkomst betreft);
- de 'Overeenkomst betreffende het leveren van maatwerkvoorziening ondersteuning';
- de 'Overeenkomst trapliften 2012-2015'; en
- het 'Raamcontract Jeugdhulp – vrij gevestigden'.

Er is niet gebleken van het bestaan van bewerkersovereenkomsten of een zogeheten privacyprotocol. De overeenkomsten, behalve de 'Overeenkomst trapliften 2012-2015' bevatten slechts enkele minimale bepalingen over privacy.

Privacyregels in overeengekomen contracten

De 'Overeenkomst specialistische begeleiding ZG' zoals opgesteld door de VNG, bepaalt dat privacy- en bedrijfsgevoelige informatie, vergaard tijdens de transformatiegesprekken en/of reguliere contractgesprekken, niet gebruikt zullen worden in het contracteringsproces (artikel 5, lid 5, onder c). De 'Overeenkomst betreffende het leveren van een maatwerkvoorziening ondersteuning' vermeldt dat partijen geheimhouding/privacy zullen regelen conform de wettelijke eisen en landelijke standaarden en – indien nodig – medewerkers bewerkersovereenkomsten laten tekenen voor geheimhouding van de beschikbare informatie (artikel 10, lid 5). Uit het Raamcontract Jeugdhulp-vrij gevestigden volgt dat verwerking van persoonsgegevens bij de uitvoering van het Raamcontract geschiedt met inachtneming van de bij of krachtens de Wet bescherming persoonsgegevens gestelde voorschriften, onverminderd het overigens in het Raamcontract bepaalde (artikel 20, lid 1). Het tweede lid van hetzelfde artikel schrijft voor dat partijen passende organisatorische en technische maatregelen treffen voor het veilig kunnen uitwisselen van persoonsgegevens en vertrouwelijke informatie.

Sommige gesprekspartners hebben aangegeven dat de regels door ketenpartners als onoverzichtelijk worden beschouwd. Elke gemeente zou namelijk weer eigen regels hanteren voor de bescherming van privacy. Gesprekspartners geven daarnaast ook aan dat de meeste zorgaanbieders zich voldoende bewust zijn van de privacyregels. Een enkeling heeft echter onvoldoende aandacht voor de privacy van burgers. Het komt wel eens voor dat vanuit zorgaanbieders informatie wordt gedeeld die niet relevant is. Aan het niet willen delen van gegevens zou een zekere mate van starheid ten grondslag liggen. En dit zou zelfs gebeuren in situaties waarin cliënten zelf hebben aangegeven dat gegevens gedeeld mogen worden.

Een lid van het sociaal team over zorgaanbieders:
"Niet elke zorgaanbieder heeft voldoende aandacht voor de privacy van cliënten. Andersom gebeurt het ook dat zorgaanbieders zich daar juist té bewust van zijn en niet snel geneigd zijn gegevens te delen. In een bepaalde situatie is zelf een zogeheten zorgconferentie belegd, opdat informatie met leden van een sociaal team werden gedeeld."

Uit het gesprek met raadsleden blijkt dat hen geen signalen hebben weten te bereiken waaruit blijkt dat ketenpartners niet op juiste wijze met de privacy van burgers zouden omgaan. Door hen wordt dan ook gewezen op het feit dat de meeste ketenpartners als jarenlang met protocollen werken. Het zou echter onduidelijk zijn in hoeverre die protocollen overeenstemmen met de door de gemeente Tynaarlo gehanteerde regels.

3.4.6. Gebruik van portals

Uit de gevoerde gesprekken met de ketenpartners blijkt dat gebruik wordt gemaakt van portals ten behoeve van gegevensoverdracht tussen de gemeente en ketenpartners. Alle contacten zouden via dit portal moeten verlopen, al wordt hiervan volgens gesprekspartners in de praktijk wel eens afgeweken. Het is niet duidelijk welke andere partijen bevoegd zijn via dit portal te werken. Zo zouden de sociaal teams hierop wel zijn aangesloten, maar de administratie niet. Voor versleutelde gegevensoverdracht is ook gewezen op het systeem Citrix, dat fungeert als zogeheten beveiligde omgeving.

Tijdens de gevoerde gesprekken zijn verschillende portals genoemd. Het is de onderzoekers niet duidelijk geworden welke portals verplicht zijn voorgeschreven. Hierover is aangegeven dat de portals pas per 2016 beschikbaar waren. Dit zou te maken hebben met het enigszins trage handelen door de Rijksoverheid en de VNG.

Door zorgaanbieders is gewezen op het belang van eenduidig werken. Voorts is door enkele medewerkers aangegeven dat ook in geval van nieuwe zorgaanbieders deze tijdig op de hoogte gesteld moeten worden omtrent het aanleveren van facturen via de portal.

Door de Security Officer is opgemerkt dat het is voorgekomen dat zorgaanbieders per e-mail excelbestanden met gevoelige informatie delen. De Security Officer houdt hier toezicht op en een formele brief met uitleg van de regels volgt, mocht het nogmaals plaatsvinden. Opvallend is dat vanuit zorgaanbieders juist is aangegeven dat het regelmatig is voorgekomen dat e-mails met bijlagen voorzien van cliëntgegevens, vanuit andere partijen naar hen worden verzonden.

Een zorgaanbieder aan het woord
"Wij zijn er zelf achter gekomen dat we niet zomaar BSN gegevens over de mail moeten versturen. Dat gebeurde eerder, aan het begin van de nieuwe Wmo 2015, wel. In 2014 was er amper beleid ten aanzien van een veilige gegevensoverdracht. Begin 2016 kwamen er

ook nog veel uitvragen over de mail, inclusief BSN-gegevens. Een zekere gemeente stuurde alle gegevens gewoon per e-mail. Dat hebben wij niet geaccepteerd. We hebben toen een brief retour gezonden waarin we hebben geschreven dat we dat anders wilden. Ook onderlinge communicatie en het versturen van gegevens gebeurt tussen partijen, maar daarvoor hebben wij gewoon een portal. Dus gegevens worden dan onveilig verstuurd, terwijl we hiervoor wel instructies hebben gegeven."

Naast bovenstaande is het voor het in kaart brengen van de risico's van gegevensverwerking en daartoe in te bouwen waarborgen ook van belang rekening te houden met de Algemene Verordening Gegevensbescherming die op 25 mei 2018 in werking treedt.

3.5 Conclusie

Voor wat betreft de regelgeving omtrent privacy wordt door gesprekspartners naar verschillende bronnen verwezen. Het merendeel van de gesprekspartners acht de Wmo beleidsregels, de gevolgde Leertuin en van toepassing zijnde beroepscodes bepalend. Zorgaanbieders verwijzen naar met de gemeente in het kader van contractering gemaakte afspraken. Een bepaalde zorgaanbieder ontwikkelt eigen privacybeleid.

Door alle gesprekspartners is aangegeven dat het door de cliënt/de ouders verlenen van toestemming belangrijk is voor het al dan niet mogen verwerken en verstrekken van persoonsgegevens. In crisissituaties wordt door de gesprekspartners terecht meteen ingegrepen en niet gewacht op de in de andere gevallen vereiste toestemming. Er bestaat geen eenduidig beeld omtrent het al dan niet gebruiken van toestemmingsformulieren in geval dat bijvoorbeeld informatie bij derden dient te worden opgevraagd.

De meeste gesprekspartners geven aan dat vrij snel aan de cliënt duidelijk gemaakt dient te worden waarom bepaalde informatie moet worden gedeeld. Als de gegevens op het moment van de aanvraag niet volledig en correct zijn, kan de aanvraag volgens de gesprekspartners niet in behandeling worden genomen. In dit kader is van belang dat cliënten voor hulp of ondersteuning doorgaans afhankelijk zijn van de gemeente en dat – zie ook het onderzoek van de Autoriteit Persoonsgegevens - toestemming eigenlijk geen juiste grondslag is.

Gegevensverwerking vindt volgens de gesprekspartners plaats op basis van het noodzakelijkheidsprincipe en zoals aangegeven enkel met toestemming van de cliënt/de jeugdige/de ouders. Hoewel gesprekspartners aangeven dat op eenduidige wijze wordt gewerkt, is dit volgens de onderzoekers lang niet altijd het geval. Dit blijkt onder andere uit het feit dat toestemming voor bijvoorbeeld het opvragen en verwerken van gegevens op verschillende manieren gevraagd en vastgelegd wordt, voor wat betreft regelgeving wordt verwezen naar verschillende bronnen, en het feit dat er geen voorlichtingsmateriaal voor burgers bestaat. Ook over de wijze waarop gegevens mogen worden gedeeld (schriftelijk of per e-mail) wordt verschillend gedacht en doet twijfelen aan de uniformiteit van werken.

Risico's
Risico's aangaande gegevensverwerking bestaan op het gebied van niet uniform werken, foutief gebruik van grondslagen, systeemtechnische beveiliging en het al dan niet naleven van eventuele met ketenpartners gemaakte afspraken. Binnen de gemeente Tynaarlo ontbreekt het, behalve de bepalingen in de Beleidsregels Wmo 2015 en de voorschriften vanuit de Leertuin, aan duidelijk privacybeleid. Logischerwijs is veel aandacht uit gegaan naar zorg-

continuïteit en de inkoop van nieuwe zorgtaken. Op grond van de onderzochte documenten, alsmede de gevoerde gesprekken, zijn risico's wat betreft gegevensdeling onvoldoende in kaart gebracht. Daarentegen zijn er echter wel waarborgen ingebouwd ter bescherming van de privacy van burgers, maar deze zijn niet beschreven vanuit een duidelijke risicobeschrijving.

Hoewel gesprekspartners allen hebben aangegeven voldoende aandacht voor de privacy van burgers te hebben, en de onderzoekers niet twijfelen aan de professionaliteit en kundigheid van deze gesprekspartners, is ook geconstateerd dat werkprocessen, verantwoordelijkheden en bevoegdheden aangaande privacyrecht onvoldoende zijn vastgelegd. Door het college is voorts ook geen onderscheid gemaakt tussen algemene en bijzondere persoonsgegevens. Daarnaast zijn medewerkers zich, als het gaat om het verwerken van gegevens, onvoldoende bewust van het gebruik van juridische grondslagen. Dit vergroot de kans op het naar eigen inzicht invullen van te hanteren normen. Er kan dan ook niet met zekerheid gezegd worden dat sprake is van een uniforme werkwijze. In dit kader is van belang te benadrukken dat er echter geen signalen van misstanden of anderszins onrechtmatig handelen zijn.

Het Informatiebeveiligingsbeleid ziet niet op gegevensverwerking en –verstrekking binnen het sociaal domein. Naast de aangetrokken Security Officer is sinds enige tijd een Functionaris Gegevensbescherming binnen de gemeente Tynaarlo werkzaam die onder andere zal toezien op privacy naleving. Dit achten de onderzoekers een goede ontwikkeling. Het systeem Aeolus Back voorziet volgens de onderzoekers in voldoende beveiliging van documenten. Het document 'Gebruikers en rechten Aeolus Back' is overzichtelijk ten aanzien van autorisaties. Het is van belang hierop te blijven toezien bij de komst van eventuele nieuwe medewerkers.

Drie van de vier bestudeerde overeenkomsten, bevatten een bepaling over privacy. Een privacyprotocol of een bewerkersovereenkomst bestaat niet. Afspraken over door zorgaanbieders in acht te nemen zorgvuldigheidseisen en op hen rustende verantwoordelijkheden aangaande de privacy van cliënten liggen dan ook onvoldoende vast. Zorgaanbieders hebben over het algemeen voldoende aandacht voor de privacy van cliënten. Maar het is in de beginfase van de decentralisaties ook voorgekomen dat gegevens werden gedeeld op een manier die niet voorgeschreven is. Tijdens het onderzoek is gebleken van het gebruik van verschillende portals. Het is niet duidelijk welke portals verplicht zijn voorgeschreven. Bovendien ontbreekt een overzicht betreffende het gebruik daarvan en of daarop toezicht worden gehouden.

Als het gaat om risico's en te nemen maatregelen/in te bouwen waarborgen is de toekomstige Algemene Verordening Gegevensbescherming van belang, waaruit blijkt aan welke regels inzake de privacy van natuurlijke personen overheden gebonden zijn.

Op grond van vorenstaande zijn de onderzoekers van mening dat het college, steviger zou kunnen inzetten wat betreft risicobeheersing.

4

De rol van de gemeenteraad

4.1 Inleiding

Het derde onderzoeksthema betreft de rol van de gemeenteraad. In dit hoofdstuk staat de kaderstellende en controlerende rol van de raad centraal. Gekeken is welke formele rol de gemeenteraad heeft ten aanzien van het privacybeleid binnen het sociaal domein en hoe deze in de praktijk wordt ingevuld.

4.2 Sturingsmogelijkheden en -instrumenten

4.2.1. Inleiding

Gegevensverwerking binnen het sociaal domein gebeurt onder de verantwoordelijkheid van het college. Daarover legt het college vervolgens verantwoording af aan de gemeenteraad, zo stelt het Kabinet in de visie op privacy en gegevensuitwisseling in het sociaal domein 'Zorgvuldig en Bewust'.[27]

De kaderstellende rol van de raad is nauw verbonden met zijn controlerende rol. Wanneer heldere kaders worden gesteld, is het voor het college helder met welke opdracht en binnen welke randvoorwaarden het aan de slag dient te gaan. Over sturing en (democratische) controle door de raad op het gebied van het privacybeleid door de raad is veel te zeggen. Het begrip democratische controle kan daarbij ruim worden opgevat: alle voorzieningen die het raadsleden mogelijk maken om het privacybeleid te sturen en te controleren. Hieronder volgt óf, en in hoeverre, de raad van de gemeente Tynaarlo gebruik maakt van deze mogelijkheden.

4.2.2. Sturing en controle

Tot op heden hebben de raadsleden zich niet of nauwelijks bezig gehouden met het onderwerp privacy. Dat is gebleken uit het groepsgesprek dat met raadsleden heeft plaatsgevonden waarin zij hebben aangegeven dat zij weet hebben van een zogeheten privacyprotocol, maar dat het onderwerp privacy in het sociaal domein verder onderbelicht is gebleven. Dit heeft volgens hen alles te maken met het feit dat voorafgaand aan de decentralisaties met name oog is geweest voor de continuering van zorg en ondersteuning. Volgens raadsleden

[27] Rijksoverheid, Kabinetsvisie Zorgvuldig en bewust, Gegevensverwerking in een gedecentraliseerd sociaal domein. Zie ook de Handreiking VNG – Verantwoording privacy sociaal domein aan de gemeenteraad, oktober 2015.

zijn er, naast het privacyprotocol, mogelijk ook andere afspraken gemaakt, maar deze zouden onvindbaar zijn. Dit betreft volgens hen een belangrijk verbeterpunt.

Door raadsleden is aangegeven dat zij niet veel van het thema afweten, terwijl dit wel als steeds belangrijker wordt ervaren. Van sturen en controleren is het tot dusverre dan ook nog niet gekomen. Raadsleden wijzen op de raadsgroep waar thema's als privacy kunnen worden besproken.

4.2.3. Knelpunten

Binnen dit onderzoek is ook aan de orde gesteld of, en zo ja, welke, knelpunten door de raad worden ervaren als het gaat om sturing en controle op het privacybeleid binnen het sociaal domein.

Het feit dat regelgeving omtrent privacy als ingewikkeld en zeer divers wordt beschouwd, met als gevolg dat raadsleden niet altijd weten welke regels van toepassing zijn en hoe deze te interpreteren, wordt als een van de grootste knelpunten ten aanzien van sturing en controle door raadsleden beschouwd. Tegelijkertijd is door raadsleden aangegeven dat zij wél belang hechten aan het controleren van de wijze waarop procedures verlopen en of dit naar behoren gebeurt. Daarbij zijn raadsleden de mening toegedaan dat het onderwerp – afhankelijk van de wettelijke taak waaraan uitvoering wordt gegeven – op verschillende wijzen zou worden benaderd. Bovendien is gebleken dat het onderwerp privacy, gezien het belang bij de continuering van zorg bij de overkomst van nieuwe taken, niet als urgent werd gezien.

Een raadslid over privacy:
"Als het gaat om de Wmo loop je eerder tegen een dichte deur aan wat betreft hetgeen je al dan niet aan informatie mag prijsgeven. Rond de Participatiewet merk ik dat dit wat soepeler is."

Op de vraag of de raad voldoende door het college in de gelegenheid wordt gesteld om te sturen en te controleren is geen eenvoudig antwoord te geven. Beschikbare – vrij te delen – informatie zou doorgaans wel op aanvraag worden verstrekt. Door raadsleden is voorts aangeven dat zij worden geïnformeerd over zaken die misgaan. Zij zouden echter meer op regelmatige basis willen worden geïnformeerd over het onderwerp privacy. Het onderwerp staat momenteel namelijk niet vaak genoeg op de agenda.

4.3 Ervaringen

4.3.1. Inleiding

In deze paragraaf wordt de mate van tevredenheid van de raadsleden beschreven als het gaat om de wijze waarop in de praktijk aan bescherming van de privacy wordt gedaan. De vraag luidt in hoeverre raadsleden hierover – voor zover zij daarover geïnformeerd zijn – al dan niet positief gestemd zijn.

Raadsleden hebben allereerst aangegeven dat het aantal klachten zoals door burgers over dit onderwerp is ingediend opvallend laag is te noemen. Zoals eerder aangegeven hebben zij onvoldoende zicht op de wijze waarop in de praktijk aan de bescherming van de privacy van burgers wordt voldaan, omdat privacy een onderbelicht thema is geweest en raadsleden niet op regelmatige basis door het college over dit thema worden geïnformeerd. In het kader van dit onderzoek is echter een tweetal andere onderwerpen door hen aangesneden, waarop in onderstaande paragrafen nader wordt ingegaan.

4.3.2. Informeren van burgers

Als het gaat om het informeren van burgers, wijzen de raadsleden op het gebrek aan informatie op bijvoorbeeld de gemeentelijke website. Voor burgers zou bijvoorbeeld een handleiding moeten bestaan met daarin informatie omtrent het recht op privacy en de wijze waarop gegevensverwerking plaatsvindt.

Een raadslid over het belang van informatie voor burgers:
"Een handreiking, of een soortgelijk document, zou nuttig zijn voor burgers. Nu weten zij niet welke regels er zijn op het gebied van privacy recht. Al zou het maar één A4'tje met informatie zijn. Daaraan bestaat wel behoefte. Bovendien creëer je daarmee vertrouwen."

Door de raadsleden is aangegeven dat de decentralisaties gepaard zijn gegaan met veel werk en dat bepaalde zaken – zoals de privacy – daardoor zijn blijven liggen. Veel aandacht is logischerwijs uitgegaan naar organisatorische zaken, zoals inkoop en ICT-systemen. Dit met het oog op zorgcontinuering. Dat thans (meer) aandacht wordt gevestigd op zorgvuldige gegevensverwerking wordt dan ook toegejuicht.

4.3.3. Delen van gegevens met raadsleden

In gesprekken met raadsleden en de wethouder is naar voren gekomen dat raadsleden soms bepaalde zaken willen weten vanuit hun rol als volksvertegenwoordiger, maar dat het niet altijd zonder meer mogelijk is om gegevens te verstrekken over bepaalde individuen. Dit zou een continue botsing zijn tussen raadsleden en uitvoerenden. Hoewel het de wethouder te doen is om raadsleden correct te informeren, kan hij – voor zover hij volledig in een casus is doorgevoerd – ook niet altijd alles prijsgeven, gelet op de privacy van betrokkenen.

Bovenstaand beeld is ook bevestigd door de overige gesprekspartners. Volgens hen is het regelmatig voorgekomen dat een raadslid om informatie over een specifieke cliënt heeft verzocht. Volgens de medewerkers was in die gevallen sprake van te vergaande bemoeienis op cliëntniveau. In die situatie zou volgens hen integriteit van raadsleden verwacht mogen worden, wat betekent dat zij de cliënt terugverwijzen naar het sociaal team of de cliënt moeten wijzen op het indienen van de klacht via de officiële klachtenprocedure.

Een medewerker:
"Mijn grootste knelpunt richting de politiek betreft de vraag omtrent het al dan niet delen van informatie. Daarover moeten afspraken worden gemaakt. Het komt wel eens voor dat men vanuit de politiek afspraken met bijvoorbeeld ouders maakt. Wij worden vervolgens op deze afspraken aangesproken, terwijl wij daarin niet gekend zijn. Politici moeten zich beseffen dat ze zorgvuldig behoren om te gaan met privacy gevoelige gegevens. Kortom, de rolverdeling wat betreft 'wat wel en niet te zeggen' moet duidelijker worden.

Raadsleden geven aan dat het wel eens gebeurt dat personen hen in privé aanspreken over situaties waarin deze personen verwikkeld zijn. Als raadslid zouden zij situaties op hoofdlijnen in de gaten kunnen houden, maar zich niet mogen mengen in individuele kwesties. Ook hierover zouden duidelijke afspraken moeten worden gemaakt.

Een raadslid:
"Als raadslid ben ik niet in de positie om iets te zeggen over individuele kwesties, maar dat is wel eens ingewikkeld. Ik verwijs dan altijd naar procedures of het sociaal team. Ik ga nooit in op concrete gevallen, maar je loopt als raadslid altijd het risico om uitspraken te doen over specifieke zaken. Ik weet niet of daarover ook afspraken zijn gemaakt. Ik zou dat echter wel op prijs stellen. Soms gebeurt het ook dat je als raadslid benaderd wordt en dat

je, voordat je er erg in hebt, al allerlei gegevens van iemand krijgt. Dit kan betekenen dat je dan opeens veel te veel weet, terwijl je al die informatie als raadslid niet hoeft te weten. Dan begeef je je op een hellend vlak. Hoewel je op elk terrein benaderd kunt worden, ligt het onderwerp privacy extra gevoelig."

Een financieel specialist:
"Er was sprake van een in de maandcijfers zichtbare grove Pgb overschrijding. Dit had echter te maken met een forse indicatie voor een bepaalde cliënt. Vanuit mijn taak richting de raad behoor ik hiervan melding te maken, maar aan de andere kant wil je niet dat iedereen weet dat deze cliënt een dergelijke indicatie toegekend heeft gekregen. Niet omdat hij er geen recht op heeft, maar je wil niet dat de gegevens van de cliënt op straat komen te liggen."

4.4 Conclusie

Tot op heden heeft de raad geen gebruik gemaakt van sturingsmogelijkheden en -instrumenten als het gaat om het onderwerp privacy binnen het sociaal domein.

Privacy is een onderbelicht thema gebleken. Dit heeft onder andere te maken met het feit dat er logischerwijs veel aandacht is uitgegaan naar organisatorische zaken zoals de inkoop van de nieuwe taken, maar ook het feit dat de privacy regels als ingewikkeld worden beschouwd ligt hieraan te grondslag. Raadsleden hechten wel belang aan het controleren van de wijze waarop procedures verlopen en of dit, privacy technisch, naar behoren gebeurt. Zij zouden graag meer op regelmatige basis geïnformeerd willen worden over het onderwerp privacy. Dit betreft ook het delen van ontwikkelingen in wet- en regelgeving en de gevolgen daarvan voor de gemeentelijke praktijk.

Volgens raadsleden is het noodzakelijk voorlichtingsmateriaal te ontwikkelen dat gebruikt kan worden om burgers op de hoogte te stellen van de regels omtrent privacy binnen het sociaal domein. Verder is het noodzakelijk duidelijke afspraken te maken over het delen van informatie met raadsleden. Het doet zich voor dat raadsleden door burgers worden aangesproken over hun ervaringen met de gemeente. Er zouden duidelijke afspraken moeten worden gemaakt over het in die situaties al dan niet delen van informatie.

5

Conclusies en aanbevelingen

Met dit rekenkameronderzoek is beoogd de stand van zaken rondom de privacy binnen het sociaal domein in de gemeente Tynaarlo te beschrijven, wat betreft het beleid, de praktijk en de wijze waarop sturing binnen de gemeente plaatsvindt. Het is dan ook nadrukkelijk niet de bedoeling geweest een oordeel over voornoemde onderdelen te vellen. Naar aanleiding van het onderzoek is het formuleren van conclusies en aandachtspunten voor de toekomst een centraal onderdeel van het vierde en laatste thema. In dit hoofdstuk zijn de conclusies geformuleerd en is ook aangegeven welke aanbevelingen ter verbetering kunnen worden gedaan.

1. Beleid

Binnen de gemeente Tynaarlo bestaat geen duidelijke visie op privacy binnen het sociaal domein. Hoewel uit de Beleidsregels Wmo 2015 en enige documenten over de uitvoering van de Jeugdwet bepalingen over gegevensverwerking blijken (de verwijzing naar de Leertuin), ontbreekt een helder afwegingskader of bijvoorbeeld een privacy protocol. Concrete doelen ten aanzien van gegevensverwerking zijn dan ook niet bekend, wat maakt dat de doeltreffendheid van het beleid niet beoordeeld kan worden.

Gegevensverwerking dient – blijkens de door het college vastgestelde Beleidsregels Wmo 2015 – plaats te vinden op basis van noodzakelijkheid. Medewerkers behoren hier voorts transparant over te zijn richting burgers. Voor zover het beleid is vastgelegd voldoet het volgens de onderzoekers aan de wettelijke kaders en biedt het handvatten. Opvallend is echter dat voor de uitvoering belangrijke begrippen zoals ‘noodzakelijkheid’ en ‘toestemming’ niet nader zijn uitgewerkt. Dit betekent dat het beleid blijft hangen in theoretische kaders en daarmee niet praktisch uitvoerbaar is. Voor wat betreft de Jeugdwet is verwezen naar de Leertuin, maar blijkt niet duidelijk welke werkwijze voor medewerkers geldt ten aanzien van de privacy binnen het sociaal domein. De onderzoekers zijn dan ook van mening dat geen sprake is van doelmatig beleid.

Als burgers onvoldoende informatie verstrekken, blijkt uit de Beleidsregels Wmo 2015 dat een gevolg daarvan kan zijn dat een negatief besluit op de aanvraag wordt genomen. Burgers worden op het moment van de melding echter meteen gevraagd om het geven van

toestemming voor het delen van gegevens. Uitgangspunt van de Wmo 2015 is echter het ondersteunen van kwetsbare personen die vanwege beperkingen niet in staat zijn tot zelfredzaamheid of maatschappelijke participatie. In geval van de Jeugdwet gaat het om het bieden van noodzakelijk jeugdhulp. Het op voorhand uitsluiten van burgers wat betreft het recht op ondersteuning/jeugdhulp - wegens een weigerachtige houding omtrent het verstrekken van gegevens – getuigt niet van doelmatig privacybeleid. Bovendien is het gezien de afhankelijkheidsrelatie – personen kunnen voor de gewenste ondersteuning doorgaans alleen een beroep op de gemeente doen – noodzakelijk om met burgers in overleg te treden omtrent de noodzakelijke gegevens. Het beleid bevat hiertoe onvoldoende handvatten.

In mei 2018 treedt de Europese Algemene Verordening Gegevensbescherming in werking. Deze Verordening bevat regels omtrent de verwerking van persoonsgegevens die ook gelden voor gemeentelijke organisaties. Op grond van de Verordening worden aan verwerkers van persoonsgegevens verplichtingen opgelegd, zoals het uitvoeren van een Privacy Impact Assessment als het aanstellen van een zogeheten functionaris voor gegevensbescherming. Ontwikkelingen rondom het privacyrecht, zowel op Europees als nationaal niveau, dienen binnen de gemeente onder de aandacht te worden gebracht.

Aanbevelingen:
Ontwikkel aan de hand van doelstellingen duidelijk privacybeleid (waaronder een privacy protocol) en verspreid dit zowel onder interne medewerkers en ketenpartners.

Heb bij het ontwikkelen van het privacybeleid voldoende aandacht voor de afhankelijkheidsrelatie tussen kwetsbare burgers en de gemeente.

Houd bij het ontwikkelen van het beleid rekening met de inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming.

2. Balans tussen gegevensverwerking en de bescherming van privacy

Niet alle medewerkers zijn bekend met het privacybeleid van de gemeente. Bovendien verwijzen gesprekspartners naar verschillende documenten c.q. regelgeving als het gaat om de grondslag van gegevensverwerking. Regelmatig is terecht gezegd dat alles geschiedt op basis van noodzakelijkheid. Er bestaat geen eenduidig beeld over het gebruik van bijvoorbeeld toestemmingsformulieren voor het opvragen van informatie. Sommige gesprekspartners hebben aangegeven dit wel te gebruiken, terwijl anderen zeggen dat een dergelijk formulier niet bestaat. Hoewel de meeste gesprekspartners aangeven dat medewerkers eenduidig werken, is dit volgens de onderzoekers niet zonder meer het geval.

Risico's van gegevensverwerking zien op het niet eenduidig verwerken van gegevens, verkeerd gebruik van grondslagen en invulling van normen, systeemtechnische beveiliging, en het door ketenpartners onjuist omgaan met de privacy rechten van burgers.

Volgens de onderzoekers heeft het college onvoldoende waarborgen ingebouwd opdat gesproken kan worden van een uniforme werkwijze ten aanzien van gegevensverwerking. Dit geldt eveneens voor het gebruik van grondslagen, daarover ligt immers onvoldoende vast. Wat betreft systeemtechnische beveiliging geldt een algemeen Informatiebeveiligingsbeleid, dat echter niet ziet op de taken binnen het sociaal domein. Binnen het sociaal domein wordt gewerkt met Aeolus Back, waarvoor geldt dat voldoende aandacht is geschonken aan

autorisaties. Verder is van met ketenpartners gemaakte afspraken omtrent gegevensverwerking niet gebleken. Sommige gesprekspartners verwijzen naar een protocol, maar van het bestaan daarvan is niet gebleken. Ook in contractering is weinig aandacht aan privacy besteed. Ketenpartners hebben aangegeven zich voldoende bewust te zijn van het bestaan van de privacy regels, terwijl het volgens gesprekspartners in de praktijk ook is voorgekomen dat niet noodzakelijke informatie wordt gedeeld. Een helder afwegingskader zou dit voorkomen. Van ketenpartners wordt verwacht via portals te werken, maar in de praktijk wordt hiervan wel eens afgeweken. Volgens ketenpartners zijn door hen ook regelmatig gegevens per e-mail ontvangen.

In het licht van bovenstaande wensen de onderzoekers te benadrukken dat, naast de zoektocht omtrent het al dan niet verstrekken van bepaalde gegevens en de wijze waarop gegevens over en weer worden gedeeld, geen sprake is van in de praktijk gebleken grove misstanden op het gebied van gegevensverwerking. Dit heeft te maken met het feit dat zowel gemeenteambtenaren als medewerkers van zorgaanbieders zich professioneel opstellen.

Aanbevelingen:
Geef medewerkers en ketenpartners duidelijke – en regelmatige terugkerende – instructies over de toepassing van het privacybeleid.

Licht toe welke grondslagen gelden voor het verwerken van gegevens, opdat medewerkers deze grondslagen op dezelfde wijze hanteren.

Zie toe op eenduidige toepassing van het privacybeleid door bijvoorbeeld de Security Officer of de onlangs aangetrokken Functionaris Gegevensbescherming.

Ontwikkel een praktijk waarin wordt gewerkt met gestandaardiseerde formulieren voor het bij derden opvragen van informatie.

Blijf toezien op duidelijke autorisaties in Aeolus, beheer deze autorisaties en instrueer medewerkers over het gebruik van dit systeem.

Leg zowel aan medewerkers als aan ketenpartners duidelijk het vereiste gebruik van portals uit.

Zie toe op het gebruik van de portals bijvoorbeeld door de Security Officer of de onlangs aangetrokken Functionaris Gegevensbescherming.

Evalueer het privacybeleid en de uitvoering daarvan.

3. Kaderstellende en controlerende rol van de raad

Raadsleden hebben zich tot op heden nauwelijks beziggehouden met het onderwerp privacy. Het feit dat regelgeving omtrent privacy als ingewikkeld en zeer divers wordt beschouwd, met als gevolg dat raadsleden niet altijd weten welke regels van toepassing zijn en hoe deze te interpreteren, wordt als een van de grootste knelpunten ten aanzien van sturing en controle door raadsleden beschouwd. Door raadsleden is de wens geuit dat vanuit de gemeente meer wordt gedaan aan informatievoorziening van burgers als het gaat om de regels op het gebied van privacy binnen het sociaal domein. Ook zouden er duidelijke afspraken moeten worden gemaakt ten aanzien van het met raadsleden delen van gegevens.

Aanbevelingen:
Informeer raadsleden op regelmatige basis over de ontwikkelingen inzake het privacy recht (hiertoe behoort ook de Europese Algemene Verordening Gegevensbescherming).
Ontwikkel een folder – of een soortgelijk document – waarmee aan de wens wordt voldaan om burgers te informeren over het privacy recht.

Maak duidelijke afspraken over de met raadsleden te delen informatie.

Bestuurlijk wederhoor

Rekenkamercommissie gemeente Tynaarlo
t.a.v. mevrouw B. Slofstra, ambtelijk secretaris
Postbus 5
9481 AW VRIES

Onderwerp: Bestuurlijke reactie op Rapport RKC - Privacy Sociaal Domein

Geachte commissie,

Op 17 januari 20167 hebben wij het rapport Privacy in het Sociaal Domein van Pro Facto ontvangen. We danken u voor uw onderzoek. In deze brief geven wij onze reactie op dit rapport en beschrijven we welke acties we op dit gebied in de komende periode zullen plegen.

Aanbevelingen Rapport Privacy Sociaal Domein
We herkennen de huidige werkwijze en de stand van zaken met betrekking tot (beleids)documenten in hetgeen u beschrijft in uw rapport. We zijn blij met uw constatering dat in de praktijk geen grove misstanden zijn op het gebied van gegevensverwerking. De onderzoekers concluderen dat dit te maken heeft met het feit dat zowel gemeenteambtenaren als medewerkers van zorgaanbieders zich professioneel opstellen.
Wij herkennen de genuanceerde beschrijving van wat er wel en nog niet is gerealiseerd op het gebied van borging en bescherming van Privacy, waarbij in hoofdstuk vijf een algemeen samenvattend beeld weergegeven wordt.

Zoals ook beschreven in het rapport heeft in de voorbereiding en in de eerste periode van werken met de nieuwe taken in het sociaal domein de nadruk gelegen op het bieden van continuiteit van zorg en ondersteuning. We hebben er voor gekozen eerst ‘het doen’ kwalitatief goed in te richten, waaronder ook valt het beschermen van de privacy van de doelgroepen. Hiertoe hebben we beleidsregels Wmo vastgesteld
en via de opleiding Leertuin werkafspraken gemaakt, We onderkennen dat een beleidsvisie en eenduidige werkwijze (intern en met netwerkpartners) nog onvoldoende zijn geborgd. Ook is voor inwoners nog geen informatie hierover beschikbaar.

We onderschrijven uw aanbevelingen. Privacy en de borging ervan is een belangrijk aspect van het werken bij een gemeente geworden. Sinds de transitie van het sociale domein is de hoeveelheid privacygevoelige informatie, die bij de gemeente wordt verwerkt, alleen maar toegenomen.

Doorontwikkeling
Ook door de aankomende Europese regelgeving staan we voor een aantal opgaven. Die willen we voortvarend oppakken. De Algemene Verordening Gegevensbescherming (AVG) treedt vanaf 25 mei 2018 in werking. Daarom dienen we een doorontwikkeling door te maken. Uw rapport onderschrijft dit belang.

Om een begin te maken aan deze doorontwikkeling is in juli 2016 een Functionaris Gegevensbescherming (FG) aangesteld. De FG heeft een controlerende en een adviserende rol.

In het Jaarplan Privacy 2017 is opgenomen dat er in 2017 een kapstokbeleid privacy vastgesteld wordt. Hierin komen in ieder geval de volgende onderwerpen aan bod:

- Governance
- Transparantie
- Rekenschap
- Privacy-services burger
- Legitimiteit
- Gemeentelijke visie
- Proportionaliteit
- Doelbinding
- Opslagbeperking
- Informatiekwaliteit
- Informatiebeveiliging

Om tot een pragmatische aanpak te komen wordt het beleid opgesteld naar de bedoeling van de wetgever, en niet naar de letter. De borging van een goede privacy gaat voornamelijk over de bescherming van onze burgers en daarom moet er door een praktische bril naar gekeken worden; het gaat uiteindelijk om klantgerichtheid. Om tot dit beleid te komen wordt de expertise van een extern bureau ingeschakeld (Privacy Management Partners). Geschat wordt dat er aan het einde van het derde kwartaal 2017 een kapstokbeleid ligt.

Vervolgens wordt ingezoomd op de specifieke domeinen. Een risicogerichte aanpak is hierbij van belang. Het is dan ook logisch dat het Sociaal Domein hierbij als eerste aan bod komt. Door het gebruik van Privacy Impact Assessments (PIA's) op de werkprocessen wordt geïnventariseerd in hoeverre er maatregelen nodig zijn om een AVG-conforme aanpak te creeren. Daarbij worden ook de aanbevelingen vanuit het rapport meegenomen. Met deze aanpak wordt aangesloten bij het kapstokbeleid om zo te komen tot een uniforme wijze van gegevensverwerking.

Aanbevelingen rapport Privacy Sociaal Domein
In uw rapport wordt een dertiental aanbevelingen gegeven, die zijn onderverdeeld in de onderdelen beleid, balans tussen gegevensverwerking en de bescherming van privacy en als laatste de kaderstellende en controlerende rol van de raad. Door het opstellen van het hierboven genoemde kapstokbeleid wordt gedeeltelijk tegemoetgekomen aan uw aanbevelingen.

Beleid
Nadat het kapstokbeleid is opgesteld, zal er worden ingezoomd op het sociaal domein en worden, zo nodig, maatregelen genomen met inachtneming van de bedoeling achter de specifieke in de Wmo en Jeugdwet opgenomen privacy bepalingen.

Balans tussen gegevensverwerking en de bescherming van privacy
Om hierin een goede balans te vinden, wordt momenteel gewerkt aan het opstellen van een aantal gestandaardiseerde formulieren (gespreksverslagen en opvragen informatie van derden en gemaakte afspraken over het gebruik van portals).

We zullen de medewerkers en ketenpartners duidelijk en regelmatig instructies gegeven over de toepassing van ons privacybeleid. Hetzelfde geldt voor het eenduidig en gestandariseerd werken, zowel via formulieren als onze geautomatiseerde systemen (Aeolus). De gemeente Tynaarlo maakt vanaf 1 januari 2017 voor de facturering van de zorgkosten gebruik van het zgn. digitale berichtenverkeer, waarmee de privacy rondom de zorgkosten van onze cliënten optimaal wordt gewaarborgd. Ook maken we in toenemende mate gebruik van zogenaamd 'secured' emailverkeer, waardoor berichten via de email met cliëntgegevens extra worden beveiligd.

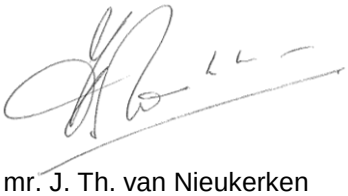
Kaderstellende en controlerende rol van de raad
Een van de aanbevelingen betreft het maken van duidelijke afspraken over de met raadsleden te delen informatie. Graag gaan wij met de raadswerkgroep aan het werk om tot een invulling te komen van deze afspraken.

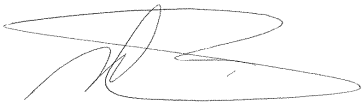
Ook wij zien een meerwaarde in een folder voor de burger, waarin informatie wordt gegeven over het privacyrecht. Om hier een goede invulling aan te geven, zal dit worden opgepakt als het kapstokbeleid vastgesteld is.

We zullen in de raadswerkgroep overleggen op welke wijze we de gemeenteraad informeren over de ontwikkelingen op het gebied van privacy.

Vragen
We gaan ervan uit u hiermee voldoende te hebben geïnformeerd. Mocht u nog vragen hebben, dan kunt u contact opnemen met Anneke van der Geest, senior adviseur Beleid Sociaal Domein.

Met vriendelijke groet,
burgemeester en wethouders





mr. J. Th. van Nieukerken
gemeentesecretaris

drs. M.J.F.J. Thijsen
burgemeester

Nawoord Rekenkamercommissie gemeente Tynaarlo

In dit nawoord spreken wij eerst een woord van dank uit aan de ambtelijke organisatie voor de goede samenwerking gedurende het onderzoek. Daarnaast gaat onze dank uit naar de geïnterviewden tijdens dit onderzoek.

De Rekenkamercommissie is verheugd om te vernemen dat het college zich herkent in de genuanceerde beschrijving in het rapport van wat er wel en nog niet is gerealiseerd op het gebied van de borging en bescherming van de privacy en er al een start is gemaakt met maatregelen die tegemoetkomen aan de aanbevelingen.

De taakuitbreiding binnen het sociaal domein bracht voor alle gemeenten verschillende nieuwe en ingrijpende uitdagingen met zich mee. Uit diverse onderzoeken was bekend dat bij gemeenten de regels rondom de privacy in het sociaal domein nog niet goed geïmplementeerd waren. De ambitie van de rekenkamercommissie met dit onderzoek was te beschrijven hoe het zit met de privacy in het sociaal domein, in beleid, in de praktijk en bij de sturing om vervolgens adviezen te kunnen geven die leiden tot verbetering.

De commissie ziet dit rapport dan ook als onderdeel van een zoektocht naar oplossingen en controle en denkt hiermee de gemeenteraad meer inzicht te hebben gegeven in de ontwikkelingen en sturingsmogelijkheden op dit terrein. Het blijf daarbij zaak zoals ook in de aanbevelingen is aangegeven dat de raad ook op dit terrein op regelmatige basis wordt geïnformeerd.