Rekenkamer Arnhem

Privacy made in [Arnhem]

Privacy en informatieveiligheid in het sociaal domein

Eindrapport.

Arnhem, 13 februari 2017

Rekenkamer Arnhem

Mr A.H. Teeuw
Drs. H.J.W. Verdellen
Drs L.M.D. Zwier-Kentie

Zaaknummer: 2016-09-00732

Rekenkamer Arnhem

Inhoudsopgave

Rekenkamer Arnhem

Bestuurlijke Nota

Reken kamer Arnhem

1 Onderzoeksverantwoording

Aanleiding

Met de decentralisaties in het sociaal domein, die vergaande samenwerking en gegevensdeling tussen gemeente en partners met zich meebrengen, is de verantwoordelijkheid van de gemeente op het gebied van privacy en informatiebeveiliging toegenomen. Binnen de gemeente Arnhem krijgt deze samenwerking onder meer gestalte via sociale wijkteams. Deze sociale wijkteams gelden voor inwoners als een centrale toegangspoort voor maatwerkvoorzieningen en ondersteuning binnen de Wet maatschappelijke ontwikkeling (Wmo) en Jeugdwet. De gemeenten hebben zich daarbij te voegen naar een veelvoud aan kaders, van (inter)nationale wetgeving, zoals de Wet bescherming persoonsgegeven en de Wet basisregistratie personen tot de normen uit de Baseline Informatiehuishouding Gemeenten. Bovendien is de regelgeving nog altijd in ontwikkeling; zo is er sinds 1 januari 2016 de meldplicht datalekken en geldt vanaf 2018 de nieuwe Europese privacyrichtlijn en -verordening.

Uit verschillende onderzoeken blijkt dat veel gemeenten moeite hebben met het inkleuren van het lokale beleid omtrent privacy en informatieveiligheid in het sociaal domein. Het inkleuren van het lokale beleid op basis van de hierboven beschreven context is complex. Deskundigen en betrokken instanties, zoals Kwaliteitsinstituut Nederlandse Gemeenten (KING) en het College voor Bescherming Persoonsgegevens (Cbp, nu Autoriteit Persoonsgegevens), maakten zich grote zorgen over de vraag of plannen om privacy van burgers te beschermen op tijd gereed zouden zijn. De vraag rijst dan ook of de gemeenteraden hun controlerende en kaderstellende rol op het gebied van privacybeleid in het sociaal domein voldoende hebben kunnen vervullen en of colleges van B&W in staat blijken de uitvoering aan te laten sluiten op deze ontwikkelingen. Dit is voor de Rekenkamer Arnhem reden geweest om op eigen initiatief een onderzoek uit te voeren naar privacy- en informatieveiligheid in het sociaal domein in de gemeente Arnhem.

Doelstelling en vraagstelling

De rekenkamer beoogt met het onderzoek inzicht te krijgen in de mate van doeltreffendheid en doelmatigheid van de informatieveiligheid en het privacybeleid in het sociaal domein. Het sociaal domein is hierbij gedefinieerd als de taken die de gemeente uitvoert op het gebied van de Wmo, Jeugdwet en Participatiewet (werk en inkomen), waarbij de nadruk ligt op de eerste twee wetten. Die keuze is gemaakt vanwege de ontwikkelingen rondom de sociale wijkteams in Arnhem, die zich met name bezighouden met de Wmo en Jeugdwet. Op een algemeen niveau is privacy en informatieveiligheid op het gebied van de Participatiewet onderzocht.

Met het onderzoek wil de rekenkamer mogelijke richtingen van verbetering identificeren (rekening houdend met de nu al bekende wettelijke veranderingen in de komende 1,5 jaar). Het onderzoek beoordeelt of de gemeentelijke kaders voldoen aan de landelijke wetgeving; in hoeverre de gemeentelijke kaders verwerkt zijn in de organisatie en werkprocessen; of de kaders als werkbaar worden ervaren (zijn er bijvoorbeeld knelpunten en risico's voor inwoners en gemeente, met specifieke aandacht voor de sociale wijkteams); en op welke wijze de raad betrokken is bij informatieveiligheid en privacy.

De centrale vraag in dit onderzoek is als volgt geformuleerd:

Reken kamer Arnhem

In hoeverre zijn de informatieveiligheid en het privacybeleid in het sociaal domein van de gemeente Arnhem doeltreffend en doelmatig?

De centrale vraag is vervolgens uitgewerkt in onderstaande deelvragen, geclusterd naar drie thema's: beleid, Governance, en bewustzijn.'

Beleid

1 Wat zijn kaders, doelen en werkwijzen?
2 Op welke wijze heeft de gemeenteraad kaders gesteld ten aanzien van informatiebeveiliging en privacybeleid in het sociaal domein; en welke rol neemt zij ten aanzien van dit onderwerp in?

Governance en werkprocessen

3 Wat zijn taken en bevoegdheden, hoe is de organisatie (governance) van het privacybeleid en informatieveiligheid vormgegeven?
    a. Tussen gemeenteraad, college en ambtelijke organisatie
    b. Tussen ambtelijke organisatie, de sociale wijkteams en ketenpartners
4 Hoe functioneert deze organisatorische constellatie in de praktijk in het sociaal domein?
5 Voldoet de Arnhemse uitvoeringspraktijk in het sociaal domein aan de relevante wet- en regelgeving?
    a. Waar zitten eventuele knelpunten?
    b. Welke risico's lopen de inwoners van Arnhem?
    c. Welke risico's loopt de gemeente Arnhem?
    d. Welke beheermaatregelen kan het college van B&W het beste nemen om deze mogelijke risico's te mitigeren?
6 Op welke wijze geeft het college van B&W invulling aan de actieve en passieve informatieverstrekking aan de gemeenteraad met betrekking tot informatieveiligheid en privacy in het sociaal domein?

Bewustzijn

7 Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers op het gebied van privacy en informatieveiligheid?

Toekomst

8 Welke verbeterpunten zijn noodzakelijk dan wel nodig?

Onderzoeksuitvoering

Het onderzoek heeft plaatsgevonden in de periode oktober-november 2016. Allereerst is een analyse uitgevoerd op documenten die het beleid, de Governance en werkwijze van de gemeente wat betreft het sociaal domein, privacy en informatieveiligheid beschrijven (zie bijlage 1 voor een overzicht van de geanalyseerde documenten). Vervolgens is met 11 gemeentelijke betrokkenen gesproken, onder wie de portefeuillehouder privacy, de Functionaris Gegevensbescherming, de Chief Information Security Officer en de Chief Information Officer (CISO en CIO) en ambtelijk betrokkenen bij de inrichting en uitvoering van de sociale wijkteams (zie bijlage 2 voor een overzicht van personen die in het kader van dit onderzoek zijn gesproken).

Rekenkamer Arnhem

Daarnaast is 116 gecontracteerde zorgpartners (op basis van contracten uit 2015) en 10 niet-gecontracteerde (zorg)partners gevraagd een enquête in te vullen over hun beeld van de wijze waarop de gemeente Arnhem omgaat met privacy en informatieveiligheid in het sociaal domein. Wat betreft gecontracteerde zorgpartners is een minimale omzet van 5.000 euro aan zorg binnen de gemeente Arnhem aangehouden.[1] Deze enquête is ingevuld door 53 organisaties (een respons van 42%), waaronder de vier grootste zorgaanbieders binnen het Wmo- en Jeugddomein. De 53 organisaties vertegenwoordigen gezamenlijk 65% van de totale omzet van zorgpartners van de gemeente Arnhem. De respons levert daarmee onderzoekstechnisch een voldoende betrouwbaar en representatief beeld op van zorgpartners (een betrouwbaarheidspercentage van 95% bij een foutenmarge van 10%). Daar waar in de antwoorden verschillen tussen de domeinen of functies zichtbaar waren, is dat vermeld in de rapportage. Er waren geen structurele verschillen in de antwoorden tussen grote en kleine organisaties, of tussen de functies van de respondenten (directie, management of uitvoerend).

Met negen organisaties vanuit verschillende domeinen (Wmo, Jeugdwet en Participatiewet) is een verdiepend gesprek gehouden over de uitkomsten van de enquête (zie bijlage 2). Deze groep vertegenwoordigde zowel instellingen die in de sociale wijkteams werkzaam zijn, niet-gespecialiseerde organisaties zonder contract met de gemeente en gespecialiseerde organisaties die op basis van een inkoopcontract werken met de gemeente Arnhem.

Tot slot zijn alle raadsfracties uitgenodigd voor een bijeenkomst om de rol van de raad op dit thema te bespreken. Acht van de elf fracties (D66, SP, PvdA, VVD, GroenLinks, Arnhem Centraal, ChristenUnie en Partij voor de Dieren) hebben hieraan deelgenomen (zie bijlage 2).

Een normenkader is als hulpmiddel gebruikt om essentiële onderdelen van privacy- en informatieveiligheidsbeleid te toetsen (Tabel 1, zie hoofdstuk 4 voor de toetsing van de normen).

Tabel 1. Normenkader

Normenkader
In het privacybeleid van de gemeente ten aanzien van het sociale domein wordt verwezen naar de relevante wettelijke kaders.
De gemeenteraad heeft in zijn beleid voor het sociaal domein bepalingen vastgelegd over de borging van privacy in het algemeen en de bescherming van persoonsgegevens in het bijzonder en hierbij ook de rolverdeling tussen college en raad vastgelegd.
De gemeente heeft met zorgpartners convenanten afgesloten waarin de voorwaarden voor uitwisseling van persoonsgegevens staan.
Binnen de gemeentelijke organisatie is een controlemechanisme aanwezig dat er voor zorgt dat er op de juiste wijze wordt omgegaan met privacygevoelige gegevens.
a. De gemeente heeft met de zorgpartners formele afspraken gemaakt over hoe zij de omgang met privacygevoelige gegevens van inwoners verantwoorden. b. De gemeenteraad is actief geïnformeerd over de wijze waarop de zorgpartners de privacy van de inwoners waarborgen.

[1] In totaal gaat het om 191 gecontracteerde zorgaanbieders in 2015.

In werkprocessen ten aanzien van de verwerking van persoonsgegevens zijn taken en bevoegdheden helder beschreven en duidelijk belegd.
De werkprocessen zijn - in ieder geval wat betreft het privacyaspect- voor ingebruikname getoetst met betrokken medewerkers op werkbaarheid en risico's.
Uit de werkprocessen is op te maken wanneer, door wie en om welke reden privacygevoelige informatie is geraadpleegd.
Er wordt periodiek aandacht besteed aan het bewustzijn van medewerkers in het sociaal domein met betrekking tot privacy en informatieveiligheid.

Op 13 december 2016 is de Nota van Bevindingen voor een controle op de feiten voorgelegd aan de ambtelijke organisatie. De reactie van de ambtelijke organisatie is op 5 januari 2016 ontvangen. Op 17 januari 2017 is de Bestuurlijke Nota aan het college van B&W verstuurd voor een bestuurlijke reactie.

Leeswijzer

Dit rapport bestaat uit twee delen, namelijk het deel Bestuurlijke Nota en het deel Nota van Bevindingen. De Bestuurlijke Nota bestaat uit vier hoofdstukken. In dit hoofdstuk legt de rekenkamer verantwoording af over het uitgevoerde onderzoek. In hoofdstuk 2 presenteert de rekenkamer haar conclusies en aanbevelingen (deelvraag 8). In hoofdstuk 3 staat de bestuurlijke reactie van het college van B&W en hoofdstuk 4 bevat het nawoord.

In de Nota van Bevindingen staan de onderzoeksresultaten, waarop de rekenkamer haar conclusies en aanbevelingen baseert. Hoofdstuk 1 introduceert het thema. Hoofdstuk 2 gaat in op de wettelijke kaders ten aanzien van privacy en informatieveiligheid die van toepassing zijn op gemeenten en de wijze waarop de gemeente Arnhem daarop beleid voert. Ook worden de organisatie van de Governance en belangrijke taken en systemen rondom informatieveiligheid en informatievoorziening aan de raad besproken (deelvragen 1 t/m 3, 6 en 7). Hoofdstuk 3 gaat in op hoe privacy en informatieveiligheid in de praktijk gestalte krijgen, of dit voldoet aan de wettelijke en lokale kaders en welk beeld zorgpartners van de praktijk hebben (deelvragen 4, 5 en ook 7). In hoofdstuk 4 wordt de toetsing van de normen gepresenteerd. Het laatste hoofdstuk 5 geeft antwoord op de hoofdvraag en vat samen welke risico's er voor inwoners en gemeente volgen uit de bevindingen.

Het rapport bevat drie bijlagen. In bijlage 1 en 2 staan de geraadpleegde bronnen en personen. In bijlage 3 is een begrippenlijst van juridische en technische begrippen en afkortingen opgenomen. Om de leesbaarheid van het rapport te vergroten, worden de begrippen niet steeds in de tekst toegelicht.

Rekenkamer Arnhem

2 Conclusies en aanbevelingen

2.1 / Algemene boodschap

De gemeente Arnhem heeft – zeker in relatie tot andere gemeenten – op tijd privacy en informatieveiligheid een goede plek gegeven in kaders, bestuur, beleid en organisatie. Hierdoor is in een vroeg stadium het besef van het belang van privacy en informatieveiligheid ontwikkeld bij wijkteammedewerkers. Op het gebied van informatieveiligheid heeft het college een duidelijk beeld van noodzakelijke acties om tot een goed basisniveau van veiligheid te komen.

Het onderzoek heeft tegelijkertijd enkele risico's voor gemeenten en inwoners naar voren gebracht, die een negatieve invloed kunnen hebben op de doeltreffendheid van het privacy- en informatieveiligheidsbeleid. Zo blijken in de praktijk wijkteammedewerkers afwegingen om gegevens te verzamelen en delen niet eenduidig te maken, waardoor er verschillen in werkwijze optreden. Ook vindt er mailverkeer met persoonsgegevens tussen wijkteams en zorgpartners onbeveiligd plaats. Verder ervaren raadsleden nog onvoldoende grip op het thema. Zij geven aan onvoldoende te weten om te bepalen of de gemeente, maar ook samenwerkende partijen, de privacy en informatieveiligheid op orde hebben. De ambtelijke organisatie is ten slotte bezig om de controle en het verkrijgen van zicht op de omgang en borging van informatieveiligheid en privacy bij samenwerkende partijen te ontwikkelen. Daar hoort ook het maken van heldere afspraken bij. Ten tijde van het onderzoek is het nog onduidelijk hoe de gemeente bijvoorbeeld de afspraken met de stichting Sociale Wijkteams Arnhem vormgeeft.

2.2 / Conclusies

1 Het college en de gemeenteraad van Arnhem hebben op een doelmatige wijze privacy- en informatieveiligheidbeleid in het sociaal domein vormgegeven, door in een vroeg stadium het onderwerp bestuurlijke dekking te geven en een helder algemeen privacykader vast te stellen.

Door vóór de decentralisaties in 2015 privacy als portefeuille te benoemen en als gemeenteraad een privacykader vast te stellen hebben privacy en informatieveiligheid al bij de invoering van nieuwe structuren, zoals de wijkteams, aandacht gekregen. Hierdoor is er sprake van veel bewustzijn voor het thema onder wijkteammedewerkers en is het informatiesysteem van de wijkteams opgebouwd aan de hand van de principes in het privacykader. De visie van het college is dat privacy en informatieveiligheid niet alleen met papier kan worden gewaarborgd, maar in de praktijk veelvuldig als gespreksonderwerp aan bod moet komen. Het is een bewuste keuze van het college om niet alles voor te willen schrijven, maar het eigen denken van professionals in de uitvoering leidend te laten zijn.

2 College en gemeenteraad zien privacy en informatieveiligheid als een politiek thema, maar raadsleden zijn nog op zoek naar de juiste invulling van hun rol om bij te dragen aan controle op doeltreffendheid van het privacy- en informatieveiligheidsbeleid.

Raadsleden willen zich graag uitspreken over het thema, maar hebben nog niet het gevoel dat ze er grip op hebben. De antwoorden op raadsvragen en informatievoorziening in de P&C-cyclus geven volgens hen niet

de informatie waarmee ze kunnen vaststellen dat privacy en informatieveiligheid binnen en buiten de gemeente is gewaarborgd. Zij verwachten bijvoorbeeld uitkomsten van steekproeven of audits binnen de gemeente en bij externe partijen. Het college vraagt zich tegelijkertijd af op welk detailniveau zij inzicht kan geven over de praktijk bij de wijkteams, zonder daarin de privacy van inwoners te schenden. Dit vraagt ook van raadsleden om zich soms anders te positioneren, bijvoorbeeld door op een andere manier vragen te stellen aan het college: los van casuïstiek en meer vanuit algemeen beleid en patronen in de uitvoering.

3 De governance binnen de gemeente is goed georganiseerd, maar het verkrijgen van zicht op de omgang met en de borging van privacy en informatieveiligheid bij derden moet nog vorm krijgen.

Er is door het college veel aandacht besteed aan de Governance rondom privacy en informatieveiligheid. Er is een nauwe samenwerking tussen deze twee thema's met een duidelijke verdeling in verantwoordelijkheden. Er is een juridisch concern controller/Functionaris Gegevensbescherming die steeds meer als interne toezichthouder zal gaan opereren, waarbij een interne auditor dat doet aan de kant van informatieveiligheid. Privacy en informatieveiligheid wordt periodiek besproken in een 'security en privacy'-overleg. Ook binnen de wijkteams is privacy als specifiek thema bij de teamleider belegd en is het vast agendapunt bij de werkoverleggen. Daarnaast worden er verschillende (verplichte) audits gedaan waardoor de gemeente zicht houdt op informatieveiligheid (bijv. DigiD en Suwi).

De wijze waarop de gemeente inzicht heeft in hoe derden omgaan met gegevens binnen het sociaal domein is nog minder ontwikkeld. De afgelopen jaren heeft de gemeente hier nog geen uitvoering aan gegeven. Er is een EDP-auditor aangetrokken om dit vorm te gaan geven. Met de Stichting Sociale Wijkteams Arnhem is ten tijde van het onderzoek nog geen afspraak gemaakt over vormen van externe toezicht (naast het installeren van een Raad van Toezicht), zoals audits, evaluaties of steekproeven. Ook zijn er geen vormen van controle bekend onder gecontracteerde zorgpartners of met Zorg-Lokaal, de organisatie die een deel van de backoffice verzorgt. Formeel heeft de gemeente dan wel geen verantwoordelijkheid voor de manier waarop gecontracteerde zorgpartners met informatiebeveiliging en privacy omgaan, maar materieel blijft de gemeente aanspreekbaar op wat er met de gegevens van haar burgers gebeurd.

4 Het college gaat planmatig en gestructureerd om met benodigde acties op het gebied van informatieveiligheid en privacy in het sociaal domein.

Er is een uitgebreid Actieplan Informatieveiligheid en Privacy met tijdspad, prioritering en benodigde inzet. De intentie is om zo snel mogelijk te voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten. Er wordt met name aandacht besteed aan een goed functionerende Plan-Do-Check-Act--cyclus. Daarnaast zijn er bij incidenten duidelijke protocollen die gevolgd worden, zoals gebeurd is bij het datalek in februari 2016.

5 Binnen sociale wijkteams is er een hoge mate van bewustzijn op het gebied van privacy en informatieveiligheid, maar binnen de ambtelijke organisatie is het bewustzijn nog geen gemeengoed.

Het bewustzijn rondom privacy en informatieveiligheid is vanaf het begin van de sociale wijkteams een aandachtspunt geweest. Sociale wijkteammedewerkers fungeren daarom op dit moment dan ook als een poortwachter op het gebied van privacy en informatieveiligheid. Er zijn meerdere voorbeelden waarbij

medewerkers van het wijkteam op basis van vragen vanuit andere gemeentelijke afdelingen waarschuwden voor mogelijke risico's voor privacy en informatieveiligheid. De aandacht voor privacy en informatieveiligheid die wel georganiseerd is in de Governance, lijkt dus nog niet breed gedeeld in de ambtelijke organisatie. Het is in de opvatting van de Rekenkamer verheugend dat deze aandacht goed geborgd is in de nieuwe werkvorm, maar tegelijkertijd zorgelijk dat de borging binnen de ambtelijke organisatie achterblijft.

6 De werkafspraken van de wijkteams met betrekking tot privacy zijn niet bekend onder alle wijkteammedewerkers en bieden geen afwegingskader voor het verzamelen en delen van gegevens.

Ondanks de hoge mate van bewustzijn op het thema, is er sprake van verschillen in de werkwijze tussen wijkteammedewerkers. Volgens zorgpartners leidt dat tot momenten waarbij wijkteammedewerkers om teveel informatie vragen (bijvoorbeeld wanneer behandelplannen moeten worden verstuurd), maar ook tot situaties waarbij privacy teveel als belemmering wordt opgeworpen om informatie te delen. Het risico daarvan is enerzijds dat de privacy van inwoners geschaad wordt, anderzijds dat er onvoldoende informatie is om tot de juiste zorg of ondersteuning te komen. De werkprocessen lijken te weinig handvatten te bieden om een eenduidigheid te waarborgen. Hoewel de algemene uitgangspunten wel bekend zijn, is er geen sprake van een stappenplan of afwegingsinstrument waardoor elke wijkteammedewerker op dezelfde manier beslist hoe en met wie gegevens te delen. Het gaat daarbij niet om het werken met een 'afvinklijst', want dat zou tot schijnzekerheid leiden. Kernpunt is het bieden van enige houvast bij het maken van afwegingen en vooral ook om die afwegingen later te kunnen reproduceren en gezamenlijk te evalueren. Deze wens wordt ook nadrukkelijk geformuleerd vanuit de wijkteammedewerkers zelf.

Er is nog geen herhaalde aandacht voor het thema informatieveiligheid en privacy binnen het opleidingsprogramma voor de gemeentelijke organisatie, al is er voor 2017 wel een algemene campagne gepland.

Ook samenwerkende (zorg)partners geven aan een eenvoudig protocol te missen waarop zij elkaar en de gemeente op kunnen aanspreken. Organisaties hebben bovendien verschillende visies op het delen van gegevens: voor sommigen is nadrukkelijke toestemming van cliënten altijd noodzakelijk, voor anderen geldt dat in bepaalde gevallen niet, of verschilt de wijze waarop toestemming wordt verkregen (bijvoorbeeld schriftelijk of mondeling).

7 Tussen zorgpartners en wijkteams vindt onbeveiligd mailverkeer plaats.

Met Vecozo is er volgens wijkteammedewerkers en zorgpartners een veilig communicatiesysteem voorhanden. Toch zien zorgpartners dat er regelmatig onbeveiligd mailverkeer met persoonsgegevens plaatsvindt tussen hen en wijkteammedewerkers. Voor de goede orde: het mailverkeer tussen de gemeente en de wijkteams is wel beveiligd.

8 Inwoners zijn onvoldoende op de hoogte van de wijze waarop de gemeente gegevens verzamelt en deelt.

In een inwonersonderzoek van april 2016 gaf 33% van de ondervraagden aan dat de wijkcoach niet had gesproken over privacy en dat 25% niet wist of het onderwerp besproken was. Dit kan een teken zijn dat het achterlaten van de folder niet voldoende informatie geeft over privacy. Uit de interviews blijkt echter ook dat

het voorkomt dat de folders vergeten worden. Ook zorgpartners geven aan dat inwoners lang niet altijd weten wat er met hun gegevens gebeurt. Omdat de gemeente de ambitie heeft om inwoners zo veel mogelijk zicht op en regie over hun eigen gegevens te geven, zal actieve communicatie over privacy en informatieveiligheid richting inwoners juist belangrijker worden.

2.3 / Aanbevelingen

Aan de raad

1 **Bespreek met het college wanneer u welke informatie over privacy en informatieveiligheid (binnen de gemeente en bij samenwerkende partijen) van het college verwacht.**

Om als raad meer grip te krijgen op de kaderstellende en controlerende rol op het gebied van privacy en informatieveiligheid, is het allereerst aan te bevelen om met het college de informatievoorziening te bespreken. De informatievoorziening wordt door raadsleden nu als te algemeen beschouwd en een logische stap zou dus zijn om meer verdiepende informatie te geven. Het college zal hierbij moeten afwegen welke informatie er vanuit privacy-oogpunt gedeeld kan worden. Wat in elk geval mogelijk lijkt is bijvoorbeeld een samenvatting van uitkomsten van audits, steekproeven en evaluaties, of voorbeelden van werkwijzen aan de hand van anonieme casuïstiek. Tegelijkertijd vraagt meer grip op het thema ook van raadsleden om zichzelf te positioneren. Dat betekent bijvoorbeeld nagaan of het college bij nieuw te ontwikkelen beleid of structuurveranderingen - zoals in het geval van de sociale wijkteams - voldoende aandacht heeft besteed aan privacy of informatieveiligheid. Het kan ook betekenen om signalen die raadsleden vanuit inwoners meekrijgen om te vormen in een vraag die expliciet gerefereerd aan de uitgangspunten in het privacybeleid.

2 **Vraag het college om:**
   a. **overzicht van samenwerkende partijen in het sociaal domein;**
   b. **hoe het college deze partijen stuurt op privacy en informatieveiligheid en;**
   c. **hoe het college controleert en/of borgt deze partijen voldoen aan het gemeentelijk privacy- en informatieveiligheidsbeleid.**

Op basis van samenwerkingsovereenkomsten en contracten heeft de gemeente met verschillende partijen afgesproken dat zij voldoen aan wettelijke en lokale kaders rondom privacy en informatieveiligheid. Controle op het naleven van deze afspraken is nog in ontwikkeling. De rekenkamer beveelt de raad aan om het college te vragen om op de hoogte te worden gehouden van deze ontwikkelingen. Nadrukkelijke aandacht hierin vraagt de stichting Sociale Wijkteams Arnhem, als een nieuwe belangrijke samenwerkingspartner binnen het sociaal domein.

Aan het college

3 **Verbreed het bewustzijn op het gebied van privacy en informatieveiligheid zoals dat nu aanwezig is bij wijkteammedewerkers onder de gehele gemeentelijke organisatie.**

De poortwachtersfunctie die wijkteams nu op meerdere momenten hebben vervuld, zal breder in de organisatie moeten worden belegd voor optimale aandacht voor bewustzijn met betrekking tot privacy en informatieveiligheid, bijvoorbeeld via het opleidingsprogramma voor de gemeentelijke organisatie. Onderzoek of de geplande bewustzijnscampagne het gewenste effect heeft.

4 Werk in samenwerking met de stichting Sociale Wijkteams Arnhem de uitgangspunten van het privacy- en informatieveiligheidsbeleid uit in een concreter afwegingskader voor wijkteammedewerkers.

Een dergelijk afwegingskader hoeft niet meer te zijn dan enkele stappen die standaard doorlopen worden of een simpel stroomschema. Het gaat hierbij niet om het zetten van vinkjes, maar om wijkteams te stimuleren bij afwegingen om informatie te verzamelen of te delen telkens dezelfde vragen te stellen. Daarmee wordt enige houvast geboden bij het maken van afwegingen en vooral ook om die afwegingen later te kunnen reproduceren en gezamenlijk te evalueren. Bovendien sluit dit aan bij de nadrukkelijke wens van en roep vanuit de wijkteammedewerkers zelf. Betrek ook (zorg)partners bij de werkbaarheid van het afwegingskader. Bediscussieer ook de rol van het verkrijgen van toestemming van de inwoner bij het opstellen van een afwegingskader, met het oog op de afhankelijkheid van de zorgbehoeftige inwoner van de gemeente.

5 Onderzoek mogelijkheden om emailverkeer beveiligd te laten plaatsvinden.

Het standaard beveiligen van e-mails tussen wijkteammedewerkers en zorgpartners heeft wat betreft informatieveiligheid de voorkeur. Het kan echter ook belemmerend werken, wanneer het negatief van invloed is op het gebruikersgemak. Daarom is het goed om te onderzoeken op welke punten beveiligd emailverkeer noodzakelijk is, en in welke gevallen dat doeltreffende samenwerking kan tegenwerken.

6 Besteed aandacht aan de communicatie over privacy en informatieveiligheid aan inwoners.

Om de communicatie over privacy en informatieveiligheid aan inwoners te verbeteren, kan een mogelijkheid zijn om op de gemeentelijke website een helder overzicht te geven van wat de gemeente doet met de gegevens van inwoners. Een grafische weergave kan hierbij helpen.

3 Reactie college van B&W

Rekenkamer Arnhem
P/a Stadhuis

Zaaknr.:
Documentnr.:
Datum: 7 februari 2017

BESTUURLIJKE REACTIE COLLEGE VAN B. EN W. OP HET RAPPORT 'PRIVACY EN INFORMATIEVEILIGHEID IN HET SOCIAAL DOMEIN' (REKENKAMERRAPPORT VERSIE D.D. 17 JANUARI 2017)

De Rekenkamer Arnhem heeft het college van burgemeester en wethouders uitgenodigd een bestuurlijke reactie te geven op haar rapport 'Privacy en Informatieveiligheid in het sociaal domein' (versie d.d. 17 januari 2017). In zijn vergadering van 7 februari 2017 heeft het college de volgende bestuurlijke reactie vastgesteld.

In hoofdlijnen een positief beeld

Ons college is verheugd dat de Rekenkamer in haar uitgebreide onderzoeksrapport als positieve elementen juist dié zaken benoemt, die vanaf het begin voor ons college centraal hebben gestaan en waar ons beleid en alle inspanningen dan ook op gericht zijn.

Al in een vroeg stadium is het besef van het belang van privacy en informatieveiligheid ontwikkeld bij de medewerkers van de Arnhemse sociale wijkteams, zo constateert de Rekenkamer.[1] Dit doet ons goed. Zonder een hoog privacybewustzijn - de juiste grondhouding - bij degenen die op de werkvloer staan, blijft iedere privacymaatregel namelijk slechts papier en zonder werkelijk effect. Dit is de basisgedachte achter het Arnhemse privacybeleid, en daarom heeft ons college juist op dit punt - privacybewustzijn - sterk ingezet. We menen dit ook terug te zien in het compliment van zorpartners, dat de gemeente Arnhem het vergeleken bij andere gemeenten in de regio 'erg goed' doet.[2]

Privacy begint bij het niét verzamelen van gegevens, zo stellen we in ons Arnhems privacybeleid. Daarom zien we het als een compliment dat de maker van het CVS (Cliëntvolgsysteem wijkteams) heeft aangegeven dat het Arnhemse CVS het meest uitgeklede systeem is (wat betreft hoeveelheid categorieën geregistreerde gegevens) dat hij heeft geleverd.[3] Dit is een goed voorbeeld van 'privacy by design'.

Sinds 1 januari 2016 geldt een plicht tot het melden van datalekken. De Rekenkamer stelt vast dat hiervoor in Arnhem een duidelijke procedure is ingericht en dat deze in de praktijk ook werkelijk wordt gevolgd. Meer in het algemeen stelt de Rekenkamer vast dat de governance van privacy en informatieveiligheid op orde is, waarbij sprake is van een goede samenwerking tussen deze twee gebieden.[4]

[1] Conclusies en Aanbevelingen (Rekenkamerrapport), Algemene Boodschap.
[2] Hoofdstuk 3 van het Rekenkamerrapport, p. 31.
[3] Hoofdstuk 2, p. 18.
[4] Hoofdstuk 2, p. 12 en 18.

We zijn trots op de algemene constatering van de Rekenkamer dat de gemeente Arnhem (zeker vergeleken bij andere gemeenten) op tijd privacy en informatieveiligheid een goede plek heeft gegeven in kaders, bestuur, beleid en organisatie.[5] Daarbij is het goed om te beseffen dat de gemeente in het sociaal domein nogal eens door de Rijksoverheid gedwongen wordt op een zeer vergaande manier inbreuk te maken op de privacy van de burger. SUWINET is hier een zeer bekend voorbeeld van. Bij het inrichten van het gemeentelijke privacybeleid en de uitvoeringspraktijk is deze vergaande landelijke wetgeving een gegeven waar we helaas aan gebonden zijn.

Punten van aandacht

Het feit dat het privacy- en informatiebeveiligingsbeleid op hoofdlijnen in orde is, wil niet zeggen dat er op onderdelen geen verbeteringen nodig zouden zijn.

A. Zo constateert de rekenkamer dat het privacybewustzijn in de ambtelijke organisatie - vergeleken bij de wijkteams - achterblijft. Dit is inderdaad een punt dat aangepakt moet worden, maar wat ons niet verrast. Bij de start van de sociale wijkteams is de aandacht namelijk vooral naar hen uitgegaan. Dáár, op de werkelijke werkvloer van het sociaal domein, moest dit op orde zijn. Gelukkig is dat ook gelukt. Het verhogen van het privacybewustzijn (en informatieveiligheidsbewustzijn) in de ambtelijke organisatie - gemeentebreed - is een zaak van de lange adem, waar gestaag aan wordt gewerkt. Zo staat voor het lopende jaar (2017) een nieuwe bewustwordingscampagne gepland.

B. Verder is van belang dat de rekenkamer heeft vastgesteld dat er geen bewaartermijnen zijn vastgesteld voor de onder de wijkteams berustende dossiers.[6] Dit is een punt dat op korte termijn moet en zal worden opgepakt. Hetzelfde geldt voor het nog plaatsvindende onbeveiligde mailverkeer tussen wijkteams en zorgpartners (voor zover de gemeente daar invloed op kan uitoefenen).[7] De voorzieningen voor beveiligd mailverkeer zijn overigens allemaal aanwezig; in de praktijk worden ze echter onvoldoende gebruikt.

C. De sociale wijkteams zijn per 1 januari 2017 verzelfstandigd (Stichting). Nadere afspraken over privacy en informatieveiligheid - en over de afbakening van ieders verantwoordelijkheid - worden vastgelegd in een bewerkersovereenkomst (Wet bescherming persoonsgegevens) en de aan de stichting te verlenen opdracht. Het is de intentie van het college om over ongeveer een jaar te onderzoeken of de privacy-praktijk zoals die dan bij de stichting wijkteams Arnhem vorm heeft gekregen, voldoet aan wetgeving en eigen beleid (via een 'Privacy Impact Assessment', PIA, of een soortgelijk instrument).

Daarnaast doet de rekenkamer in haar rapport ook een aantal constateringen en aanbevelingen, waar ons college zich niet in kan vinden.

D. Zo leidt de rekenkamer uit gehouden interviews af dat het privacybewustzijn bij de wijkteammedewerkers weliswaar hoog is, maar dat er ook veel verschil zit in de werkwijze van de wijkteammedewerkers. Soms leidt dat tot momenten - aldus geïnterviewde zorgpartners - waarop de wijkteammedewerkers om *teveel* informatie vragen, en op andere momenten om te *weinig.* [8] De rekenkamer ziet dit per definitie als een probleem, waarvoor men een oplossing ziet in de vorm van

[5] Conclusies en aanbevelingen. P. 6.
[6] Hoofdstuk 3, p. 28.
[7] Conclusies en aanbevelingen, p. 8.
[8] Hoofdstuk 4, p. 40.

vaststelling door ons college van een 'stappenplan' of ander afwegingsinstrument dat kan dienen als handvat om een eenduidig werkproces te waarborgen.
Ons college ziet dit anders. Anders dan de rekenkamer - en zorgpartners - kennelijk veronderstellen, hebben de situaties waarin privacy een rol speelt zelden een 'zwart-witkarakter'. Het gaat zelden om vragen die eenvoudig en eenduidig met een ja of nee te beantwoorden zijn. De grijstinten zijn divers en complex. Altijd moet er bij het al dan niet verzamelen of delen van persoonsgegevens een afweging worden gemaakt tussen belangen van zorg, veiligheid, privacy en bijvoorbeeld bedrijfsvoering. Dat de ene wijkteammedewerker dan - na die afweging - soms tot een andere beslissing komt over het delen van gegevens dan een collega van hem, is een normale zaak.
Waar het om gaat, is dat iedere medewerker:
a) een goede basiskennis van de regelgeving heeft,
b) bewust een afweging maakt in elk geval, en
c) zijn gemaakte keuze ook goed kan uitleggen en verantwoorden.
Daarom is het juist privacybewustzijn dat het eerste vereiste is om de naleving van privacynormen en -waarden op een hoger niveau te brengen. Natuurlijk hoort daar ook bij dat de wijkteammedewerkers goed op de hoogte zijn van de privacywetgeving, voor zover van belang voor het sociaal domein.
Anders dan de rekenkamer, is ons college daarom van mening dat een stappenplan geen wezenlijke meerwaarde heeft om privacy meer te waarborgen**.** Het eigen denken van professionals, gefundereerd op kennis van- en een goed begrip van de wetgeving, staat voorop.

Iets anders is het, dat ons college in het rapport terugvindt dat de wijkteammedewerkers ook zelf vragen om meer houvast bij het maken van keuzes die raken aan privacy.
Samen met de Stichting wijkteams Arnhem zullen we bezien waaraan de teams behoefte hebben, hoe ook vanuit de gemeente de wijkteammedewerkers kunnen worden geholpen in het nog verder vergroten van hun deskundigheid en kunde op het vlak van privacy. Zo kan worden gedacht aan (herhaal)cursussen op het gebied van privacyregels. Verder is het van belang om van elkaar te leren; daarvoor is het nodig om met elkaar de gemaakte keuzes te evalueren.

E. De rekenkamer ziet een probleem in het feit dat de wijkteams veel waarde hechten aan het verkrijgen van toestemming van de inwoner voor gegevensdeling.[9] 'Toestemming' is - naast bijvoorbeeld 'wettelijke plicht' en 'publieke taak' - een grondslag voor gegevensdeling (Wet bescherming persoonsgegevens). Vanwege de afhankelijkheidsrelatie in de zorg, moet men voorzichtig zijn met de grondslag 'toestemming' voor gegevensdeling. Het is inderdaad zo dat de wijkteams veel waarde hechten aan de toestemming van de inwoner. Dit is echter niet het geval omdat men die toestemming zoekt als formele grondslag voor gegevensdeling - doorgaans is er al sprake van een 'wettelijke plicht' of een 'publieke taak' als grondslag-, maar een kwestie van fatsoen. Het heeft immers altijd de voorkeur dat de inwoner weet en accordeert dat gegevens gedeeld gaan worden. Wel moeten de wijkteammedewerkers dit verschil tussen toestemming als 'wettelijke grondslag' en als 'fatsoensnorm' goed begrijpen. In de scholing, zo zullen we dat met de Stichting wijkteams Arnhem bespreken, moet hiervoor aandacht zijn.

F. 'Idealiter heeft de gemeente een beeld van de wijze waarop externe partijen omgaan met privacy en infomatieveiligheid', aldus de rekenkamer.[10]
Vanuit de verantwoordelijkheid van ons college voor de uitvoering van de Jeugdwet en de Wet maatschappelijke ondersteuning door zorgpartners kan ons college hiermee instemmen. Wel past de

[9] Hoofdstuk 3, p. 24.
[10] Hoofdstuk 2, p. 12.

kanttekening, dat deze verantwoordelijkheid slechts betrekking kan hebben op de verwerking van persoonsgegevens door zorgpartners in het kader van de uitoefening van bevoegheden die het college hen in mandaat heeft opgedragen (bv. het toekennen van een Wmo-voorziening). Deze verantwoordelijkheid krijgt dan vorm door middel van een zogenaamde bewerkersovereenkomst (Wet bescherming persoonsgegevens). Voor verwerkingen van persoonsgegevens door zorgpartners die buiten deze opdracht van ons college plaatsvinden, draagt ons college geen verantwoordelijkheid. Ons college is géén toezichthouder op zorgpartners in het kader van privacy.[11] Iets anders is het, dat wij - en de wijkteams - een zorgpartner natuurlijk aanspreken op zijn gedrag indien wij constateren dat deze een houding jegens privacy aanneemt die afwijkt van onze visie. Dat is echter geen kwestie van 'controle' of hiërarchie, maar van samenwerking en professionaliteit.

Behoefte van de raad

Raadsleden hebben in een bijeenkomst met de rekenkamer aangegeven dat zij geen grip ervaren op het dossier privacy en informatieveiligheid in het sociaal domein. Er bestaat het gevoel dat men de juiste informatie mist.[12]

Ons college wil zich graag inspannen om de raad van de juiste informatie te voorzien. De raad heeft waarschijnlijk vooral behoefte aan eenduidige en overzichtelijke informatie. In dat kader is het goed om te weten dat de implementatie van het project ENSIA ('Eenduidige Normatiek Single Information Audit') in de tweede helft van 2017 zal starten.[13] ENSIA moet leiden tot meer overzicht - en daarmee de raad beter in staat stellen haar controlerende taak jegens het college uit te kunnen oefenen. Ook moet het mogelijk worden de prestaties van gemeenten op dit vlak onderling te vergelijken. Arnhem vervult een voortrekkersrol in het project ENSIA, en is pilotgemeente.

Zoals we in ons gemeentelijk privacybeleid schrijven, is privacy een thema waar de politiek zich nadrukkelijk over uit moet spreken. Ons college zou het daarom heel mooi vinden, als het nu voorliggende rapport van de rekenkamer voor de raad aanleiding is een open discussie over privacy in het sociaal domein te voeren. Zo'n discussie kan duidelijke politieke uitspraken en wensen op privacygebied opleveren, waar de werkvloer - sociale wijkteams, ambtelijke organisatie, zorgpartners - in de praktijk van alledag rekening mee kan houden. Zo kan de politiek richting geven aan de zorgprofessionals, meer dan een stappenplan dat zou kunnen. Het privacyveld in het sociaal domein is en blijft divers en complex. Het is aan de zorgprofessionals om in elk individueel geval een afgewogen beslissing te nemen. Heldere uitspraken van de politiek kunnen hen daarbij wel helpen.

(Zoals vastgesteld door het college van burgemeester en wethouders op 7 februari 2017)

Reken kamer Arnhem

4 Nawoord rekenkamer

De Rekenkamer dankt het college voor haar bestuurlijke reactie. De Rekenkamer is verheugd dat het college toezegt de aangereikte verbeterpunten, in haar reactie genoemd in de punten A, B en C, ter hand te nemen.

Met betrekking tot de opmerking gemaakt bij punt D (afwegingskader privacybewustzijn) hecht de Rekenkamer eraan om te onderstrepen dat het belang van het eigen denken van professionals in de uitvoering binnen het sociaal domein geenszins tegen wordt gesproken, in tegendeel. Het zijn fundamenten onder een professionele uitvoering. De reden voor de aanbeveling waar het college aan refereert, is gelegen in het bieden van door de wijkteams zelf gevraagde enige mate van houvast bij het maken van afwegingen. Het college maakt een knip in de aanbeveling van de Rekenkamer die door de Rekenkamer zelf niet gemaakt wordt. Het is overigens positief om te lezen dat het college samen met de Stichting wijkteams Arnhem dit punt gaat oppakken. De Rekenkamer geeft daarbij nogmaals de suggestie om daar ook zorgpartners bij te betrekken. Op dit aspect uit de aanbevelingen gaat het college niet nader in.

Bij punt E suggereert het college dat de Rekenkamer het een probleem vindt dat de wijkteams veel waarde hechten aan het verkrijgen van toestemming van de inwoners voor gegevensdeling. Het college legt daarbij de link dat het juist een kwestie van fatsoen is om die toestemming wel te vragen. De Rekenkamer heeft alleen het standpunt van de Autoriteit Persoonsgegevens weergegeven dat, gelet op de afhankelijkheidsrelatie met de gemeente, toestemming alleen in het sociaal domein geen grondslag oplevert voor het delen van gegevens. Het gaat om het afwegen van noodzaak, proportionaliteit en subsidiariteit. Dat bewustzijn lijkt niet aanwezig. Fatsoen moet je doen, op blijvende basis van een professionele grondslag.

Met betrekking tot de behoefte van de raad is het een prima zaak om een open discussie te gaan voeren, zoals door het college voorgesteld. Daarbij gaat het overigens niet alleen om inhoudelijke uitspraken die richting geven aan de uitvoering. Wat daarnaast van belang is – en dat is ook onderstreept in het onderzoek – is dat het college ook de raad in positie brengt en houdt om de gestelde kaders te kunnen controleren en toetsen in de praktijk. Dat zou naar de mening van de Rekenkamer ook een element moeten zijn in de te voeren open discussie.

De Rekenkamer dankt de betrokken medewerkers van de gemeente Arnhem, van de Stichting wijkteams Arnhem en de zorgpartners voor de constructieve medewerking aan het onderzoek.

Rekenkamer Arnhem

Nota van Bevindingen

Rekenkamer Arnhem

1 Introductie

Decentralisaties leiden tot meer aandacht voor privacy en informatieveiligheid

Per 1 januari 2015 hebben gemeenten te maken met decentralisaties van taken op het gebied van zorg, werk en jeugdhulp. Deze zogeheten 'stelselwijzigingen' zijn vastgelegd in drie materiewetten: de Wet Maatschappelijke Ondersteuning (Wmo), de Jeugdwet en de Participatiewet. De taken van de gemeenten in het sociaal domein zijn hierdoor aanzienlijk verbreed: taken uit de Algemene Wet Bijzondere Ziektekosten (Awbz) zijn overgeheveld naar de Wmo, de Jeugdwet bepaalt dat gemeenten een jeugdhulpplicht hebben voor iedereen tot 18 jaar, en de Participatiewet maakt gemeenten verantwoordelijk voor alle mensen met arbeidsvermogen die ondersteuning nodig hebben bij het vinden van werk. Het doel van het Rijk is dat zorg en ondersteuning 'anders en dichter bij de burger' worden georganiseerd, waardoor mensen sneller geholpen worden en oplossingen beter aansluiten op de persoonlijke situatie.[2]

De decentralisaties bleken een enorme opgave voor gemeenten. Pas laat werd op grote lijnen duidelijk wat er werd verwacht van gemeentes in de uitvoering van hun nieuwe taken waardoor er nog veel onzekerheden waren op 1 januari 2015. Omdat het in het sociaal domein juist gaat om een kwetsbare groep inwoners was zorgcontinuïteit van belang, ook terwijl het stelsel veranderde. Veel gemeentes – zo ook gemeente Arnhem – hebben het voortzetten van de zorg voor haar inwoners geprioriteerd om vervolgens de beleidskaders in te vullen. Nog steeds zijn veel gemeentes bezig met het vormgeven van hun beleid en het uitwerken van de processen in de uitvoering.

Als gevolg van de nieuwe taken hebben gemeenten hun organisatie in het sociaal domein moeten aanpassen. Gemeenten dienen te regelen dat inwoners toegang hebben tot ondersteuning, zorg en voorzieningen waar inwoners volgens de materiewetten recht op hebben. Voor gemeenten betekent dat een nauwere samenwerking met partners in het sociaal domein en het opzoeken van samenwerking met nieuwe organisaties en instellingen. Om tegemoet te komen aan de doelstelling van het Rijk hebben daarnaast veel gemeenten, waaronder de gemeente Arnhem, sociale wijkteams ingericht. Deze teams, bestaande uit professionals met verschillende achtergronden, moeten helpen een goed beeld te krijgen van de leefomgeving van inwoners met een ondersteuningsbehoefte (waarbij het 'keukentafelgesprek' bij inwoners thuis een vaak gebruikte methode is). Zo zou de gemeente beter tot passende oplossingen kunnen komen en ook vaker preventieve maatregelen treffen.

Door de verbreding van gemeentelijke taken en verantwoordelijkheden op het sociaal domein, de toegenomen samenwerking tussen gemeente en (zorg)partners en de werkwijze van het ophalen van informatie over de leefsituatie van inwoners door middel van sociale wijkteams, hebben gemeenten in grotere mate te maken met de bescherming van privacy en de bewerking en beveiliging van persoonsgegevens. Dat betekent dat gemeenten steeds meer moeten nadenken over privacy- en informatieveiligheidsbeleid, over de wijze waarop informatie over inwoners wordt verzameld en gedeeld, en welke risico's de opslag van gegevens in ICT-systemen met zich meebrengen.

[2] Minister Plasterk, Decentralisatiebrief (19 februari 2013).

Aandacht versterkt door Europese regelgeving

De gemeentelijke aandacht voor privacy en informatieveiligheid wordt nog eens versterkt door de nieuwe Europese privacy-verordening van 25 mei 2016 (waar organisaties vanaf 25 mei 2018 op mogen worden aangesproken), die de verantwoordelijkheden voor (overheids)organisaties op deze terreinen nog eens aanscherpt. De verordening kan organisaties verplichten om een Privacy Impact Assessment (PIA, of gegevensbeschermingseffectbeoordeling) te doen bij bijvoorbeeld omvangrijke verwerkingen van persoonsgegevens, en schrijft de benoeming van een Functionaris Gegevensbescherming (FG) voor. De FG geldt als een interne toezichthouder op de verwerking van persoonsgegevens.

De privacy-verordening kent ook een meldplicht datalekken, die in Nederland al per 1 januari 2016 was geregeld door de toevoeging van een artikel (34a) aan de Wet bescherming persoonsgegevens (Wbp). Een datalek kan bijvoorbeeld een hack zijn van de gemeentelijke website, het versturen van persoonsgegevens naar de verkeerde ontvangers, maar ook het verliezen van een laptop met persoonsgegevens. Sinds de meldplicht zijn er al verschillende gemeenten die een datalek hebben moeten melden.

Volgens Autoriteit Persoonsgegevens hebben gemeenten nog onvoldoende aandacht voor privacy

De Autoriteit Persoonsgegevens (AP, de Nederlandse toezichthouder, voorheen College bescherming persoonsgegevens) heeft op verschillende momenten aandacht gevraagd voor de privacy risico's die als gevolg van de decentralisaties zijn ontstaan. De AP wijst er in het rapport 'De rol van toestemming' op dat er geen overkoepelende wettelijke regeling is voor de domeinoverstijgende verwerking van persoonsgegevens in het sociaal domein.[3] Op basis van onderzoek (waar ook de gemeente Arnhem aan deelnam) ziet de AP dat veel gemeenten daarom toestemming vragen aan betrokkenen voor het verwerken van gegevens. Volgens de AP wordt het probleem daarmee echter niet omzeild. Toestemming moet volgens de Wbp in 'vrijheid' gegeven kunnen worden, terwijl in het sociaal domein inwoners vaak afhankelijk zijn van de gemeente voor hulp. De AP concludeert dat gemeenten een beter overzicht moeten hebben van de doelen, grondslagen en persoonsgegevens in het sociaal domein, om te weten wanneer persoonsgegevens verwerkt mogen worden én om inwoners beter te kunnen informeren.

Privacy en informatieveiligheid in gemeente Arnhem

Ook in de gemeente Arnhem is de toegenomen aandacht voor privacy en informatieveiligheid waar te nemen. Dat blijkt bijvoorbeeld uit schriftelijke vragen vanuit de fracties van D66 en SP op 24 juni 2015 over de bescherming van privacy en Suwinet[4] en vragen vanuit de partij Verenigd Arnhem op 8 december 2015 over jeugdbescherming, toezicht en privacy. Ook heeft de gemeenteraad in juli 2015 een privacykader vastgesteld[5] en heeft het college op 23 december 2014 de 'Notitie privacy in het sociaal domein' vastgesteld.[6] In de volgende hoofdstukken wordt besproken hoe de gemeente Arnhem omgaat met privacy en informatieveiligheid in het sociaal domein. Het sociaal domein is hierin gedefinieerd als de gemeentelijke taken binnen de Wmo, Jeugdwet en Participatiewet. De nadruk zal echter op de eerste twee domeinen

[3] Autoriteit Persoonsgegevens (april, 2016). Verwerking van persoonsgegevens in het sociaal domein: de rol van toestemming.

[4] Het systeem waarin persoonsgegevens worden verwerkt en gedeeld in het kader van uitvoering van o.a. de Participatiewet.

[5] http://www.gelderlander.nl/regio/arnhem-e-o/arnhem/privacy-arnhemse-burger-beter-beschermen-1.5045199.

[6] Notitie privacy in het sociaal domein, december 2014.

liggen, vanwege enerzijds de belangrijke ontwikkeling van sociale wijkteams die sinds 2015 in de gemeente actief zijn[7] en anderzijds de toegenomen samenwerking met zorgpartners op deze domeinen.

[7] Koersnota Van Wijken Weten (2016).

Reken kamer Arnhem

2 Beleid, Governance en informatievoorziening

Dit hoofdstuk gaat in op de wettelijke kaders ten aanzien van privacy en informatieveiligheid die van toepassing zijn op gemeenten. Vervolgens komen de volgende aspecten aan bod: de wijze waarop de gemeente Arnhem daarop beleid voert, de Governance heeft georganiseerd, welke taken en systemen van belang zijn met betrekking tot informatieveiligheid en hoe de raad van informatie wordt voorzien (deelvragen 1 t/m 3, 6 en 7).

2.1 / Wettelijke kaders

Gemeenten hebben te maken met verschillende wettelijke kaders voor de omgang met persoonsgegevens in het algemeen en voor het sociaal domein specifiek. Deze worden hieronder kort beschreven.

Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) is het algemene en belangrijkste kader voor verwerking van persoonsgegevens. De Wbp noemt de voorwaarden waaraan gegevensverwerking moet voldoen. Zo schrijft de Wbp voor dat persoonsgegevens slechts 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.*"[8] Deze eis betekent dat gegevensverwerking moet voldoen aan de eisen van *proportionaliteit* en *subsidiariteit*. Proportionaliteit en subsidiariteit houden in, dat het middel in verhouding moet staan tot het doel en dat gekozen moet worden voor het middel met de minst ingrijpende gevolgen. Verder schrijft de Wbp voor dat persoonsgegevens worden verzameld voor *welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden*.[9]

Persoonsgegevens mogen slechts worden verwerkt als daar een wettelijke grondslag voor is. De Wbp somt limitatief de gronden op voor gegevensverwerking. Voor de gemeente, die voor haar publiekrechtelijke taakuitoefening persoonsgegevens moet verwerken, zijn met name de gronden uit artikel 8 sub a, c en e relevant:

- de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend (a);
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke is onderworpen (c), of
- de gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt (e).

Zoals in de inleiding is aangegeven, heeft de Autoriteit Persoonsgegevens in haar onderzoek van april 2016 geconstateerd dat gemeenten geen duidelijk beeld hebben van welke gegevens zij in het sociaal domein mogen verwerken, voor welke doelen zij dit mogen en op basis van welke grondslagen.[10] Bovendien is de crux bij de toestemming, sub a van art. 8 Wpb, dat deze geen grondslag vormt voor gegevensverwerking

[8] Wet bescherming persoonsgegevens, art. 11

[9] Wet bescherming persoonsgegevens, art. 7

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

wanneer deze niet ‘in vrijheid’ is gegeven. In situaties waarin de betrokkene afhankelijk is van de gemeente voor hulp, zoals de intake/toegangsverlening, wordt toestemming niet ‘in vrijheid’ gegeven. Daarom levert toestemming in het sociaal domein vaak geen grondslag op voor gegevensverwerking. De gemeente mag in dat geval alléén persoonsgegevens verwerken als zij zich kan baseren op een van de andere grondslagen uit artikel 8 van de Wbp, de grondslagen sub c/e.

Vanaf artikel 16 geeft de Wbp voorschriften voor verwerking van specifieke persoonsgegevens, zoals gegevens betreffende gezondheid. Verwerking van dergelijke gevoelige persoonsgegevens is in beginsel verboden.[11] Artikel 21 benoemt de uitzonderingen op dit verbod. Zo mogen persoonsgegevens betreffende iemands gezondheid worden verwerkt door bestuursorganen voor zover dat noodzakelijk is voor “een goede uitvoering van wettelijke voorschriften, pensioenregelingen of collectieve arbeidsovereenkomsten die voorzien in aanspraken die afhankelijk zijn van de gezondheidstoestand van de betrokkene.”[12] Verder legt de Wbp geheimhouding op aan alle personen die verwerkte persoonsgegevens onder ogen krijgen.[13]

De meldplicht datalekken, die per 1 januari 2016 aan de Wbp is toegevoegd, houdt in dat organisaties (bedrijven en overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra er sprake is van een ernstig datalek. Van een datalek is sprake als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wbp). Hierbij valt te denken aan de toegang tot, of vernietiging, wijziging of het vrijkomen van persoonsgegevens bij een organisatie zonder dat dat de bedoeling is van de organisatie.[14]

Kaders voor privacy in materiewetten: Jeugdwet, Wmo en Participatiewet

Naast de Wpb vinden we kaders voor privacy in de materiële wetten in het sociaal domein, zoals de Jeugdwet, de Wmo en de Participatiewet. Deze wetten voorzien in de noodzakelijke wettelijk grondslag voor het verwerken van persoonsgegeven. Zo legitimeert de Jeugdwet verwerking van persoonsgegeven voor zover deze noodzakelijk zijn voor, onder meer “het doelmatig en doeltreffend functioneren van de toegang tot de jeugdhulp, de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering”.[15]

De Wmo legitimeert onder meer het verwerken van persoonsgegevens (betreffende de gezondheid) die noodzakelijk zijn voor de beoordeling van de behoefte aan ondersteuning van participatie of zelfredzaamheid. Aan alle partijen die bij de uitvoering van de Wmo betrokken kunnen zijn, zoals het college maar ook de aanbieder van een Wmo-voorziening, zijn in de Wmo geheimhoudingsplichten ten aanzien van persoonsgegevens opgelegd.[16] Daarnaast zijn bepalingen opgenomen die regelen hoe lang persoonsgegevens mogen dan wel moeten worden bewaard[17] en die verplichten tot transparantie richting de personen waarvan de gegevens bewaard worden.[18]

[11] Wet bescherming persoonsgegevens, art. 16
[12] Wet bescherming persoonsgegevens, art. 21, lid 1 sub f
[13] Wet bescherming persoonsgegevens, art. 12
[14] https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken
[15] Jeugdwet, art. 7.4.4, lid 1
[16] Wet maatschappelijke ondersteuning 2015, art. 5.3.3
[17] Wet maatschappelijke ondersteuning 2015, art. 5.3.4 en 5.3.5
[18] Wet maatschappelijke ondersteuning 2015, art. 5.3.2

De Participatiewet harmoniseert de Wet Werk en Bijstand, Wet Sociale Werkvoorziening en Wajong. Gegevensverwerking is in deze wetten geregeld conform het gesloten verstrekkingenregime Wet structuur uitvoeringsorganisatie werk en inkomen (Suwi). Dat regime houdt in dat in de sector Werk en Inkomen gegevens uitsluitend hergebruikt mogen worden als daar een wettelijke grondslag voor is:

- De wet Suwi biedt in artikel 9 de grondslag voor de samenwerking tussen de ketenpartners en gemeenten;
- In artikel 62 van de wet Suwi wordt de grondslag voor de gegevensverwerking via elektronische voorzieningen gelegd. Deze wordt verder uitgewerkt in het Besluit Suwi art 5.24 en de Regeling Suwi hoofdstuk 6;
- De geheimhoudingsplicht is in artikel 74 van de wet Suwi vastgelegd.

De Autoriteit Persoonsgegeven constateert dat bepaling van de grondslagen voor de verwerking van persoonsgegevens bij de uitvoering van taken in het sociaal domein complex is. De verschillende wetten op grond waarvan gemeenten in het sociaal domein taken uitvoeren bevatten elk bepalingen over de verwerking van persoonsgegevens in dat specifieke domein. Deze wetten voorzien onvoldoende in een regeling voor integrale taakuitvoering en er ontbreekt een overkoepelende wettelijke regeling.[19]

Informatieveiligheid: BIG en zeven informatiebeveiligingsnormen

De Wbp geeft ook kaders voor informatieveiligheid: De gemeente legt "*passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*"[20]

In november 2013 is door alle gemeenten de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' bekrachtigd.[21] De resolutie schrijft onder andere voor dat gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG) onderschrijven als hét gemeentelijke basisnormenkader voor informatieveiligheid.[22] Gemeenten dienen een beleidsplan informatieveiligheid vast te stellen aan de hand van de Baseline Informatiebeveiliging Gemeenten. In het BIG-normenkader gelden een aantal normen specifiek voor het gebruik van Suwinet - het systeem waarmee gemeenten en uitvoeringsorganisaties (zoals het Uitvoeringsinstituut Werknemersverzekeringen) persoonlijke gegevens van burgers in het kader van de Wet Suwi (Structuur Uitvoeringsorganisatie werk en inkomen) uitwisselen. Het gaat om zeven normen die ook zijn opgenomen in het Normenkader Gezamenlijke elektronische Voorzieningen Suwi (GeVS), dat gebruikt wordt door de Inspectie Sociale Zaken en Werkgelegenheid om toezicht te houden op de toepassing van deze normen.[23] Het gaat om de volgende normen:

---

[19] Autoriteit Persoonsgegevens, "Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming", april 2016, p. 2.

[20] Wet bescherming persoonsgegevens, art. 13

[21] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente

[22] https://vng.nl/files/vng/brieven/2013/attachments/20131031_resolutie-informatieveiligheid.pdf, p. 2

[23] Verantwoordingsrichtlijn en Normenkader GeVS (23 juni 2011).
http://www.bkwi.nl/uploads/media/Verantwoordingsrichtlijn_GeVS_2011.pdf

- ‘De gemeente heeft een formeel vastgesteld beveiligingsbeleid en -plan. Het Beveiligingsplan is het actieprogramma dat het beveiligingsbeleid moet omzetten in daden, door de inzet van mensen en middelen.’ (norm 1.3 in GeVS en paragraaf 5.1.1 van de BIG)
- ‘De gemeente draagt op reguliere basis het beveiligingsbeleid en -plan uit.’ (norm 1.4 in GeVS en paragraaf 5.1.1 van de BIG)
- ‘De gemeente evalueert op reguliere basis beveiligingsbeleid en –plan.’ (norm 1.5 in GeVS en paragraaf 5.1.2 van de BIG)
- ‘De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinetgegevens, -applicaties, -processen en -infrastructuur moeten zijn beschreven en duidelijk en afhankelijk van de schaalomvang van de organisatie gescheiden zijn belegd.’ (norm 2.2 in GeVS en paragraaf 10.1.3 van de BIG)
- ‘De Security Officer beheert en beheerst beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.’ (norm 2.3 in GeVS en paragraaf 6.1.2 van de BIG)
- ‘De organisatie autoriseert en registreert de toegang die gebruikers hebben tot de Suwinet applicaties op basis van een formele procedure.’ (norm 13.1 in GeVS en paragraaf 11.5.1 van de BIG)
- ‘De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.’ (norm 13.5 in GeVS en paragraaf 10.10.2 van de BIG)

2.2 / Arnhemse visie op privacy

In deze paragraaf worden de belangrijkste uitgangspunten van de gemeente Arnhem op het gebied van privacy beschreven.

Aandacht voor privacy door toewijzing portefeuille

In 2014 is op initiatief van het college een portefeuille privacy toegevoegd aan het takenpakket van de wethouder Jeugdzorg. Met het benoemen van een portefeuillehouder privacy werd beoogd privacy als beleidsinhoudelijk onderwerp meer tot zijn recht te laten komen en uit de schaduw te halen van informatieveiligheid/ICT, waar privacy tot dan toe onder resideerde. Deze aandacht voor privacy dateert dus van voor de decentralisaties en is breder dan alleen het sociaal domein. Het college merkt dat sinds de introductie van de privacy portefeuille privacy ook vaker aan de orde komt in beleidsprocessen en dat privacy-issues vaker expliciet aan het college worden voorgelegd.

Binnen het college ligt de verantwoordelijkheid voor privacy primair bij de portefeuillehouder privacy, maar als er onderwerpen zijn die zowel domeinspecifiek beleid als privacy raken, dan wordt dat gezamenlijk besproken. Met name rondom de organisatie van de sociale wijkteams vindt er gezamenlijk overleg plaats tussen de portefeuillehouder Wmo en portefeuillehouder privacy (die ook Jeugdwet in de portefeuille heeft). Tegelijkertijd worden veel keuzes ook op ambtelijk niveau gemaakt en zijn veel zaken gemandateerd aan de ambtelijke organisatie. Dit past bij de visie van het college dat een goede waarborging van privacy en informatieveiligheid voor een groot deel afhankelijk is van de acties van uitvoerende ambtenaren.

Het privacybeleid is voor het *sociale domein* organisatorisch uitgewerkt in de Notitie privacy sociaal domein (2014). Het college heeft werk gemaakt van een algemeen beleidskader voor privacy en dit laten vaststellen door de gemeenteraad op 29 juni 2015 (het ‘Kader voor het gemeentebrede privacybeleid’). Verder is het privacybeleid verankerd in de organisatie door middel van werkprocessen c.q. werkafspraken. De visie van het college is evenwel dat ‘papieren’ afspraken niet voldoende basis zijn voor een goede organisatie van

privacy en informatieveiligheid, maar dat het juist gaat om bewustzijn, aandacht en continu gesprek over het thema.

Algemeen privacybeleid kent zeven basisprincipes

Met het kader voor het gemeentebrede privacybeleid beoogt de gemeenteraad een basis te bieden voor een goede 'grondhouding' ten opzichte van privacy.[24] Die goede grondhouding houdt in dat iedere bestuurder en medewerker zich bewust is van situaties waarin privacy een rol speelt. Bewustzijn moet er voor zorgen dat men aan de voorkant - voordat een beslissing wordt genomen - de relevante vragen stelt. Daarmee moeten niet-gerechtvaardigde inbreuken op de privacy van de inwoner zoveel mogelijk worden voorkomen. Het zorgt er volgens het college voor dat er ook minder gegevens verzameld worden, en er dus minder gegevens beveiligd hoeven te worden. Het beleidskader moet daarnaast leiden tot 'accountability' op privacygebied: dat de gemeente kan uitleggen wat ze doet om aan de privacywetgeving te voldoen, en waarom ze in een bepaalde situatie op een bepaalde manier handelt.

Het beleidskader biedt geen concrete antwoorden, maar een afwegingskader. Het is volgens de gemeente aan de professionals in het veld, zoals coaches in de sociale wijkteams, om de afweging te maken of gegevens gedeeld mogen worden of niet. Het beleidskader reikt beginselen aan die de professionals bij de afweging in acht nemen. De kern is dat gegevens alleen verwerkt worden wanneer dat noodzakelijk is, dat nooit meer verwerkt wordt dan nodig is, en dat er geen gegevens worden gedeeld zonder toestemming van de inwoner, tenzij de veiligheid in het gedrang komt.

Het kader benoemt zeven basisprincipes die leidend zijn bij de door de professional te maken afweging:

1. *Data-minimalisatie: nee, tenzij*
   Alleen voor zover er een noodzaak toe bestaat, vindt verwerking (verzameling, deling) van persoonsgegevens plaats. Persoonsgegevens worden slechts verwerkt met toestemming van de betrokkenen, en worden niet langer bewaard dan strikt noodzakelijk.
2. *Doelbinding*
   Persoonsgegevens worden slechts verzameld voor een van te voren bepaald, concreet omschreven doel. Nooit wordt meer verzameld dan strikt nodig is voor dát doel (proportionaliteit), en er wordt niet verzameld als er een manier voorhanden is om informatie te krijgen die minder inbreuk maakt op de privacy (subsidiariteit).
3. *Correctheid*
   Alle redelijke maatregelen moeten worden genomen om onjuiste persoonsgegevens onverwijld te wissen en te rectificeren (artikel 11, lid 2, Wbp).
4. *Privacy by design*
   Direct bij de inrichting van een werkproces moet nagedacht worden welke vragen en problemen vanuit privacy-oogpunt een rol (kunnen) spelen, zodat privacy-problemen worden voorkomen.
5. *Transparantie*
   De gemeente is open over het feit dat ze persoonsgegevens verwerkt en voor welke doeleinden, informeert inwoners over hun rechten, zoals klachtrecht en inzagerecht, en is open over haar standpunt vanuit privacy-oogpunt over bepaalde (technologische) ontwikkelingen, en over de afweging van belangen.
6. *Privacy als politiek onderwerp*

[24] Kader voor privacy gemeente Arnhem, juli 2015
http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/historie/Arnhem/372032/372032_1.html

Privacy is een onderwerp waarover de politiek gezaghebbende uitspraken moet doen. Als zich (in Arnhem) een ontwikkeling voordoet met impact op de privacy, die maatschappelijk gevoelig ligt en waarbij de wettelijke kaders niet duidelijk zijn, dan zal het college (de plannen voor) een dergelijke ontwikkeling aan de raad voorleggen om de raad zich hierover uit te laten spreken.

7 *Geen profilering*
Alleen op grond van een menselijk signaal komt een inwoner met zijn gegevens bij de gemeente Arnhem in beeld, niet op basis van selectie door een computer.

Alle gemeentelijke maatregelen die impact hebben op de privacy moeten aan dit privacykader worden getoetst. Ook verplicht het beleidskader het college om de raad vooraf te raadplegen wanneer het college "een bepaalde vorm van gegevensverwerking wenst uit te voeren of te ondersteunen waarvan niet op voorhand duidelijk is waar de wettelijk grens ligt en die maatschappelijk gevoelig ligt."

Notitie Privacy sociaal domein biedt uitgangspunten, maar geen concrete handvatten

Het algemene privacy beleidskader kent een organisatorische uitwerking voor het sociaal domein in de vorm van de Notitie Privacy sociaal domein (hierna kortweg 'de Notitie'). De Notitie geeft aandacht aan de onderwerpen beleid, governance, werkprocessen en triage, opslag en beheer van gegevens en bewustwording en communicatie. Centraal staat dat de wens om integraal te werken, ertoe leidt dat gemeenten 'ontschot' moeten werken. De gemeente moet persoonsgegevens uit verschillende sectoren samenbrengen als de situatie daarom vraagt. Dat mag er echter niet toe leiden dat er nodeloos of overmatig gegevens worden verwerkt.[25]

De Notitie geeft uitgangspunten voor het verzamelen van persoonsgegevens, zoals "Alleen die persoonsgegevens worden verzameld, die noodzakelijk zijn voor een bepaald, concreet omschreven doel (subsidiariteit), en vervolgens niet meer dan strikt nodig voor dát doel (proportionaliteit)", en "Persoonsgegevens worden in principe alleen verzameld met toestemming van de betrokkene".[26] Verder geeft de Notitie aan dat verzamelde persoonsgegevens zo min mogelijk worden gedeeld en gekopieerd, en dat persoonsgegevens niet langer worden bewaard dan strikt noodzakelijk.

Hiervóór is genoemd dat de Autoriteit Persoonsgegevens erop heeft gewezen dat toestemming in het sociaal domein, vanwege de afhankelijkheid van de inwoner jegens de gemeente/hulpverlener, zelden vrij is en dus zelden een grondslag vormt voor gegevensdeling. De Notitie geeft desondanks veel gewicht aan toestemming en spreekt niet over andere grondslagen voor gegevensverwerking. Uit interviews met wijkteammedewerkers en zorgpartners blijkt ook dat er twijfel is, of toestemming wel als basale grondslag kan worden gebruikt of zelfs enige grondslag vormt voor gegevensdeling in het sociaal domein.

Net als het gemeentebrede beleidskader schrijft de Notitie beginselen voor die de professionals in het veld moeten toepassen om hun beslissingen te nemen. Het is aan de professionals, zoals de leden van de sociale wijkteams, om de beslissing te nemen of gegevens gedeeld mogen worden of niet. Daartoe biedt de Notitie echter geen concrete handvatten, zoals een stappenplan of een stroomschema. De beginselen uit het beleidskader en Notitie bieden volgens de ambtelijke organisatie echter in de praktijk wel een

[25] Zie ook de Brief van 27 mei 2014, behorende bij de aanbieding van de door het Ministerie van BZK opgestelde Beleidsvisie 'Zorgvuldig en Bewust: gegevensverwerking en privacy in een gedecentraliseerd sociaal domein'.

[26] Tenzij een wettelijk uitzonderingsgeval zich voordoet, uit art. 8 Wbp. Belangrijke uitzonderingen zijn die van een 'vitaal belang' van de betrokkene, en de uitvoering van een wettelijke plicht waaraan het college onderworpen is.

afwegingskader of een richtlijn om in elk concreet geval een juiste afweging te maken. Het is overigens een bewuste keuze van het college om niet alles voor te willen schrijven, maar het eigen denken van professionals in de uitvoering leidend te laten zijn.

2.3 / Arnhemse visie op informatieveiligheid

In deze paragraaf worden de belangrijkste uitgangspunten van de gemeente Arnhem op het gebied van informatieveiligheid beschreven.

Informatiebeveiligingsbeleid beschrijft definities en uitgangspunten rondom informatieveiligheid

De gemeente Arnhem beschrijft haar belangrijkste afwegingen rondom informatieveiligheid in het (door het college vastgestelde) Beleid voor Informatiebeveiliging 2015-2018. In vergelijking met de Notitie Privacy Sociaal Domein geeft dit beleid een wat concreter beeld van werkprocessen en beoogde strategie voor de komende jaren. In het beleid zijn de definities opgenomen van informatiebeveiliging ('het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen') en informatiesysteem ('een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur, alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie').[27]

Aan de hand van zes uitgangspunten wordt invulling gegeven aan informatiebeveiliging:

- Er zijn dreigingen. Hogere muren helpen niet, veerkrachtig optreden wanneer er iets misgaat is van belang.
- Verantwoord en bewust gedrag van gebruikers.
- Van beveiligen naar veilig faciliteren aan de hand van maatregelen om de impact van ongewenste activiteiten te voorkomen.
- Risicoafweging als basis voor de te nemen maatregelen.
- Conformeren aan (landelijke) standaarden.
- Controleerbaarheid.

In deze uitgangspunten is aandacht voor de kaders, governancestructuur, werkprocessen en het bewustzijn, belangrijke aspecten voor een goede implementatie van privacybeleid (zie het Implementatieplan 'Privacy sociaal domein' van de Vereniging Nederlandse Gemeenten[28]). Informatiebeveiliging moet volgens het plan integraal worden opgepakt, waarbij gestreefd wordt naar samenwerking met meerdere afdelingen (P&O, Facilitair, Financial Control, Communicatie, Juridische zaken en Business Control).[29] Uit de interviews blijkt dat deze integraliteit in de praktijk wordt gewaarborgd door de samenstelling van het securityteam (zie volgende paragraaf). In dit team zijn medewerkers van beleid, uitvoering en toezicht vertegenwoordigd.

[27] Beleid voor informatiebeveiliging 2015-2018, p.4

[28] VNG Implementatieplan privacy sociaal domein, 2015, p.2

[29] Beleid voor informatiebeveiliging 2015-2018, p.5

Het beleid voor informatiebeveiliging beschrijft de strategie voor informatiebeveiliging in de jaren 2015-2018. Het beleid richt zich vooral op het voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van de Informatiebeveiligingsdienst (IBD).

Informatiebeveiligingsbeleid geldt voor de gemeente en voor derden

Het informatiebeveiligingsbeleid is van toepassing op de gemeente Arnhem en alle derden die informatie verwerken voor de gemeente Arnhem (dus ook sociale wijkteams en dienstenleveranciers).[30] Dit wordt benoemd in de contracten die de gemeente sluit met externen; zij worden geacht zelf zorg te dragen voor een adequaat beveiligingsbeleid dat aansluit bij de standaard van de gemeente. Ook worden met partijen die persoonsgegevens bewerken in opdracht van de gemeente bewerkersovereenkomsten afgesloten. Idealiter heeft de gemeente een beeld van de wijze waarop externe partijen omgaan met privacy en informatieveiligheid. De afgelopen jaren heeft de gemeente hier nog geen uitvoering aan gegeven. Voor de nieuw op te richten stichting van de sociale wijkteams zijn hier ook nog geen afspraken over gemaakt (zie hoofdstuk 3). Recentelijk is wel een Electronic Data Processing (EDP)-auditor aangesteld die dit vorm moet gaan geven.

2.4 / Inrichting van Governance

Functionele governance met goede samenwerking tussen privacy en informatieveiligheid

Governance verbindt privacy en informatieveiligheid
Om duidelijkheid te hebben over de verschillende verantwoordlijkheden op het gebied van privacy en informatieveiligheid, is in 2014 een systeem van governance voor privacy en informatieveiligheid uitgedacht in de Notitie privacy sociaal domein.[31] Dit systeem is in de praktijk op sommige punten anders ingevuld om de governance beter te laten functioneren.[32] De belangrijkste rollen in de praktijk zijn de volgende:

- Het college is verantwoordelijk voor de waarborging van de privacy.
- De leidinggevenden binnen de sociale wijkteams, het klantcontactcentrum en de backoffice zijn verantwoordelijk voor de uitvoering en het naleven van de privacyregels in de dagelijkse praktijk. Zij leggen hierover verantwoording af aan hun eenheidsmanager, respectievelijk clustermanager. Binnen de sociale wijkteams is er één wijkteamleider die privacy als 'portefeuille' heeft.
- De FG is belast met het houden van intern toezicht op de naleving van de Wbp in de gemeentelijke organisatie, inclusief de sociale wijkteams. De FG rapporteert aan het college en staat het college en de organisatie bij door het gevraagd en ongevraagd geven van advies op privacy-gebied. Wanneer een gemeente ervoor kiest een Functionaris voor de Gegevensbescherming (FG) aan te stellen, hoeft gegevensverwerking niet meer rechtstreeks aan de Autoriteit Persoonsgegevens (AP) gemeld te worden maar kan dat bij de FG gebeuren.[33] In de gemeente Arnhem is de juridisch concerncontroller aangesteld als FG.
- De Chief Information Officer (CIO) is verantwoordelijk voor het informatiebeveiligingsbeleid. FG en CIO informeren en consulteren elkaar over alle aspecten die van belang zijn in verband met de privacy.

[30] Beleid voor informatiebeveiliging 2015-2018, p.4

[31] Notitie privacy in het sociaal domein, december 2014.

[32] Het betreft marginale verschillen, zo heeft de clustermanager intern advies uiteindelijk geen inhoudelijke rol gekregen in het governancemodel.

[33] Dat geldt overigens niet voor datalekken, die wel direct aan de AP gemeld moeten worden.

- De Chief Information Security Officer (CISO) is verantwoordelijk voor de organisatie van de informatiebeveiliging.
- Er is een ‘security en privacy’-overleg opgezet dat maandelijks bijeen komt. In dit overleg zijn de FG, Juridisch Advies, de CIO, de CISO, de Auditor Informatieveiligheid/privacy en Gegevensmanagement vertegenwoordigd.

In de interviews komt naar voren dat de Governance zorgt voor een nauwe verbinding tussen privacy en informatieveiligheid. Het ‘security en privacy’-overleg is opgezet vanuit de gedachte dat informatieveiligheid en privacy gezamenlijk behandeld moeten worden. Zoals gezegd, de opvatting van het college is dat hoe meer privacy-bewustzijn er voorafgaand aan gegevensverzameling en –deling is, hoe minder gegevens er beveiligd hoeven te worden. Een voorbeeld van een onderwerp dat in het overleg is besproken is het inrichten van de procedure rondom datalekken.

De juridisch concerncontroller vervult tevens de rol van Functionaris Gegevensbescherming (FG). De FG heeft als taak om binnen de gemeente, inclusief de sociale wijkteams, toezicht te houden op de naleving van de Wbp. Omdat de juridisch concern controller nauw betrokken is geweest bij het opzetten van de Governance en het privacybeleid geldt hij op dit moment naast toezichthouder ook als algemeen aanspreekpunt. De intentie is om de toezichthoudende rol in de komende tijd te versterken. Uit de interviews volgt dat de professionalisering van de functie van FG merkbaar is. Privacy krijgt de laatste jaren meer aandacht, waardoor de rol van de FG groter wordt. Er is meer beleid waarop moeten worden toegezien en er wordt vaker overlegd (bijvoorbeeld met de CIO).

Governance informatieveiligheid steeds formeler en structureler

Het informatiebeveiligingsbeleid beschrijft specifieker dan de notitie Privacy sociaal domein wat de verantwoordelijkheden rondom informatieveiligheid zijn en waar deze zijn belegd. Zo staat er dat informatiebeveiligingsbeleid een verantwoordelijkheid is van het college en is opgenomen in de planning en control cyclus. Via deze cyclus verantwoordt het college zich over het gevoerde beleid. De directie is gedelegeerd opdrachtgever van de CISO, die verantwoordelijk is voor de organisatie van de informatiebeveiliging. In het beleid staat dat bij de afdelingen ICT, Functioneel beheer en facilitaire zaken een (Information) Security Officer (ISO) verantwoordelijk is voor de informatiebeveiliging (taken: vertalen van het beleid naar operationele maatregelen binnen de afdeling, toezicht houden op implementatie en naleving).

In de praktijk bleek de organisatorische inrichting van informatieveiligheid niet optimaal te werken, waardoor de ontwikkeling daarvan eind 2015/begin 2016 is gestagneerd. Sinds eind april 2016 (toen een interim-CISO als kwartiermaker werd aangesteld) staat de organisatorische verankering van het taakveld informatieveiligheid weer prominent op de agenda van het college. In augustus 2016 is op basis van de eerste indrukken/bevindingen en in overleg met de CIO de opdracht van de CISO/kwartiermaker bijgesteld en verder geconcretiseerd. De verankering van de rollen en verantwoordelijkheden binnen het taakveld informatieveiligheid is expliciet opgenomen in het (door de directie vastgestelde) actieplan informatieveiligheid en privacy 2016-2018 (versie 1.2). Dit actieplan is tot stand gekomen door een GAP-analyse: een vergelijking van de huidige situatie (IST) met de gewenste situatie (SOLL) (zie paragraaf 2.5).

De Governance rondom informatieveiligheid is dus in de loop der tijd steeds structureler en formeler ingericht. De organisatorische inrichting van informatieveiligheid ziet er nu als volgt uit:

- Op *strategisch niveau* wordt overlegd met de portefeuillehouder informatieveiligheid en de gemeentesecretaris c.q. diens plaatsvervanger. Dit overleg wordt meer en meer geformaliseerd; zo wordt inmiddels gewerkt met een vaste agenda en verslaglegging. De intentie is om minimaal één keer per kwartaal op dit niveau te overleggen.
- Op *tactisch niveau* wordt minimaal één keer per maand overlegd in het security en privacy overleg onder voorzitterschap van de CIO. In dit overleg zijn verder aanwezig: functionaris gegevensbeheer (privacy officer), stafjurist met focus op privacy, senior adviseur gegevensbeheer, senior (IT) auditor en risicomanager en de CISO. Doel van dit overleg is afstemming met betrekking tot taakvelden informatieveiligheid en privacy en de gezamenlijke aanpak/voortgang. Het security en privacy overleg werkt al met een formele agenda, verslaglegging is in opbouw.
- Op *tactisch/operationeel* niveau overlegt de CISO met name met twee ISO's. Deze ISO's behoren tot GemICT, de nieuwe gemeentelijke ICT-organisatie van de gemeenten Arnhem, Renkum en Rheden. GemICT valt onder de bedrijfsvoeringorganisatie De Connectie, die nog in oprichting is. Daarom kent het overleg tussen de CISO en ISO's nog een informeel karakter. Wel heeft de CISO de twee ISO's bij de IBD als algemeen èn vertrouwelijk coördinator informatiebeveiliging laten aanmelden.
- Op *operationeel niveau* wordt met alle relevante spelers overlegd als daartoe aanleiding is (vraag gestuurd en incident gedreven). Met vertegenwoordigers van de afdelingen functioneel beheer, IT-Audit & risk management en gegevensbeheer vindt nu nog op ad-hoc basis overleg plaats (korte lijnen). Gewerkt wordt aan een meer structurele overlegstructuur, waarbij nadrukkelijk wordt gekeken naar regionale samenwerking.

De CISO en ISO's vormen samen het Incident Management Team. Het Incident Management Team is verantwoordelijk voor het behandelen van informatiebeveiligingsincidenten en neemt passende maatregelen bij informatiebeveiligingsincidenten.[34] In uitvoerende taken is de proceseigenaar/lijnmanager verantwoordelijk voor de integrale informatiebeveiliging van zijn of haar werkproces/organisatieonderdeel. In interviews komt naar voren dat het per afdeling verschilt hoe invulling wordt gegeven aan deze verantwoordelijkheid. Dat onderstreept volgens geïnterviewden het belang van de specifieke functies en overleggen op het gebied van privacy- en informatieveiligheid.

2.5 / Taken en systemen rondom informatieveiligheid

In deze paragraaf wordt aandacht besteed aan specifieke taken en systemen waar het informatieveiligheidsbeleid invloed op heeft. Eerst wordt het 'actieplan informatieveiligheid en privacy' beschreven. Vervolgens wordt ingegaan op de organisatie van autorisaties voor informatiesystemen, hoe de gemeente zicht heeft op beveiliging van gegevens in de backoffice en de procedure voor datalekken. Tot slot wordt besproken hoe de gemeente invulling geeft aan 'privacy by design' en informatieverarming.

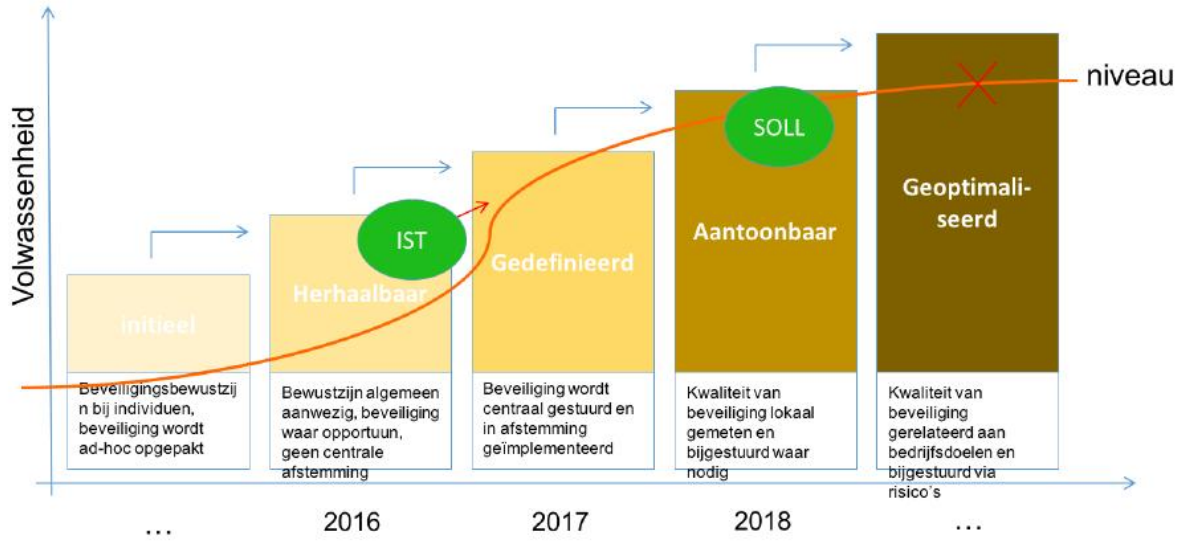
Strategie uitgewerkt in een concreet en meetbaar actieplan

In het informatieveiligheidsbeleid is genoemd dat de gemeente in een strategie uitwerkt welke onderwerpen er in de komende jaren aangepakt moeten worden om tot de BIG te komen. Begin 2015 is daar een start mee gemaakt door een GAP-analyse uit te voeren aan de hand van een 'educated guess'. Deze GAP-analyse wordt als basis gebruikt voor het door de directie vastgestelde actieplan informatieveiligheid en privacy 2016-2018. In het actieplan staat de ambitie vermeld om eind 2018 aantoonbaar 'in control' te zijn taakvelden informatieveiligheid en privacy, regie te voeren èn daarover op professionele wijze

[34] Beleid voor informatiebeveiliging 2015-2018, p.8

verantwoording af te leggen (zie Figuur 1). Door het college zijn hier middelen voor vrijgemaakt: voor het taakveld informatieveiligheid in 2016 en 2017 jaarlijks € 145.000,- en daarna jaarlijks € 85.000,-.

Figuur 1. Ambitie actieplan informatieveiligheid en privacy 2016-2018



Om aan de ambitie van het actieplan te kunnen voldoen investeert het college onder andere in een information security management system (ISMS), waarmee informatieveiligheid en privacy op procesniveau kan worden geborgd. Ook is er een aantal 'pleisterprojecten' benoemd, waar de gemeente direct mee aan de slag moet. Eén van deze projecten is een inventarisatie van de processen waarin gegevensverwerking plaatsvindt. Verder is een belangrijk speerpunt van het actieplan het optimaliseren van de Plan-Do-Check-Act-cyclus, waarin onder andere planning, acties, controle en evaluatie een plek moeten krijgen. Intern worden de acties nu bijgehouden aan de hand van kwartaalrapportages. Daarin komen zowel technische maatregelen, als maatregelen op beleid, Governance en incidenten aan bod. Er is sprake van een duidelijke planning en een heldere en concrete onderbouwing van de genomen of geplande maatregelen.

Duidelijk overzicht van autorisaties

De gemeente heeft een duidelijk overzicht van autorisaties. De gemeente heeft autorisatieregisters voor CVS, GWS, Stratech en Suwinet. Het CVS is het cliënt- volgsysteem voor de sociale wijkteams. GWS is een registratiesysteem voor afdelingen Werk, Inkomen en Zorg. Stratech wordt vooral gebruikt op het gebied van Participatie. Suwinet is het ICT-systeem voor de Structuur Uitvoering Werk en Inkomen waar meerdere uitvoeringsorganisaties in samen kunnen werken.

Voor CVS (van software-ontwikkelaar Conclusion) is inzichtelijk gemaakt in welke systeemonderdelen een coach, een cliënt en een teamleider toegang hebben. Voor GWS bestaat per medewerker een overzicht van de taken die hij/zij kan uitvoeren, uitgesplitst per module, optie en suboptie daarvan. Voor Stratech bestaat het autorisatieregister uit een overzicht van de gebruiker (weergegeven volgens een viercijferig ID) plus de bijbehorende autorisatie. Voor Suwinet bestaat een autorisatiematrix waarin staat beschreven welke

functieprofielen bij welke Suwinet pagina's horen. Maandelijks worden door het Bureau Keteninformatisering Werk en Inkomen (BKWI) algemene gegevens beschikbaar gesteld over het gebruik van Suwinet.[35]

De sociale wijkteams maken verder gebruik van het communicatiesysteem Vecozo, een beveiligde omgeving waarin onderling en met zorgpartners gecommuniceerd kan worden. De sociale wijkteams maken geen gebruik van Suwinet.

Vertrouwen in informatieveiligheid backoffice, beperkte controle

Gevolgen transitie waren lastig in te schatten voor de gemeente en voor Zorg-Lokaal

Het bedrijf Zorg-Lokaal regelt de backoffice (verwerken toewijzing zorgaanbieder, betalingen regelen, persoonsgebonden budget regelen met de Sociale Verzekeringsbank) van Wmo-dienstverlening zoals pgb, beschermd wonen, jeugdzorg, dagbesteding. De gemeente (afdeling Ondersteuning Werk &Inkomen, OWI) doet de backoffice voor Wmo-voorzieningen: wonen, rollen en vervoer. Wanneer wordt besloten tot een behandeling geeft de wijkcoach bij Zorg-Lokaal aan dat deze stap wordt genomen. Wanneer een zorgaanbieder een factuur indient kan Zorg-Lokaal vervolgens inzien of de factuur wordt ingediend voor een behandeling die daadwerkelijk toegewezen is.

Vanaf augustus/september 2014 is besloten dat een deel van de backoffice bij Zorg-Lokaal terecht zou komen, omdat de gemeente er niet klaar voor was om dat zelf te organiseren. Mede door de landelijke onduidelijkheden rondom de transities stonden de gemeente en Zorg-Lokaal vervolgens nog voor een grote uitdaging. De gemeente dacht dat de transitie grotendeels was geregeld door de backoffice extern te organiseren en sociale wijkteams aan te stellen. Maar er bleek een groot grijs gebied: gegevens die vanuit de AWBZ/Jeugdzorg kwamen waren niet op orde, waardoor de systemen van sociale wijkteams, gemeente, Zorg-Lokaal, zorgaanbieders en de Sociale Verzekeringsbank (SVB) niet op elkaar aansloten. De productencatalogus die werd gebruikt was niet handzaam voor gebruikers. Gevolgen hiervan waren bijvoorbeeld het achterblijven van declaraties, maar ook bijvoorbeeld dat sociale wijkteams geen signaal kregen bij overlijden doordat zij geen inzage in de Gemeentelijke basisadministratie (GBA) hadden.[36] De gemeente moest als verantwoordelijke meer werk verzetten dan van tevoren was ingeschat. Om helderheid te krijgen over bijvoorbeeld verkeerde productcodes moest er overleg plaatsvinden via mail of telefoon, waarbij ook persoonsgegevens gedeeld werden. Dat is verbeterd toen de landelijke data werden opgeschoond.

Controle op privacy Zorg-Lokaal is beperkt

In een interview is aangegeven dat de samenwerking met Zorg-Lokaal op vertrouwen is gebaseerd. De gemeente Arnhem is een grote klant van het bedrijf en door het belang dat het college hecht aan privacy zal Zorg-Lokaal zich daarom goed willen laten zien op het gebied van privacy en informatieveiligheid. Zorg-Lokaal is volgens ambtelijk betrokkenen scherp op privacy en werkt op 'need to know' basis. Zorg-Lokaal wil alleen de gegevens hebben die ze nodig heeft om de facturen op rechtmatigheid te kunnen toetsen ('dataminimalisatie'). Er is volgens de ambtelijke organisatie dus geen reden om te twijfelen aan de werkwijze van Zorg-Lokaal. De ambtelijke organisatie geeft aan dat op ad hoc-basis vanuit de gemeente

[35] Handboek Suwinet, p.9.

[36] De sociale wijkteams krijgen nu een wekelijks GBA mutatie-overzicht met betrekking tot hun klanten.

aandacht wordt besteed aan privacy bij Zorg-Lokaal, en niet op structurele wijze. Het is bij de ambtelijke organisatie wel bekend dat Zorg-Lokaal een eigen procedure 'Meldplicht datalekken' kent en hanteert.

Het is de wens van de ambtelijke organisatie om via overleg meer invloed te kunnen uitoefenen op de strategische keuzes van Zorg-Lokaal, bijvoorbeeld om wel of niet te investeren in systemen, ICT en beveiliging. Dit past volgens de ambtelijke organisatie ook bij een strategisch partnerschap.

Procedure datalekken is goed georganiseerd

De procedure rondom het melden van een datalek is vastgelegd en is bekend in de gemeente. Wanneer een datalek heeft plaatsgevonden vult de betrokken ambtenaar het zogenaamde 'meldingsformulier beveiligingsincident' in. De deelnemers van het privacy- en securityoverleg ontvangen automatisch een mail met dit meldingsformulier. Degene die de melding als eerste ziet beoordeelt (vaak na overleg) de ernst en spoedeisendheid van de kwestie. Hierbij worden zaken afgewogen als de ernst en omvang van het lek, wat de risico's zijn, of het lek nog steeds plaatsvindt, hoe gevoelig de gegevens zijn en hoe politiek gevoelig de zaak is. Ook wordt afgewogen of er een melding gemaakt moet worden aan de Autoriteit Persoonsgegevens, hier kunnen de 'Beleidsregels meldingsplicht' van de AP voor worden doorgenomen. Tot slot wordt aan de hand voor door de AP opgestelde criteria besloten of de betrokken inwoner op de hoogte moet worden gesteld.[37] De beoordelaar van de melding stelt alle leden van het privacy- en securityoverleg op de hoogte van de gemaakte afwegingen.

Wanneer er een melding gemaakt moet worden bij de AP wordt het meldingsformulier ingevuld door de CISO, met vermelding van de FG als contactpersoon. In februari 2016 kreeg de gemeente Arnhem te maken met een datalek. Het meldingsformulier van dit datalek bevestigt deze procedurele stappen. Daarmee kan gezegd worden dat er een duidelijke procedure is rondom datalekken en dat deze in de praktijk ook daadwerkelijk wordt gevolgd.

Aandacht wordt besteed aan privacy by design en informatieverarming

Uit de interviews met betrokkenen blijkt dat het college van burgemeester en wethouders zich bewust is van het belang van informatieverarming, waarbij informatie tot een abstracter niveau wordt gereduceerd zonder dat aan effectiviteit of efficiency wordt ingeboet. Hier speelt echter wel dat de gemeente soms afhankelijk is van andere partijen voor het bereiken van verarming. Betrokkenen geven aan dat een voorbeeld waarbij geen sprake is van verarming gevonden kan worden bij Suwinet, het systeem dat de gemeente vanuit het Rijk krijgt opgelegd. In feite hoeft een gemeentelijk medewerker alleen te weten of iemand bijvoorbeeld wel of niet in aanmerking komt voor een uitkering, terwijl het systeem veel meer informatie toont. Wanneer een systeem ingericht zou worden waarbij de meest informatie-arme gegevens worden getoond, kent volgens de gemeente ook de beveiliging minder risico's: wanneer het eventueel toch mis gaat, wordt veel minder informatie blootgegeven. Hier ligt ook een 'privacy by design'-vraagstuk: hoe richt je een systeem zo in, dat alleen de noodzakelijke informatie wordt opgeslagen en gedeeld? De gemeente heeft de uitgangspunten van informatieverarming en privacy by design wel goed kunnen verwerken in het CVS, het cliëntvolgsysteem dat gebruikt wordt door de sociale wijkteams. Uit de interviews blijkt dat de maker van het CVS, Conclusion, aangaf dat het CVS van Arnhem het meest uitgeklede systeem is (in termen van wat er wordt geregistreerd) dat hij heeft geleverd.

[37] Autoriteit Persoonsgegevens, 2015. De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp), p. 32.

Sociale wijkteams als poortwachter informatieveiligheid

Ondanks het feit dat het belang van informatieverarming wordt gezien, geven betrokkenen ook voorbeelden van situaties waarin dit niet in eerste instantie als uitgangspunt wordt gehanteerd. Wijkteammedewerkers gelden dan als poortwachter. Zo wilde een aantal medewerkers van de gemeente Arnhem graag een koppeling tussen de systemen van de gemeente en het CVS. De sociale wijkteams hebben toen aangegeven dat dit niet mogelijk was omdat in het CVS gegevens staan die in vertrouwelijkheid door inwoners zijn aangedragen. Een ander voorbeeld op casusniveau was een bezwaarprocedure waarbij de afdeling juridische zaken graag het hele dossier van een cliënt in wilde zien, terwijl dit volgens de wijkcoach niet noodzakelijk was voor het behandelen van het bezwaar. De opvatting van de wijkcoach is in dit geval opgevolgd. Een laatste voorbeeld betreft een project (‘Ontknoping’) waarin een grootschalige data-opschoning plaatsvindt om de vervuiling in systemen minimaal te houden (vanuit het uitgangspunt ‘correctheid’). De sociale wijkteams attendeerden er bijvoorbeeld op dat de gemeente niet zomaar een uitzendkracht kan inschakelen voor de opschoning van de gegevens. Het is voor de gemeentelijke backoffice-medewerkers een leerproces geweest om te ontdekken wat mag en wat niet mag op het vlak van privacy, in combinatie met een zo pragmatisch mogelijke aanpak.

Deze voorbeelden lijken erop te duiden dat de aandacht voor informatieveiligheid en privacy sterk aanwezig is bij wijkteammedewerkers, er wel een goede Governance is binnen de ambtelijke organisatie wat betreft eindverantwoordelijkheden, maar dat het bewustzijn nog niet breed aanwezig is onder medewerkers in de ambtelijke organisatie. Dat wordt ook ondersteund door een datalekincident, waarbij de betrokken ambtenaar zich niet bewust was van de plicht om dit te melden met hulp van het ‘meldingsformulier beveiligingsincident’.[38]

2.6 / Informatievoorziening aan de raad

In deze paragraaf wordt besproken hoe de raad wordt geïnformeerd over het gevoerde beleid op privacy en informatieveiligheid.

Informatievoorziening via raadsinformatiebrief en P&C-cyclus

Over informatievoorziening aan de raad staat in de Notitie Privacy Sociaal Domein (december 2014) dat het college verantwoording aflegt door:[39]

- de raad te informeren over wezenlijke aspecten van het privacybeleid en incidenten van ernstige aard;
- periodiek (tenminste eenmaal per jaar) aan de raad verantwoording af te leggen – bijvoorbeeld door middel van een raadsbrief – over de wijze waarop aan het privacybeleid uitvoering is gegeven, gehouden evaluaties en eventueel genomen maatregelen ter verbetering;
- de raad te informeren over de resultaten van het in de eerste helft van 2015 te houden Privacy Impact Assessment (PIA), inclusief eventuele voorstellen ter verbetering.

Een incident van ernstige aard heeft zich nog niet voorgedaan. De periodieke verantwoording heeft plaatsgevonden in december 2014, toen de Notitie ter vaststelling in de raad is voorgelegd. In februari 2016 is in een raadsinformatiebrief informatie gegeven over de stand van zaken met betrekking tot privacy in het

[38] Dit datalek is bekend bij de rekenkamer. Nadat het datalek bekend werd bij de Functionaris Gegevensbescherming, zijn wel de voorgeschreven stappen ondernomen.

[39] Notitie Privacy Sociaal Domein, p. 7.

sociaal domein, waarin onder ander wordt ingegaan op de PIA (zie paragraaf 3.1). Er zijn geen raadsbrieven gestuurd waarin gehouden evaluaties gepresenteerd zijn.

In het algemeen informatieveiligheidsbeleid staat dat het college verantwoording aflegt over het functioneren van informatieveiligheid conform de planning en control cyclus. In de jaarrekening 2015 wordt kort iets over het thema gezegd. Zo wordt de ambitie genoemd om een betrouwbare IT te hebben, waarbij 'Snel, Safe en Simpel' het uitgangspunt is.[40] Ook geeft het college aan, de klant centraal te willen stellen en dat via een aantal projecten, waaronder informatieveiligheid, te willen uitwerken. Het functioneren van de informatieveiligheid komt niet aan de orde. In het jaarverslag 2015 komt dat wat uitgebreider ter sprake: zo wordt aangegeven dat de governance structuur van informatiebeveiliging en privacy in elkaar geschoven is en dat werkprocessen ten behoeve van informatiebeveiliging zijn verbeterd.[41] Er is een bewustwordingscampagne gestart in 2014 en afgerond in 2015, die in 2016 hernieuwd zal worden. Verder staat er dat wegens de noodzaak tot externe verantwoording de auditlast sterk toeneemt. Het college geeft aan dat de volgende audits en (verplichte) zelfonderzoeken zijn uitgevoerd:

- EDP audit Beaufort en Decade (in het kader van de controle op de jaarrekening);
- DigiD audit;
- Archiefinspectie;
- zelfevaluatie BRP (Basisregistratie personen, vervanging van de GBA audit);
- zelfevaluatie P-Nik (waardepapieren en reisdocumenten);
- zelfevaluatie Suwi.

Er wordt in de jaarrekening 2015 niet aangegeven of deze audits tot opmerkelijke uitkomsten of verbeteringen hebben geleid. Op basis van de jaarrekening is het daarom niet vast te stellen wat de mate van informatieveiligheid binnen de gemeente op dat moment was.[42]

Privacy als politiek thema: raadsleden ervaren geen grip op dossier

Hoewel het college dus op verschillende momenten de gemeenteraad van informatie heeft voorzien, hebben raadsleden in een bijeenkomst aangegeven dat zij geen grip ervaren op het dossier. Zij hebben het gevoel de juiste informatie te missen om als raadslid te kunnen controleren of het college voldoet aan de gestelde kaders. De gesproken raadsleden vinden dat er heldere kaders zijn gesteld door middel van de Notitie Privacy Sociaal Domein, maar hebben het gevoel dat ze niet de vinger aan de pols kunnen houden. Dat komt zowel doordat zij zichzelf onvoldoende in positie brengen, en doordat zij volgens hen onvoldoende in positie worden gebracht door het college. Raadsleden geven aan dat het moeilijk te achterhalen is in welke mate de uitgangspunten in de praktijk worden nageleefd. Raadsleden merken dat ze op zoek zijn naar hun rol met betrekking tot privacy en informatieveiligheid. Als volksvertegenwoordiger krijgen zij wel verhalen of incidenten mee, maar het is lastig om aan de hand daarvan de juiste vragen aan het college te stellen. Sommige raadsleden vragen zich af tot op welk detailniveau zij zich moeten bemoeien met de uitvoering van het privacy- en informatieveiligheidsbeleid. Het college merkt dat ook: vragen vanuit raadsleden zijn vaak gebaseerd op signalen vanuit individuele gevallen. Het college kan dan juist vanuit de bescherming van privacy niet specifiek ingaan op de casuïstiek. Volgens het college zit er dus een spanning tussen het verzamelen van informatie om inzicht te geven in de praktijk van de sociale wijkteams en de bescherming van privacy.

---

[40] Jaarrekening 2015, p. 34.

[41] Jaarverslag 2015, p. 124.

[42] In de ambtelijke reactie op dit rapport is aangegeven dat de 'mate van informatieveiligheid binnen de gemeente op een bepaald moment' vanuit het bureau van de CIO/CISO elke dag kan worden aangegeven.

Er zijn verschillende momenten geweest waarop raadsfracties vragen hebben gesteld over privacy en/of informatieveiligheid. Zo zijn bijvoorbeeld vragen gesteld door de SP over de waarborging van privacy binnen de sociale wijkteams (9 januari 2014), door D66 over de beveiliging van Suwinet (24 juni 2015), door Verenigd Arnhem over privacy binnen de Jeugdwet (8 december 2015) en door GroenLinks en SP over het datalek in februari 2016. Een ander voorbeeld (hoewel niet in het sociaal domein) werd tijdens de bijeenkomst met raadsleden in het kader van dit onderzoek aangereikt. Dit voorbeeld ging over een inwoner die een klacht heeft ingediend naar aanleiding van een gemeentelijk formulier dat moet worden ingevuld voor de WOZ-waardebepaling. Volgens deze inwoner vraagt de gemeente in dit formulier naar niet-relevante, persoonlijke informatie.

Bij raadsleden heerst het gevoel dat de antwoorden van het college op vragen van de raad appelleren aan het ‘vertrouwen’, namelijk dat er vanuit het college aandacht voor is, en dat er geen signalen zijn dat het niet goed gaat. Raadsleden geven aan dat zij informatie wensen die dat vertrouwen onderbouwt, bijvoorbeeld uitkomsten van controles, steekproeven en evaluaties. Tegelijkertijd geven sommige raadsleden aan dat zij dergelijke informatie misschien te weinig hebben geëist van het college. De gesproken raadsleden zijn het erover eens dat de kans bestaat dat in de toekomst een keer een groot incident zal plaatsvinden, waarbij bijvoorbeeld de hulpverlening tekort is geschoten doordat informatie niet is gedeeld. Een goede informatievoorziening zou volgens hen een debat over een dergelijk voorval minder complex maken.

Reken kamer Arnhem

3 Uitvoering: sociale wijkteams en zorgpartners

Dit hoofdstuk gaat in op hoe privacy en informatieveiligheid in de praktijk gestalte krijgen, of dit voldoet aan de wettelijke en lokale kaders en wat dit betekent voor inwoners (deelvragen 4, 5 en 7). De praktijk van de sociale wijkteams en de ervaringen van zorgpartners komen in dit hoofdstuk aan bod.

3.1 / Privacy binnen de sociale wijkteams

In deze paragraaf wordt besproken welke afspraken sociale wijkteams hebben gemaakt rondom privacy en hoe er in de praktijk wordt omgegaan met privacy. De communicatie met inwoners komt ook aan de orde. Tot slot wordt uitgebreid ingegaan op de overgang van de sociale wijkteams naar de stichting Sociale wijkteams Arnhem.

Sociale wijkteams als toegangspoort Wmo en Jeugdwet

Op 1 januari 2015 zijn in Arnhem acht sociale wijkteams voor volwassenen en voor jeugd van start gegaan. De sociale wijkteams bestaan uit wijkteamleiders en wijkcoaches (medewerkers die in dienst zijn van maatschappelijke organisaties, de gemeente Arnhem en/of ZZP-ers). De gemeente Arnhem heeft met de ca. 25 moederorganisaties van de medewerkers van de sociale wijkteams samenwerkingsovereenkomsten gesloten. Daarin is vastgelegd dat alle partijen zich aan het beleid van de gemeente houden op het gebied van gegevensbewerking en privacy en dat alle medewerkers tot geheimhouding zijn gehouden met betrekking tot informatie die de gemeente Arnhem betreft.

Het doel van de sociale wijkteams is het ondersteunen van de inwoners van de Gemeente Arnhem bij hun zelfredzaamheid, het versterken van deze zelfredzaamheid en het waar nodig organiseren en coördineren van hulp en ondersteuning. Het wijkteam fungeert als toegangspoort naar de voorzieningen en ondersteuning op het terrein van de Jeugdwet en de Wmo.[43] De opzet voor de sociale wijkteams is tijdelijk; vanaf 1 januari 2017 worden de sociale wijkteams op afstand gezet in een stichting met coöperatieve eigenschappen. Hierna zal dit nog aan de orde komen.

Status werkafspraken privacy sociale wijkteams

Bij het opstellen van de Notitie Privacy Sociaal Domein was het uitgangspunt dat het privacybeleid zou worden verankerd in de vorm van werkprocessen en een privacy-protocol. Daarnaast zou een PIA, Privacy Impact Assessment, worden uitgevoerd. Het privacy-protocol is echter niet opgesteld en de PIA niet uitgevoerd. Het college heeft daarvoor de volgende uitleg gegeven: omdat de privacy in de ogen van het college voldoende geborgd is in de sociale wijkteams en de sociale wijkteams per 1 januari 2017 een andere vorm aan zullen nemen, wordt de situatie afgewacht die na 1 januari 2017 zal ontstaan. Na 1 januari 2017 zal het college bekijken of het sluiten van een privacy-protocol nog toegevoegde waarde heeft, omdat in de 'Samenwerkingsovereenkomst Sociale wijkteams' de geheimhoudingsplicht van de wijkteammedewerkers al is vastgelegd en is vastgelegd dat de sociale wijkteams zich op het gebied van gegevensverwerking en

[43] Zie art. 2.2. van de Samenwerkingsovereenkomst Sociale wijkteams.

privacy houden aan het beleid van de gemeente Arnhem. Ook zal het college na 1 januari 2017 bekijken op welke wijze een PIA een bijdrage kan leveren aan een goede borging van het onderwerp privacy bij de inrichting van de sociale wijkteams.[44] Echter, de Samenwerkingsovereenkomst is slechts geldig tot 1 januari 2017.

Voor de daarin opgenomen afspraken zal dus per 1 januari 2017 vervanging moeten komen. Hierop wordt later in dit hoofdstuk nog ingegaan.

Wel zijn er in november 2014 werkafspraken gemaakt voor de sociale wijkteams, opgesteld door de wijkteammanager met privacy 'in de portefeuille'. Deze afspraken zijn vastgesteld na raadpleging van de FG. De werkafspraken houden bijvoorbeeld in dat de coach alleen persoonsgegeven verzamelt ten behoeve van een bepaald doel, dat de coach informatie altijd deelt met alle betrokkenen, tenzij de veiligheid van een inwoner of zijn/haar omgeving in het gedrang komt, en dat het wijkteam alleen in contact treedt met inwoners wanneer de inwoners daarmee instemmen. Verder schrijven de afspraken voor welke informatie de coach bij het eerste contactmoment met de inwoner dient te verstrekken,[45] dat informatie niet per mail wordt uitgewisseld, maar bij voorkeur in persoon en anders telefonisch en dat in teamoverleg bij casusbespreking alleen namen worden genoemd wanneer daarvoor een reden bestaat. Daarnaast bepalen de werkafspraken dat de coach bij twijfel of er wel of geen info gedeeld mag/moet worden, altijd samen met een collega besluit.

Privacy-bewustzijn goed aanwezig in het wijkteam, maar afwegingskader ontbreekt

In de interviews is aangegeven dat niet alle coaches de werkafspraken op papier kennen, maar dat de meeste coaches in de praktijk wel volgens de afspraken werken, al is dit niet altijd het geval. Privacy komt in het teamoverleg aan de orde en is onderdeel van het inwerkprogramma (waarbij een nieuwe coach 'meeloopt' met collega's). Zo krijgt de coach de werkwijze rondom privacy mee, zoals het delen van gegevens van de cliënt, het informeren van de cliënt over privacy et cetera.

De sociale wijkteams hanteren het principe 'nee, tenzij…'. Dat het 'handig' kan zijn, is geen reden om gegevens te delen. Voor gegevensverwerking wordt altijd de toestemming van de inwoner gevraagd. De enige uitzondering op die regel is wanneer de veiligheid in het gedrang is. Hierbij kan gedacht worden aan kinder- of oudermishandeling. Een inwoner kan met het wijkteam in aanraking komen op eigen initiatief of bijvoorbeeld via Veilig Thuis (VT). In dat laatste geval ontvangt het wijkteam via de mail een summiere zaakomschrijving van VT, bijvoorbeeld "Er heeft huiselijk geweld plaatsgevonden in aanwezigheid van 3-jarige dochter", en persoonsgegevens zoals adres, namen en geboortedatum. Coaches bespreken een casus zolang dat kan, anoniem. Neemt een derde, bijvoorbeeld de overlastcoördinator, met toestemming van de cliënt contact op met de coach, dan kan de coach telefonisch met de derde overleggen, maar informatie geven via mail is dan niet aan de orde.

Dossiers zijn toegankelijk voor de leden binnen een wijkteam (zie paragraaf 3.2 voor het informatiesysteem). In teamvergaderingen worden cases teambreed besproken; daarbij worden volgens wijkteammedewerkers geen namen genoemd. Soms vindt binnen het wijkteam overdracht plaats naar een andere coach met toestemming van de cliënt.

[44] Zie Raadsinfo d.d. 23-2-2016 "Privacy in het sociale domein: Stand van zaken na een jaar van sociale wijkteams".

[45] "Bij ieder eerste huisbezoek deel je de folder "Sociale wijkteams; steun en advies dichtbij" en de folder "informatie van de sociale wijkteams over; privacyregeling, klachtenregeling, bezwaar en beroep en vertrouwenspersoon" uit."

Transparantie is voor wijkteammedewerkers essentieel: de coach neemt de inwoner mee in alle beslissingen die raken aan privacy en gegevensdeling, bijvoorbeeld of derden bij de zaak betrokken worden, welke gegevens gedeeld worden. Bij de afweging of de wijkteamcoach gegevens deelt, staat het belang van de inwoner, de individuele behoefte centraal. Coaches ervaren volgens hen geen dilemma's bij het maken van privacy-afwegingen. Overleg blijft bijna altijd binnen het team en mocht een externe worden betrokken, dan noemt de coach geen namen, maar bespreekt de zaak anoniem.

Bij het opstellen van de Notitie in 2014 was voorzien dat het systeem van triage zou worden toegepast door de sociale wijkteams. Triage is een proces waarmee zorgvragen worden verhelderd en gerouteerd en dat ondersteuning biedt bij het nemen van besluiten over gegevensdeling. Uit de interviews blijkt echter niet dat triage wordt toegepast. Volgens het college vindt dat overigens wel plaats, zo blijkt uit het antwoord van het college op vragen gesteld door het toenmalige College bescherming persoonsgegevens.[46] Het per stap om toestemming vragen (eerst toestemming voor contact met omgeving, dan toestemming voor contact met hulpverlening) is volgens het college een vorm van triage. Dit sluit echter niet aan bij de definitie van triage als een verhelderend en gerouteerd proces voor besluiten rondom gegevensdeling.

Wat opvalt, is dat de sociale wijkteams zich enerzijds zeer bewust lijken van privacy: bij verzoeken om gegevensdeling wordt gekeken of en zo ja welke gegevens noodzakelijk gedeeld moeten worden, er wordt zoveel als mogelijk gesproken over cases zonder namen te noemen, er wordt altijd toestemming gevraagd voor gegevensdeling en er wordt gekozen voor de communicatiemethoden die het minste risico voor privacy opleveren. Anderzijds ontbreekt een eenvoudige systematiek of een stappenplan waarin in ieder geval de juridische afwegingen (zoals proportionaliteit en subsidiariteit) zijn opgenomen. Daarmee kan de wijze van afwegen persoonsafhankelijk zijn en kan een eenduidige werkwijze ontbreken, hoewel getracht wordt dit te voorkomen door privacy-issues met collega's of binnen het team te bespreken. Bovendien wordt ook in de praktijk (net als in de werkafspraken) veel waarde gehecht aan het verkrijgen van toestemming voor gegevensdeling van de inwoner. Dat is problematisch gezien de afhankelijkheidsrelatie die bij hulpverlening vaak speelt en die maakt dat toestemming niet volledig vrij wordt gegeven: daarom heeft de Autoriteit Persoonsgegevens het standpunt ingenomen dat toestemming in het sociaal domein vaak geen grondslag oplevert voor het delen van gegevens.[47] De sociale wijkteams zouden zich er daarom van bewust moeten zijn dat er in dat geval een andere grondslag dan toestemming dient te bestaan voor de gegevensdeling. Ook moet men zich ervan bewust zijn dat toestemming, ook wanneer deze wel 'vrij' is gegeven en een grondslag vormt voor gegevensverwerking, nooit afdoet aan de eis om noodzaak, proportionaliteit en subsidiariteit van de gegevensverwerking af te wegen. Dit bewustzijn lijkt niet aanwezig.

Overigens staat ten tijde van het schrijven van deze rapportage aanpassing van de werkafspraken op de agenda. Omdat communicatiemiddelen als Whatsapp en sms niet in de werkafspraken zijn meegenomen, voldoen de werkafspraken niet meer volledig. Bij de herziening van de werkafspraken worden de coaches in de sociale wijkteams geraadpleegd.

Praktische oplossingen voor preventief handelen

Wijkcoaches komen alleen bij een inwoner terecht wanneer de inwoner daar zelf mee instemt. Soms krijgen wijkcoaches echter ook signalen van bijvoorbeeld omwonenden of andere organisaties dat een inwoner

[46] Brief van College van B&W aan College bescherming persoonsgegevens, 1 mei 2015.

[47] Zie het Onderzoeksrapport "Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming", van april 2016 en hiervoor voetnoot 17.

mogelijk een ondersteuningsbehoefte heeft. Vanuit de ambitie om ook preventief en 'vroegsignalerend' te werken, probeert de gemeente daar praktische oplossingen voor te vinden. Als bijvoorbeeld het signaal vanuit de politie komt, kunnen wijkcoaches samen met de politie in contact treden met een inwoner. Voor het college is het nog wel de vraag hoe dit goed georganiseerd kan worden. De inzet van algemene voorzieningen (voorzieningen waarvoor geen indicatie nodig is) zal in de komende jaren steeds belangrijker worden. Wijkteams 'leefomgeving' zullen daarin een belangrijke rol vervullen. De koppeling tussen wijkteams leefomgeving en sociale wijkteams in het kader van privacy moet volgens het college nog verder worden uitgedacht.

Informatievoorziening over privacy aan inwoners is niet altijd toereikend

Wanneer de wijkcoaches het keukentafelgesprek aangaan, laten ze voor de inwoner standaard drie flyers achter: één over het wijkteam in het algemeen, één over de klachtenbehandeling in de sociale wijkteams en één over privacy. In deze laatste folder wordt aangegeven dat gegevens alleen worden gedeeld met toestemming van de betreffende inwoner, tenzij er een wettelijke plicht is om informatie te delen. Ook wordt de geheimhoudingsplicht van de coaches benoemd, evenals de rechten van inwoners.

In een inwonersonderzoek van april 2016 gaf 33% van de ondervraagden aan dat de wijkcoach niet had gesproken over privacy en dat 25% niet wist of het onderwerp besproken was.[48] Dit kan een teken zijn dat het achterlaten van de folder niet voldoende informatie geeft over privacy. Uit de interviews blijkt echter ook dat het voorkomt dat de folders vergeten worden. Via de website van de gemeente is de folder wel te achterhalen, maar er is verder geen pagina waarop wordt uitgelegd hoe de gemeente omgaat met persoonsgegevens. Informatievoorziening over privacy aan inwoners is daardoor aanwezig, maar beperkt.

Overgang naar stichting laat ingezet, nog veel onbekend over zicht op privacy

Coöperatieve stichting

Per 1 januari 2017 worden de sociale wijkteams opnieuw gepositioneerd in een stichting, de Stichting Sociale wijkteams Arnhem. In de kadernota 'Naar een veerkrachtige samenleving' (2014) is deze herpositionering al aangekondigd.[49] Het principebesluit om een stichting op te richten is op 17 mei 2016 ter kennisgeving voorgelegd aan de gemeenteraad, waarna is vastgesteld dat de raad geen wensen en bedenkingen heeft ten aanzien van het besluit.[50] De keuze voor een zogeheten 'coöperatieve stichting' is onder andere gemaakt vanuit de ambitie om een regiegemeente te zijn en belangenverstrengeling bij aanbieders te voorkomen (wat bijvoorbeeld kan voorkomen als er aanbieders van algemene voorzieningen de wijkteams organiseren).[51]

In de business case Sociale wijkteams is te lezen hoe de structuur van de stichting eruit ziet. De stichting kent een Dagelijks Bestuur en een Algemeen Bestuur, met een fulltime bestuur dat de dagelijkse leiding heeft over de organisatie en samen met de bestuurder-teamleiders het algemeen bestuur vormt van de organisatie. Een Raad van Toezicht is werkgever van het algemeen bestuur en houdt toezicht op het beleid

[48] De sociale wijkteams door inwoners beoordeeld, Onderzoek & Statistiek gemeente Arnhem, april 2016.

[49] Notitie Naar een veerkrachtige samenleving, 2013.

[50] Besluitenlijst vergadering van de raad Arnhem 27 juni 2016.

[51] Business case Sociale wijkteams, 27 april 2016.

van het bestuur en op de algemene gang van zaken in de organisatie. De RvT bestaat uit onafhankelijke leden. In de business case is aangegeven dat in de opbouwfase een gemeentelijk afgevaardigde zal deelnemen, maar in een latere raadsinformatiebrief geeft het college aan dat hiervan afgeweken wordt. De reden daarvoor is de gewenste afstand tussen de gemeente en de stichting, en dat de invloed van de gemeente op de totstandkoming voldoende is geborgd omdat de gemeente de werving van de leden van de RvT op zich neemt.[52] Naast de RvT is er nog sprake van een Adviesraad, een Cliëntenraad en een Ondernemingsraad.

Sturing op privacy en informatieveiligheid
Omdat de gemeente verantwoordelijk blijft voor de uitvoering van het Arnhemse stelsel in het kader van de Wmo 2015 en Jeugdwet, geeft de gemeente als opdrachtgever en financier ook vorm aan sturing op de stichting. Dat betekent dat een aantal afspraken zijn vastgelegd in de statuten (vastgesteld door het college op 8 november 2016). In een bedrijfsplan en bijbehorende opdrachtverlening geeft de gemeente de stichting eisen en voorwaarden mee voor de uitvoering en organisatie van de sociale wijkteams. Ten tijde van dit onderzoek was het bedrijfsplan nog niet bekend: op 6 december zal het bedrijfsplan in het college worden besproken. Het is daarom niet vast te stellen welke aandacht privacy en informatieveiligheid in het bedrijfsplan krijgen.

In de business case krijgt privacy geen aandacht. Over informatieveiligheid zegt de business case het volgende: de coöperatieve stichting zal gebruikmaken van de IT-infrastructuur die specifiek voor de sociale wijkteams is ontworpen (onder andere het CVS-systeem). Het idee is dat de stichting geleidelijk meer verantwoordelijk wordt voor de inkoop en het beheer van de IT-infrastructuur (denk aan service-applicaties, opslag en dienstverlening). Dat betekent dat er afspraken gemaakt moeten worden tussen de stichting en de gemeente over het uitwisselen van gegevens, zodat de gemeente bijvoorbeeld gegevens ter beschikking heeft om afspraken te maken met aanbieders. Hoe controle en zicht op informatieveiligheid van bewaarde gegevens precies georganiseerd wordt, is nog niet bekend. De onlangs aangestelde EDP-auditor moet hierin een rol vervullen. Voor zover de stichting als 'bewerker' persoonsgegevens verwerkt in opdracht van de gemeente als 'verantwoordelijke' (in de zin van de Wbp), worden afspraken vastgelegd in een bewerkersovereenkomst. Een voordeel van het organiseren van wijkteams in een stichting is uiteraard wel dat er slechts één organisatie hoeft te worden gecontroleerd, in plaats van alle deelnemende organisaties.

Geen privacy-protocol of PIA
De raadsinformatiebrief van 23 februari 2016 gaat wel in op privacy binnen de stichting. Er wordt gerefereerd aan de Notitie Privacy Sociaal Domein, waarin is aangegeven dat er een (aanvullend) privacy-protocol met de partners zou worden gesloten en een Privacy Impact Assessment (PIA), om de privacy-risico's van de stichting in kaart te brengen, zou worden uitgevoerd. Vanwege de snel naderende overgang naar de stichting acht het college deze twee stappen niet meer zinvol. De privacy is volgens het college gewaarborgd onder andere doordat het CVS-systeem niet gekoppeld is aan de gemeentelijke systemen en dat de geheimhoudingsplicht al is vastgelegd in de algemene 'Samenwerkingsovereenkomst Sociale wijkteams'. Ook is in die overeenkomst al vastgelegd dat de sociale wijkteams zich op het gebied van gegevensverwerking en privacy houden aan het beleid van de gemeente Arnhem. Of een privacy-protocol of een PIA een bijdrage kan leveren, wil het college bekijken wanneer bekend is welke vorm de sociale wijkteams gaan krijgen.

[52] Raadsinformatiebrief Oprichting Stichting Sociale Wijkteams Arnhem, 8 november 2016.

De samenwerkingsovereenkomst waar het college naar verwijst, geldt voor de periode 2015-2016.[53] Als deze van belang is voor afspraken omtrent privacy en informatieveiligheid, zal er per 1 januari 2017 een vervanging moeten komen. In een interview is aangegeven dat de afspraken een plek zullen krijgen in de opdrachtverlening, waarin zal staan dat de stichting moet voldoen aan de kaders die de gemeente heeft gesteld op dit thema. Het is niet bekend of en hoe de gemeente wil sturen op het waarborgen van privacy in de werkwijze van de sociale wijkteams. In het gesprek met raadsleden kwam naar voren dat ook voor hen hier nog weinig zicht op is. De tijd voor raadsleden om hier vragen over te stellen is beperkt, aangezien eind november de statuten, het bedrijfsplan en de opdrachtverlening nog niet bekend waren bij de gemeenteraad. Naar aanleiding hiervan hebben verschillende fracties een agendaverzoek ingediend voor de Politieke Maandag op 12 december 2016, dat gehonoreerd is.[54]

3.2 / Informatieveiligheid binnen de sociale wijkteams

In deze paragraaf wordt ingegaan op de wijze waarop informatieveiligheid is vormgegeven binnen de sociale wijkteams.

Systemen sociale wijkteams zijn beveiligd

Wanneer een inwoner contact opneemt met een wijkcoach, volgt een keukentafelgesprek met twee wijkcoaches. Vanaf dat moment wordt gebruikgemaakt van het Cliënt Volg Systeem (CVS). De wijkcoaches maken gebruik van email en laptops van de gemeente Arnhem, op basis van systemen van Vecozo. Met behulp van een code die op de telefoon (eveneens door de gemeente geleverd) binnenkomt kunnen de coaches inloggen in het CVS. De coaches werken dus – mits zij er gebruik van maken – binnen een beveiligde omgeving. Wanneer de coach per mail gegevens verstuurt naar een ander mailsysteem (bijvoorbeeld omdat informatie naar een inwoner wordt gestuurd) is er geen sprake van een beveiligde verbinding of versleuteling. Het mailverkeer tussen de gemeente en de wijkteams is beveiligd.

Dataminimalisatie meegenomen in vormgeving CVS

Bij het ontwerpen van het CVS is volgens de principes van dataminimalisatie en privacy by design gewerkt, zo blijkt uit de interviews. Bij de ontwikkeling van het CVS is een team van 8-9 wijkteammedewerkers betrokken. Samen is gekeken naar welke informatie echt geregistreerd moest worden. Om over goede managementinformatie te beschikken, is veel geregistreerde informatie handig, maar het uitgangspunt voor het sociaal domein was om zo min mogelijk te registreren. Zoals gezegd levert dat dus een spanning op tussen het verkrijgen van gedetailleerde informatie, die het college ook kan gebruiken om de raad te informeren, en het zo minimaal houden van registratie in het kader van privacy en informatiebeveiliging. Alles wat niet bijdraagt aan de primaire taak van een wijkcoach hoeft niet in het systeem opgenomen te worden. Naast privacyoverwegingen zit hier ook een gebruiksvriendelijk aspect in. Als het systeem minder functionaliteiten biedt is het eenvoudiger te bedienen.

[53] Overeenkomst Samenwerking Sociale wijkteams, artikel 5.

[54] Op 6 december 2016 heeft het college het bedrijfsplan van de stichting Sociale Wijkteams Arnhem, met onder andere de opdrachtformulering, opgestuurd aan de raad. Dat wordt op 12 december 2016 naar aanleiding van het agenderingsverzoek besproken.

Transparantie door burgerportaal, bewaartermijnen onbekend

Zowel de cliënt als de coach heeft toegang tot het Mijn Plan/Ons Plan (MP/OP) dat samen wordt opgesteld. Er is één toegang voor burgers in het CVS (burgerportaal), en één voor de wijkcoach en de teamleider. Hierdoor is transparantie voor inwoners georganiseerd. Het college geeft hierbij aan terughoudend te willen zijn: hoe meer systemen ook open worden gezet voor inwoners, des te meer beveiligingsrisico's de gemeente loopt. Daarom zullen stappen richting meer zelfregie van inwoners over hun dossier met voorzichtigheid worden benaderd.

De autorisaties voor wijkcoaches en wijkteamleiders verschillen. Binnen een wijkteam kunnen alle coaches en de teamleider de dossiers inzien. Dit faciliteert dat de coaches elkaar kunnen vervangen als dat nodig is. Het is niet mogelijk om de dossiers van een ander wijkteam te bekijken. Wanneer een cliënt klaar is (het MP/OP is gerealiseerd) wordt het dossier gesloten. Dan blijft het dossier nog wel bestaan. Wanneer hier om wordt gevraagd, kan een dossier wel vernietigd worden. Bij wijkteammedewerkers is het niet bekend welke termijnen er gelden voor het bewaren van de dossiers, en er is geen procedure voor het afsluiten van dossiers. Hierop vindt ook geen geautomatiseerde controle plaats. Uit een groepsgesprek met enkele zorgpartners kwam ook naar voren dat het voor hen niet helder is hoe lang dossiers bewaard blijven in het informatiesysteem. Dat vormt een risico voor het uitgangspunt dataminimalisatie: worden gegevens onnodig langer bewaard?

Overgang naar stichting heeft ook gevolgen voor ICT en informatieveiligheid

Op dit moment faciliteert de gemeente Arnhem de ICT van de sociale wijkteams. Als de nieuwe stichting volledig zelfstandig opereert huurt de stichting ICT als dienst in bij de gemeente Arnhem. De sociale wijkteams bepalen dan het beveiligingsniveau en de autorisaties. Het is mogelijk dat de sociale wijkteams uiteindelijk voor andere ICT-oplossingen kiezen. Dit vraagt dat de gemeente zicht houdt op de kwaliteit van de systemen en de borging van de privacy daarin.

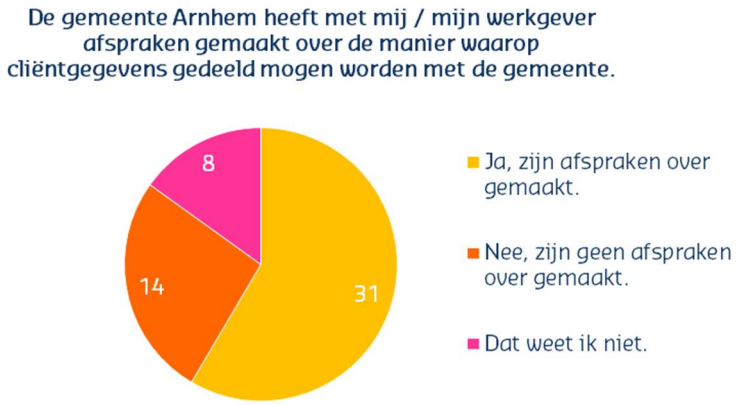
3.3 / Ervaringen van (zorg)partners

In deze paragraaf wordt het beeld van zorgpartners[55] over privacy en informatieveiligheid in de gemeente Arnhem besproken. Om hier een indruk van te krijgen, is een enquête verstuurd onder 116 gecontracteerde en een 10 niet-gecontracteerde partners in het sociaal domein (zie Hoofdstuk 1 van de Bestuurlijke Nota: Onderzoeksverantwoording). De respons (42%) levert een betrouwbaar beeld van de meningen van zorgpartners. Het gaat hierbij om de meningen/indrukken van de partners en niet per definitie om de feitelijke situatie. Om duiding te geven aan de uitkomsten uit de enquête is een groepsgesprek met vertegenwoordigers van negen organisaties gehouden. Deze organisaties vertegenwoordigen alle onderdelen van het sociaal domein (Wmo, Jeugdwet en Participatiewet) en verschillende samenwerkingen met de gemeente (met en zonder contract, deelnemers aan het wijkteam). De bevindingen uit de enquête en uit het groepsgesprek worden hieronder beschreven.

[55] De enquête is grotendeels door gecontracteerde zorgpartners ingevuld, maar ook door andere organisaties (bijv. basisschool, reïntegratiebedrijf). Voor de leesbaarheid wordt vanaf nu de term 'zorgpartners' gebruikt.

Niet elke partner heeft afspraken gemaakt over privacy

Aan de zorgpartners is ten eerste de vraag voorgelegd of de gemeente Arnhem afspraken heeft gemaakt met de zorgpartner over de manier waarop cliëntgegevens worden gedeeld (Figuur 2). Een meerderheid van de respondenten (31 van de 54) geeft aan dat de gemeente inderdaad afspraken heeft gemaakt met de zorgpartner over het delen van cliëntgegevens. In het domein Jeugd antwoordt bijna driekwart van de respondenten positief, in het domein Wmo is dat aandeel kleiner (8 van de 15, 53%). Kennelijk meent een aanzienlijk deel van de respondenten dat er geen afspraken zijn gemaakt met de gemeente over gegevensdeling. Ook in het groepsgesprek met enkele zorgpartners bleek dat niet iedereen afspraken heeft met de gemeente of de sociale wijkteams (of daar van af weet) over het delen van gegevens. Een deel zegt ook niet te weten van afspraken. Dit kan erop duiden dat bijvoorbeeld afspraken die door middel van contracten met de gemeente zijn gemaakt, door de organisaties niet bekend zijn gemaakt bij hun medewerkers.

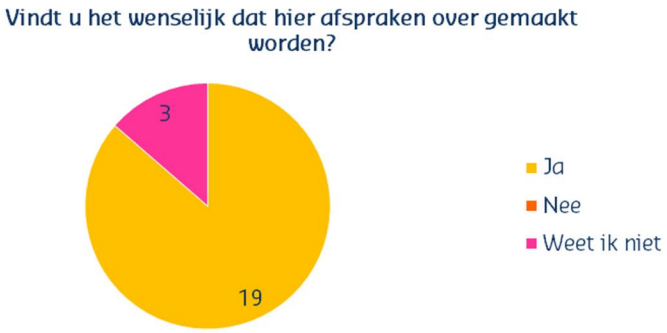


Figuur 2. Afspraken zorgpartners en gemeente

Onderstaande grafiek geeft aan in hoeverre men bekend is met de gemaakte afspraken. Het overgrote deel van de respondenten geeft aan bekend te zijn met de afspraken en deze toe te passen in de praktijk (Figuur 3). In het groepsgesprek is aangegeven dat men hierbij denkt aan afspraken over geheimhouding en het vragen om toestemming van de cliënt.

Figuur 3. Bekendheid met afspraken

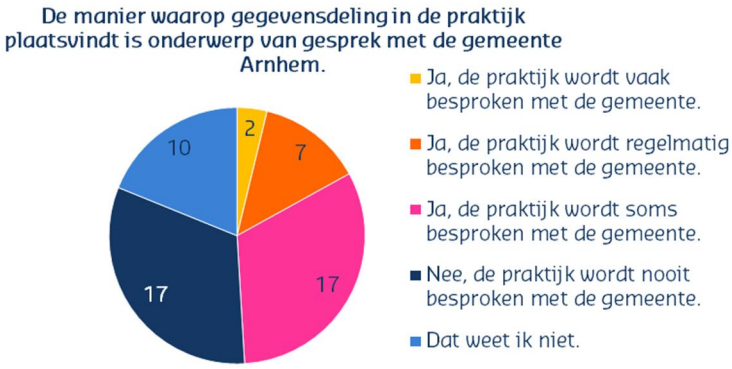
Aan de respondenten die hebben aangegeven dat er geen afspraken zijn gemaakt of dit niet weten (22), is gevraagd of het maken van afspraken wenselijk is (Figuur 4). Verreweg de meeste respondenten zijn van mening dat dit inderdaad wenselijk is (19 van de 22).



Figuur 4. Wenselijkheid maken afspraken

Gemengde beelden over gesprek met gemeente over privacy

Ook is zorgpartners de vraag voorgelegd of de manier waarop gegevensdeling in de praktijk plaatsvindt wordt besproken met de gemeente (Figuur 5). De antwoorden laten een wisselend beeld zien. Bijna de helft van de respondenten geeft aan dat dat gebeurt; ongeveer een derde geeft aan dat dit nooit het geval is. In het groepsgesprek is aangegeven dat in individuele contacten met wijkteamcoaches het onderwerp wel aan de orde komt, maar dat er niet op een structurele manier aandacht aan wordt besteed. Enkele deelnemers aan het gesprek gaven aan wel een keer aanwezig te zijn geweest bij een gemeentelijke bijeenkomst over privacy.

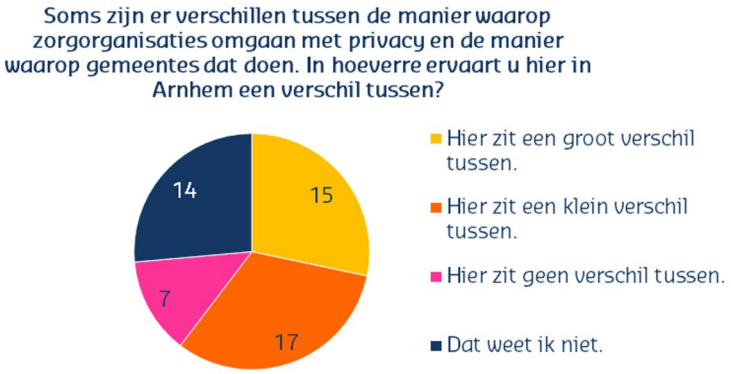


Figuur 5. Delen gegevens met de gemeente[56]

[56] 'Vaak', 'regelmatig', 'soms' zijn niet gedefinieerd. Het gaat om het beeld van de zorgpartners.

De gemeente heeft een andere houding jegens privacy dan zorgpartners

Wanneer personen uit verschillende domeinen en richtingen samenwerken, zoals gemeente en maatschappelijk veld, kan het zijn dat zij signaleren dat hun partners op een andere wijze omgaan met privacy. De zorgpartners is de vraag voorgelegd of zij verschil ervaren tussen de gemeente en de zorgorganisatie in de manier waarop wordt omgegaan met de privacy (Figuur 6). Een ruime meerderheid (32 van de 53) geeft aan inderdaad een verschil te ervaren. Slechts een kleine groep (7 van de 53) geeft aan geen verschil te ervaren.



Figuur 7. Verschil in omgang met privacy zorgpartners en gemeente[57]

Dit beeld wordt bevestigd in de interviews, waarin wordt aangegeven dat de sociale wijkteams privacy meer op het netvlies hebben dan de gemeentelijke organisatie. Dit werd overigens niet alleen gezegd door gesprekspartners van buiten de gemeente, maar ook van binnen de gemeentelijk organisatie. Genoemde voorbeelden van deze andere kijk op privacy bij de gemeente, zijn het verzoek van de gemeente om de gemeentelijk systemen te koppelen aan het CVS, of verzoeken van de gemeente om inzicht in het complete cliëntdossier in een bezwaarprocedure. Bij sociale wijkteams leeft het gevoel dat de gemeente wel soms ‘gemak, handigheid’ als grond gebruikt om gegevens te verwerken.

In samenhang hiermee heeft een respondent aangegeven dat de gemeente inhoudelijk qua privacy meer de beroepscodes uit de zorg zou moeten volgen.

Overigens zijn er ook bemoedigende geluiden te horen. Zo geven respondenten aan dat de gemeente Arnhem het vergeleken bij andere gemeenten (rondom Arnhem) ‘erg goed’ doet.

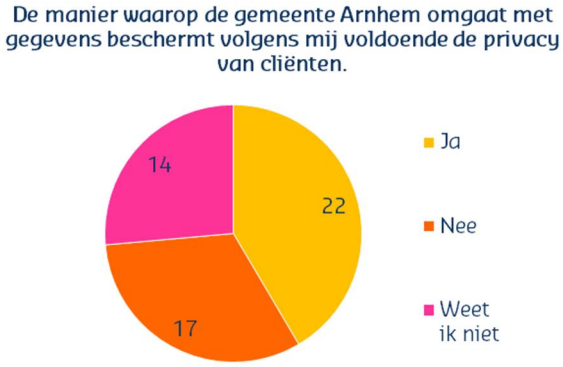
Zorgpartners aan het woord:

“Op inhoudelijk vlak vind ik dat de gemeente meer de beroepscode die in ons vak geldt mag volgen. Als een wijkcoach contact met ons opneemt, is het belangrijk dat daar een schriftelijke toestemming voor is. Ook is het belangrijk dat er een beveiligde communicatie (bijv. zorgmail) tot stand gaat komen.”

[57] ‘Groot’ en ‘klein’ zijn niet gedefinieerd. Het gaat om het beeld van de zorgpartners.

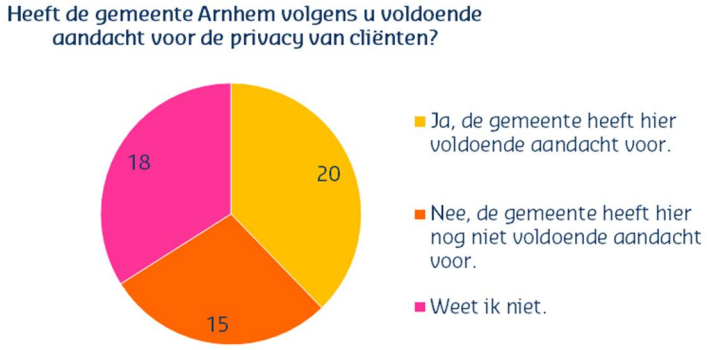
Zorgen bij zorgpartners over bescherming persoonsgegevens

De zorgpartners zijn ook bevraagd over de mate waarin de privacy van de inwoners van Arnhem wordt beschermd en over de aandacht van de gemeente Arnhem voor privacy (Figuur 8). De antwoorden laten zien dat er bij een aanzienlijk deel van de zorgpartners die geantwoord hebben, zorgen zijn. Maar 22 van de 53 respondenten geven aan dat de manier waarop de gemeente Arnhem omgaat met gegevens de privacy van cliënten voldoende beschermt; 17 personen, een derde van de respondenten, vinden dat de privacy van Arnhemmers niet voldoende is beschermd. Meer dan een kwart heeft 'weet ik niet' geantwoord. Overigens antwoordden de respondenten uit het domein Wmo het meest positief. In het groepsgesprek kwam naar voren dat het antwoord 'weet ik niet' is gegeven omdat men gewoonweg geen zicht heeft op hoe de sociale wijkteams de gegevens opslaan en delen met derden.



Figuur 8. Bescherming privacy door gemeente[58]

Slechts 20 van de 53 respondenten vinden dat de gemeente voldoende aandacht heeft voor privacy (Figuur 9). Het is daarmee nog wel de grootste responsgroep, tegenover 15 personen die menen dat de gemeente onvoldoende aandacht heeft voor privacy en 18 personen die het niet weten. In de open antwoorden kwam ook naar voren dat zorgverleners geen zicht hebben op hoe er binnen de gemeente wordt omgegaan met privacyregels en daarom 'weet ik niet' antwoorden.



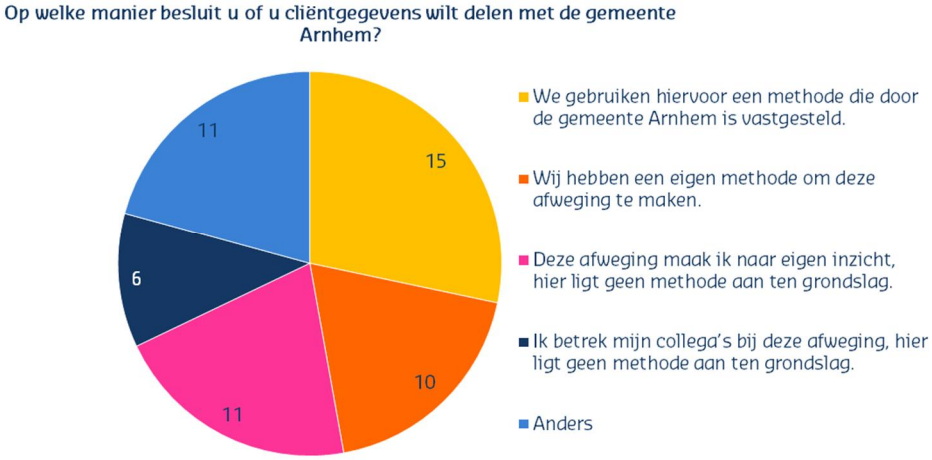
Figuur 9. Aandacht voor privacy cliënten

[58] 'Voldoende' is niet gedefinieerd. Het gaat om het beeld van de zorgpartners.

Variatie in beslismethodes gegevensdeling

De zorgpartners zijn ook ondervraagd over de wijze waarop binnen hun organisatie wordt beslist over gegevensdeling (Figuur 10). Er is een grote verscheidenheid zichtbaar in de wijze waarop de afweging om gegevens te delen wordt gemaakt (ook binnen de verschillende domeinen). Alle vijf mogelijke antwoorden zijn in bijna evenredige mate vertegenwoordigd, van gebruik van een methode van de gemeente, het gebruik van een eigen methode, tot naar eigen inzicht of met behulp van collega's. Daarnaast is er een redelijk grote categorie (11 van de 53 respondenten) die 'anders' heeft geantwoord. Zorgpartners die dit antwoord hebben gegeven, geven daarbij in de toelichting bijvoorbeeld aan dat ze een stappenplan gebruiken: "We gaan na 1. wat is het doel van de gegevensverstrekking 2. Welke gegevens zijn noodzakelijk 3. Kan de informatie beveiligd verstuurd worden? 4. Is de privacy van de cliënt voldoende gewaarborgd in het registratiesysteem?" Een ander antwoord luidt dat de zorgverlener nooit zelf iets naar de gemeente stuurt; als de gemeente/wijkcoach vraagt om bijvoorbeeld een rapportage, laat de zorgorganisatie dit door de ouders zelf overhandigen. Ook opvallend veel respondenten hebben geantwoord "via Vecozo", of "uitsluitend met toestemming van de cliënt". Mogelijk hebben die respondenten de vraag gelezen als stond er "op welke manier deelt u cliëntgegevens met de gemeente".

In het groepsgesprek met enkele zorgpartners werd aangegeven dat de zorgpartners verschillen ervaren in de wijze van gegevensdeling die verschillende wijkcoaches hanteren. Er lijkt geen uniformiteit te zijn in de manier waarop wijkcoaches een afweging maken om gegevens te delen. Het wordt dan ook door alle gesproken zorgpartners als een gemis ervaren dat er geen eenduidige werkwijze is op dit gebied. In de sessie werd de optie aangedragen om met de gemeente en zorgpartners in gesprek te gaan over gegevensdeling met inwoners, met de gemeente en met zorgpartners.



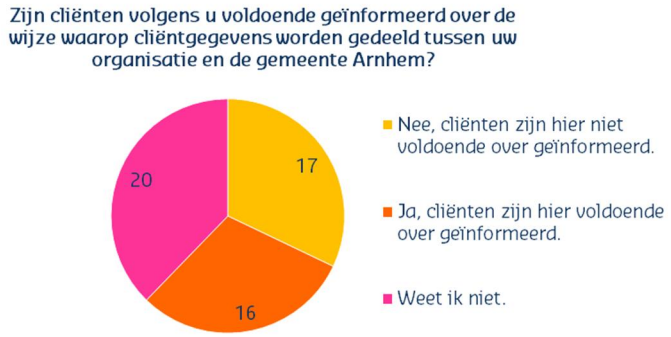
Figuur 10. Beslissen over gegevensdeling

Informeren cliënten moet beter volgens zorgpartners

In de enquête is de zorgpartners gevraagd of zij menen dat cliënten voldoende zijn geïnformeerd over de wijze waarop cliëntgegevens worden gedeeld tussen de organisatie en de gemeente (Figuur 11). Wederom

zijn de antwoorden zeer gevarieerd: een derde van de responderende zorgpartners vindt dat cliënten niet voldoende worden geïnformeerd over gegevensdeling, een kleine derde vindt dat dit wel voldoende gebeurt, en een iets grotere groep weet het niet.

Overigens is in gesprekken met de wijkteammedewerkers naar voren gekomen dat cliënten volgens hen nog niet altijd erg privacybewust zijn. Voor cliënten staat voorop dat er antwoord komt op hun hulpvraag; indien daartoe gegevens gedeeld moeten worden, dan zij dat zo, is het signaal dat wijkteamcoaches opvangen. Dit lijkt een onderschrijving van de door de AP naar voren gebrachte waarschuwing dat in een hulpsituatie de cliënt niet volledig in vrijheid de keuze maakt om toestemming te geven tot gegevensdeling.



Figuur 11. Informeren cliënten over gegevensdeling[59]

Zorgpartners aan het woord:

"Wij tillen als overheid en hulpverleners in de regel zwaarder aan de privacy dan de cliënten zelf. Er zijn nog steeds cliënten die zelf de neiging hebben om via internet zonder beveiligde verbinding te communiceren, terwijl ik hier een beveiligde omgeving voor heb voor lopende cliënten."

Ook zijn de zorgpartners bevraagd op het wel of niet plaatsvinden van evaluatie binnen de organisatie (Figuur 12). Een ruime meerderheid van de respondenten (34 van de 53) geeft aan dat de manier waarop gegevens worden opgevraagd en gedeeld, wordt geëvalueerd binnen de organisatie. Bijna een derde van de respondenten (30%) antwoordt dat er geen evaluatie plaatsvindt. Binnen de domeinen 'Jeugd' en 'Wmo+Jeugd' vindt er relatief iets vaker *geen* evaluatie plaats dan in het domein Wmo.

[59] Voldoende' is niet gedefinieerd. Het gaat om het beeld van de zorgpartners.

Figuur 12. Evaluatie opvraag en delen gegevens binnen de organisatie

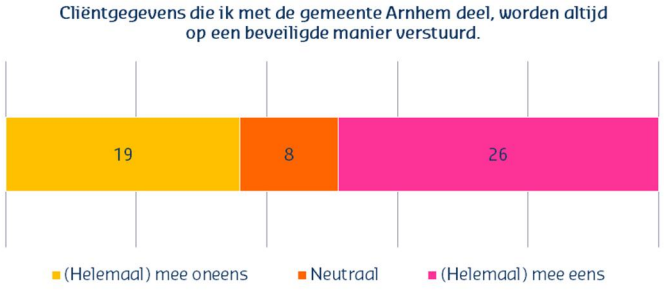
In de enquête is de respondenten ook een open vraag gesteld over de manier waarop evaluatie plaatsvindt. In veruit de meeste gevallen (17 van de 25 gegeven antwoorden) gebeurt evaluatie in de vorm van overleg. De overlegvormen die worden genoemd zijn werk- en teamoverleg, clusteroverleg, overleg in het verband van de commissie Veiligheid en overleg in het samenwerkingsverband. Minder vaak vindt evaluatie plaats door audits, evaluatie, in het kader van de kwaliteitstoetsing, in de vorm van periodieke bevindingen en van risico-inventarisatie en –analyse.

Zorgen over informatieveiligheid

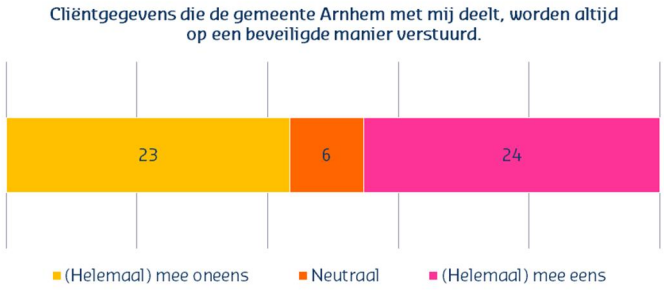
In de enquête is de zorgpartners de mogelijkheid gegeven zaken te uiten die zij kwijt wilden over privacy en informatieveiligheid binnen de gemeente Arnhem. De antwoorden laten zien dat de zorgverleners het van groot belang vinden dat de gegevensdeling veilig verloopt; dat onderwerp wordt buitengewoon vaak genoemd. De zorgpartners hechten veel belang aan beveiligde verbindingen tussen gemeente en zorgverleners en Vecozo wordt genoemd als een veilige werkwijze. Dat soms nog gebruik wordt gemaakt van onversleutelde email baart de respondenten zorgen.

De zorgpartners is gevraagd of de cliëntgegevens die zij met de gemeente Arnhem delen altijd op een beveiligde manier worden verstuurd (Figuur 13). Een bescheiden meerderheid van 26 van de 54 respondenten geeft aan klantgegevens altijd beveiligd te delen met de gemeente; 19 respondenten niet. Gezien het belang dat zorgpartners volgens de open antwoorden in de enquête hebben voor beveiligde gegevensdeling, had wellicht een grotere meerderheid verwacht mogen worden in het ‘eens-kamp’.

Opvallend is ook dat de respondenten slechts een klein beetje sceptischer zijn over gegevensdeling door de gemeente (Figuur 14). De zorgpartners is namelijk dezelfde vraag voorgelegd over de gegevens die de gemeente Arnhem met de zorgpartners deelt. De respondenten denken dat de gegevens die de gemeente deelt iets minder vaak beveiligd zijn.



Figuur 13. Beveiligd versturen gegevens door zorgpartners



Figuur 14. Beveiligd versturen gegevens door gemeente

Zorgpartners aan het woord:

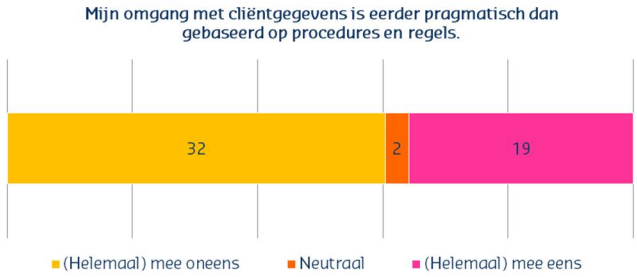
"Correspondentie via Vecozo is OK, via e-mail onversleuteld is geen goede optie. Soms wordt hiervan nog gebruikgemaakt. Wij gaan binnenkort cryptshare gebruiken om privacygevoelige info via email te versturen. Daarnaast is het in de praktijk lastig om exact te weten welke informatie de gemeente nodig heeft voor haar taak. Mogelijk wordt te snel te veel info verstrekt."

Een duidelijker meerderheid zien we in het antwoord op de vraag of cliëntgegevens alleen toegankelijk zijn voor mensen voor wie dat strikt noodzakelijk is (Figuur 15). Een forse meerderheid van 41 respondenten is van oordeel dat cliëntgegevens alleen toegankelijk zijn voor mensen voor wie dat strikt noodzakelijk is. In het groepsgesprek met enkele zorgpartners is aangegeven dat cliënten wel zicht hebben op het ondersteuningsplan ('Ons plan, mijn plan'), maar inwoners worden niet of zelden meegenomen in mailuitwisselingen tussen zorgpartner en wijkteam.

Figuur 15. Cliëntgegevens beperkt toegankelijk

Tot slot is in de enquête aan de zorgpartners gevraagd of hun omgang met cliëntgegevens meer pragmatisch is dan gebaseerd op procedures en regels. Hiermee wordt bedoeld of zorgpartners soms regels omzeilen omdat die in de weg staan van goede zorg. Een minderheid (19 van de 53) bevestigt een meer pragmatische omgang maar een aanzienlijk grotere groep (32 van de 53) ziet zijn omgang met

cliëntgegevens niet als meer pragmatisch. In de gesprekken met de professionals uit de sociale wijkteams is het beeld naar voren gekomen dat professionals het uitgangspunt omarmen dat gegevens niet worden gedeeld omdat dat 'handig' is, maar dat gegevens gedeeld worden wanneer dat noodzakelijk is. Over de wijze waarop de beslissing wordt genomen om wel of niet tot het delen van gegevens over te gaan, werd aangegeven, dat dit zelden tot dilemma's leidt en dat daarbij gewoonweg 'het belang van de cliënt' vooropstaat. Aangezien de primaire opdracht van de zorgverlener is om de cliënt bij te staan/te helpen, is een zeker 'pragmatisme' daarbij onontbeerlijk, maar het belang van privacy en privacybeschermende procedures en regels wordt volgens respondenten niet uit het oog verloren.



Figuur 16. Pragmatische omgang met gegevens

In de open antwoorden komt verder vaak aan bod dat er bij de zorgpartners behoefte bestaat aan meer duidelijkheid: over waar informatie terechtkomt/wie inzicht heeft in informatie, welke gegevens uitgewisseld mogen worden en bij wie de zorgverlener terecht kan met vertrouwelijke informatie. Zo geeft een respondent aan: "Het is mij geheel onduidelijk in iedere gemeente waar ik mee samenwerk wat specifiek de personen zijn waar je vertrouwelijke informatie kwijt kan. Voor ouders is dit ook niet duidelijk." Naast de informatieveiligheid (beveiligde verbinding tussen gemeente en zorgorganisaties) is het gebrek aan duidelijkheid het meest genoemde aandachtspunt.

Zorgpartners aan het woord:

"Er is, zeker naar cliënten toe en soms ook naar hulpaanbieders toe, te weinig helderheid over de plek waar informatie terechtkomt. Bij een beschikkingsaanvraag gaat de informatie naar de backoffice; wie heeft hier inzicht in en wie niet: onvoldoende duidelijkheid. Nog grotere onduidelijkheid is er als er inhoudelijke informatie gedeeld wordt met een wijkcoach: wie heeft inzicht in het dossier?"

Rekenkamer Arnhem

4 Toetsing van normen

In dit hoofdstuk worden de bevindingen op een systematische manier gepresenteerd. Vooraf opgestelde normen worden getoetst aan de hand van de uitkomsten van het onderzoek. Het volgende hoofdstuk geeft vervolgens een antwoord gegeven op de hoofdvraag en benoemt de belangrijkste risico's voor gemeente en inwoners als het gaat om privacy en informatieveiligheid.

Norm	Toetsing
In het privacybeleid van de gemeente ten aanzien van het sociale domein wordt verwezen naar de relevante wettelijke kaders.	**Voldaan:** Het algemeen privacykader en de notitie Privacy in het sociaal domein verwijzen naar de belangrijkste wettelijke kaders: de Wbp en de materiewetten en de toekomstige Algemene Verordening Gegevensbescherming. In het informatiebeveiligingsbeleid 2015-2018 wordt in algemene zin gerefereerd aan 'bestaande wet- en regelgeving' als externe randvoorwaarde. De informatiebeveiliging in Arnhem is opgezet volgens de 'Baseline Informatiebeveiliging Gemeenten', die voldoet aan landelijk wetgeving.
De gemeenteraad heeft in zijn beleid voor het sociaal domein bepalingen vastgelegd over de borging van privacy in het algemeen en de bescherming van persoonsgegevens in het bijzonder en hierbij ook de rolverdeling tussen college en raad vastgelegd.	**Deels voldaan:** Met het algemene privacykader en het Informatieveiligheidsbeleid 2015-2018 heeft de raad bepalingen vastgelegd over de borging van privacy en bescherming van persoonsgegevens. Wat betreft privacy is een heldere rol weggelegd voor de raad en is aangegeven welke verantwoordelijkheden het college op dit thema heeft. In de praktijk zijn raadsleden nog wel op zoek naar de invulling van deze rol en de manier waarop zij grip kunnen houden op privacy. Met betrekking tot informatiebeveiliging is in het beleid geen rolverdeling tussen college en raad vastgelegd.
De gemeente heeft met zorgpartners convenanten afgesloten waarin de voorwaarden voor uitwisseling van persoonsgegevens staan.	**Deels voldaan:** Met de deelnemers van de acht sociale wijkteams zijn samenwerkingsovereenkomsten afgesloten waarin afspraken staan over de uitwisseling van persoonsgegevens. Ten tijde van het onderzoek was het nog niet duidelijk op welke manier afspraken zijn gemaakt met de (toekomstige) stichting Sociale wijkteams Arnhem. Zorgpartners die een contract met de gemeente hebben afgesloten hebben door middel van bepalingen in dat contract afspraken gemaakt omtrent privacy en informatieveiligheid, die niet altijd bekend zijn. 42% van 53 ondervraagde zorgpartners zegt geen afspraken te hebben met de gemeente of niet te weten of er afspraken zijn.
Binnen de gemeentelijke organisatie is een controlemechanisme aanwezig dat er voor zorgt dat er op de juiste wijze	**Deels voldaan:** Er is door het college veel aandacht besteed aan de Governance rondom privacy en informatieveiligheid. Er is een nauwe samenwerking tussen deze twee thema's

wordt omgegaan met privacygevoelige gegevens.	met een duidelijke verdeling in verantwoordelijkheden. Er is een juridische concern controller/Functionaris Gegevensbescherming die steeds meer als interne toezichthouder zal gaan opereren, waarbij een interne auditor dat doet aan de kant van informatieveiligheid. Privacy en informatieveiligheid worden periodiek besproken in een 'security en privacy'-overleg. Ook binnen de sociale wijkteams is privacy als specifiek thema bij een teamleider belegd. Daarnaast worden er verschillende (verplichte) audits gedaan waardoor de gemeente zicht houdt op informatieveiligheid (bijv. DigiD en Suwi). De wijze waarop de gemeente zicht houdt op hoe derden omgaan met gegevens binnen het sociaal domein is minder ontwikkeld. Er is een EDP-auditor aangetrokken om dit vorm te gaan geven. Met de Stichting Sociale wijkteams Arnhem is ten tijde van het onderzoek nog geen afspraak gemaakt over vormen van extern toezicht (naast de Raad van Toezicht), zoals audits of steekproeven. Ook zijn er geen vormen van controle bekend voor gecontracteerde zorgpartners of met Zorg-Lokaal, de organisatie die een deel van de backoffice verzorgt.
a. De gemeente heeft met de zorgpartners formele afspraken gemaakt over hoe zij de omgang met privacygevoelige gegevens van inwoners verantwoorden. b. De gemeenteraad is actief geïnformeerd over de wijze waarop de zorgpartners de privacy van de inwoners waarborgen.	a. **Niet voldaan:** Over de verantwoording van de omgang met privacygevoelige gegevens zijn geen formele afspraken gemaakt. Wel worden in de contracten met zorgpartners algemene bepalingen over privacy opgenomen. b. **Deels voldaan:** De gemeenteraad is via raadsbrieven en in antwoord op vragen geïnformeerd over de wijze waarop wordt omgegaan met privacy in het sociaal domein. De gemeenteraad heeft echter geen informatie ontvangen over de wijze waarop zorgpartners met privacy omgaan. Raadsleden geven aan juist informatie te missen waaruit blijkt dat gemeente en zorgpartners privacy hebben gewaarborgd en gegevens goed hebben beveiligd (bijvoorbeeld via audits/steekproeven).

In werkprocessen ten aanzien van de verwerking van persoonsgegevens zijn taken en bevoegdheden helder beschreven en duidelijk belegd.	**Niet voldaan:** Uit interviews blijkt dat de aandacht en het bewustzijn met betrekking tot privacy en informatieveiligheid bij wijkteammedewerkers hoog is. Het is echter ook gebleken dat er nog veel verschil in werkwijze tussen wijkteammedewerkers zit. Volgens een vertegenwoordiging van zorgpartners die in een groepsgesprek zijn gesproken leidt dat tot momenten waarbij wijkteammedewerkers om (te) veel informatie vragen (bijvoorbeeld wanneer behandelplannen moeten worden verstuurd), maar ook tot situaties waarbij privacy als belemmering wordt opgeworpen om informatie te delen. De werkprocessen lijken te weinig handvatten te bieden waardoor geen eenduidig werkproces gewaarborgd wordt. Hoewel de algemene uitgangspunten wel bekend zijn, is er geen sprake van een stappenplan of afwegingsinstrument waardoor elke wijkteammedewerker op dezelfde manier beslist hoe en met wie gegevens te delen. Tot slot is er onduidelijkheid onder zorgpartners en wijkteammedewerkers wat betreft de bewaartermijnen van dossiers in het CVS.
De werkprocessen zijn - in ieder geval wat betreft het privacyaspect- voor ingebruikname getoetst met betrokken medewerkers op werkbaarheid en risico's.	**Voldaan:** de werkprocessen rondom de sociale wijkteams zijn in samenspraak met de organisaties die in de sociale wijkteams deelnemen tot stand gekomen. De werkprocessen zijn nog altijd onderdeel van gesprek binnen de sociale wijkteams, onder andere doordat een teamleider de 'portefeuille' privacy heeft toebedeeld gekregen. De werkbaarheid en risico's van het CVS zijn ook met medewerkers van het wijkteam besproken. Ook bij het verder ontwikkelen van het CVS zijn sociale wijkteams betrokken.
Uit de werkprocessen is op te maken wanneer, door wie en om welke reden privacygevoelige informatie is geraadpleegd.	**Voldaan:** De gemeente houdt autorisatieregisters bij voor de systemen CVS, GWS, Stratech en Suwinet, waarbij mutaties in autorisaties bij in- en uitdiensttreding en wisselingen van functies worden bijgehouden. Het informatiesysteem voor de sociale wijkteams, Vecozo, is 'green field' ontwikkeld op basis van het uitgangspunt 'privacy by design'. Hierdoor is het systeem beperkt toegankelijk, worden gegevens niet tussen sociale wijkteams gedeeld en is er geen koppeling met een gemeentelijk systeem. Er vindt geen controle achteraf plaats (bijv. aan de hand van loggegevens).

Er wordt periodiek aandacht besteed aan het bewustzijn van medewerkers in het sociaal domein met betrekking tot privacy en informatieveiligheid.	**Deels voldaan:** Uit interviews blijkt dat het bewustzijn onder medewerkers van het wijkteam hoog is. Privacy is een regulier, vast onderwerp van gesprek in teamoverleggen van de wijkteams. Bij de start van de sociale wijkteams zijn trainingen en bijeenkomsten geweest wat betreft het omgaan met privacy en informatieveiligheid. Deze zijn nog niet herhaald. Voor algemene informatieveiligheid in de hele gemeentelijke organisatie van Arnhem is in 2017 een campagne gepland. Het is ten tijde van dit onderzoek niet duidelijk of de gemeente eisen stelt aan de Stichting Sociale wijkteams Arnhem wat betreft aandacht voor privacy en informatieveiligheid onder medewerkers (bijvoorbeeld als standaardonderdeel in het personeelsbeleid). Het is daardoor onduidelijk op welke manier de stichting aandacht zal gaan geven aan privacy bewustzijn.

5 Samenvattend: doelmatigheid, doeltreffendheid en risico's

5.1 / Doelmatigheid en doeltreffendheid

De hoofdvraag van dit onderzoek luidde: *in hoeverre zijn de informatieveiligheid en het privacybeleid in het sociaal domein doeltreffend en doelmatig?*

Door vóór de decentralisaties in 2015 privacy als portefeuille te benoemen en als gemeenteraad een privacykader vast te stellen hebben privacy en informatieveiligheid al bij de invoering van nieuwe structuren, zoals de sociale wijkteams, aandacht gekregen. Deze vroegtijdige investering in beleid en Governance kan als doelmatig[60] worden beschouwd: er sinds de opzet van de sociale wijkteams sprake van veel bewustzijn voor het thema onder wijkteammedewerkers en het informatiesysteem (CVS) van de sociale wijkteams is efficiënt opgebouwd aan de hand van de principes in het privacykader. De visie van het college is dat privacy en informatieveiligheid niet alleen op papier kunnen worden gewaarborgd, maar in de praktijk veelvuldig als gespreksonderwerp aan bod moeten komen.

De gemeenteraad heeft een aantal heldere uitgangspunten vastgelegd in het algemeen privacykader, die als basis fungeren voor de wijze waarop de gemeente omgaat met privacy en informatieveiligheid. De gemeente moet nog stappen zetten in de organisatie en operationalisering van het beleid en is zich daar bewust van. Het is helder dat op dit moment nog niet aan alle uitgangspunten doeltreffend[61] uitvoering wordt gegeven:

- Wijkteammedewerkers zijn zich bewust van *dataminimalisatie*, maar het is onduidelijk hoe lang dossiers bewaard blijven en de werkwijze rondom het vragen van toestemming verschilt per wijkcoach en per (zorg)partner.
- *Doelbinding* (proportionaliteit en subsidiariteit) kent nog geen vaste plek in het afwegingsproces bij het verzamelen en delen van gegevens, en ook hier bestaan verschillende meningen over tussen wijkteammedewerkers en (zorg)partners (onderling).
- De ontwikkeling van het CVS is een voorbeeld van *privacy by design*, maar er worden nog wel veel mails verstuurd die mogelijk ook via een beveiligd systeem zouden kunnen worden verstuurd.
- De gemeente heeft *transparantie* georganiseerd door cliënten ook mee te laten kijken in CVS en er zijn ideeën om nog meer te experimenteren met zelfregie van cliënten. Wel blijkt dat veel cliënten nog niet op de hoogte zijn van hoe de gemeente omgaat met hun gegevens.
- Raadsleden zien *privacy als politiek onderwerp,* maar zoeken ook nog naar hun rol. Zij hebben de indruk dat de informatievoorziening hen daar op dit moment onvoldoende bij helpt, maar beamen dat zij ook zichzelf nog onvoldoende in positie brengen.
- Het kader zou de basis voor een goede *'grondhouding'* van de gemeente ten opzichte van privacy moeten zijn, die inhoudt in dat *iedere bestuurder en medewerker* zich bewust is van situaties waarin privacy een rol speelt. In het college, bij specifieke (eindverantwoordelijke) functies binnen de

[60] Dat wil zeggen: de mate waarin de investeringen van de gemeente op het gebied van privacy en informatieveiligheid staan in verhouding tot de opbrengsten.

[61] Dat wil zeggen: de mate waarin de inspanningen van de gemeente dragen bij aan de realisatie van de vooraf opgestelde doelen.

governance en bij sociale wijkteams is dit bewustzijn inderdaad aanwezig, maar verschillende voorbeelden laten zien dat dit bewustzijn nog niet bij iedere afdeling en alle medewerkers aanwezig is.

De eerste twee jaar na de decentralisaties heeft de gemeente Arnhem aandacht besteed aan de interne structuur en processen rondom privacy en informatieveiligheid. Deze aandacht gaat nu ook steeds meer uit naar privacy en informatieveiligheid bij partnerorganisaties. Voor bijvoorbeeld organisaties als Zorg-Lokaal en de stichting Sociale wijkteams Arnhem, maar ook zorgpartners is het nog de vraag hoe de gemeente hen controleert op waarborging van privacy en informatieveiligheid.

5.2 / Risico's voor inwoners en gemeente

Bovenstaande bevindingen leiden volgens de rekenkamer tot verschillende risico's voor inwoners en gemeente:

- Het bewustzijn over privacy en informatieveiligheid onder wijkteammedewerkers is hoog en zij bieden weerstand aan mogelijke inbreuken op privacy vanuit andere onderdelen van de organisatie. Er is nu nog een risico dat het bewustzijn nog niet gemeentebreed wordt gedeeld.
- Er is geen eenduidig afwegingsinstrument (bijvoorbeeld een stappenplan, een stroomschema) dat algemeen bekend is of wordt toegepast door wijkteammedewerkers. Hierdoor ontbreekt een eenduidige werkwijze van sociale wijkteams in het verzamelen en delen van gegevens per medewerker of team. Het risico hiervan is dat in het ene geval meer (te veel), en in het andere geval minder (te weinig) gegevens van inwoners verzameld en gedeeld worden.
- Zorgpartners en sociale wijkteams hebben verschillende visies en werkwijzen wat betreft het delen van gegevens, waardoor misverstanden kunnen ontstaan die doeltreffende ondersteuning in de weg kunnen staan. Het kan bijvoorbeeld zijn dat informatie niet wordt gedeeld omdat er verschillende ideeën zijn over de manier van toestemming verkrijgen, waarbij in tussentijd geen zorg of ondersteuning wordt opgestart.
- Er worden mails met persoonsgegevens tussen zorgpartners en sociale wijkteams onbeveiligd en soms buiten het zicht van inwoners verstuurd, waardoor persoonsgegevens in de verkeerde handen kunnen vallen en er geen zicht is op de archivering van die mails.
- Inwoners krijgen meer zicht op en regie over hun dossier, maar weten zelf niet altijd genoeg over privacy en informatieveiligheid. Het risico is dat inwoners onvoldoende in positie worden gebracht om regie te voeren over hun dossier.
- Raadsleden hebben nog te weinig grip op het dossier privacy en informatieveiligheid. Zij kunnen zo het college onvoldoende sturen en controleren op het thema.
- De gemeente heeft nog geen of beperkte controlemechanismen ontworpen om zicht te kunnen houden op privacy en informatieveiligheid bij partnerorganisaties. Het risico voor gemeente en inwoners is dat partnerorganisaties, zoals de stichting Sociale wijkteams Arnhem, onvoldoende maatregelen nemen om privacy en informatieveiligheid te borgen en zich daar onvoldoende over verantwoorden.

Bijlagen

Bijlage 1. Geraadpleegde documenten

Naam document
/ Notitie Naar een veerkrachtige samenleving (april 2013) en bijbehorende documenten
/ Kadernota De Veerkrachtige Samenleving Arnhem (december 2013) en bijbehorende documenten
/ Uitvoeringsplan De Veerkrachtige Samenleving Arnhem (juni 2014) en bijbehorende documenten
/ Uitvoeringsnotitie Transformatie Sociaal Domein (mei 2016)
/ Koersnota Van Wijken Weten (2016)
/ Beleidskader voor privacy gemeente Arnhem
/ Notitie privacy in het sociaal domein december 2014
/ Raadbrief 23 december 2014 bij beleid privacy sociaal domein
/ Organisatiebesluit gemeente Arnhem 2013
/ Business case Sociale wijkteams, 27 april 2016
/ VNG Implementatieplan privacy sociaal domein, 2015
/ Samenwerkingsovereenkomst Sociale wijkteams Arnhem
/ Privacy werkafspraken privacy sociale wijkteams
/ Privacy-protocol OZO 2015
/ Handboek voor de coach
/ Jaarrekening gemeente Arnhem 2015
/ Jaarverslag gemeente Arnhem 2015
/ Regeling voor de behandeling van klachten sociale wijkteams
/ Richtlijn voor de behandeling van klachten
/ Beleid voor informatiebeveiliging 2015-2018
/ Handboek Suwinet
/ Overeenkomst Sociaal Domein 2015 hoofdstuk 2 (aanbestedingsdocumenten regionale contractering)
/ Bewerkersovereenkomst Arnhem
/ Autorisatieregisters
/ De sociale wijkteams door inwoners beoordeeld, Onderzoek & Statistiek gemeente Arnhem, april 2016
/ Autoriteit Persoonsgegevens (april 2016), *Onderzoeksrapport: Verwerking van persoonsgegevens in het sociaal domein: de rol van toestemming*
/ Contractkalender sociaal domein
/ Rapport inwonerservaringsonderzoek sociale wijkteams
/ Raadbrief brede evaluatie sociaal domein
/ Collegenota brede evaluatie sociaal domein
/ Flyer wijkteam
/ Folder klachtenbehandeling sociale wijkteams
/ Folder privacy klacht bezwaar en vertrouwenspersoon
/ Melding datalek februari 2016
/ Jaarverslag klachten en bezwaren 2015
/ Raadsbrief afdoen klachten en bezwaren 2015

- Raadsbrief art. 44 18 augustus 2015 privacy Suwinet
- Raadsbrief art. 44 17 februari 2015 waarborging privacy sociale wijkteams
- Raadsbrief art. 44 5 januari 2016 Jeugdbescherming privacy
- Raadsinformatiebrief februari 2016 Stand van zaken 'Privacy in het sociaal domein'
- VNG, Resolutie Informatieveiligheid, randvoorwaarde voor de professionele gemeente
- Verantwoordingsrichtlijn en Normenkader GeVS (23 juni 2011)
- Raadsinfo d.d. 23-2-2016, "Privacy in het sociale domein: Stand van zaken na een jaar van sociale wijkteams"
- Besluitenlijst vergadering van de raad Arnhem 27 juni 2016
- Verordeningen decentralisaties, waaronder Vo Jeugdhulp, Vo Tegenprestatie en Vo Voorzieningen maatschappelijke ondersteuning

Bijlage 2. Gesproken personen

Interviews

Naam	Functie	Datum
De heer M. Leisink	Wethouder, portefeuillehouder privacy	21 oktober 2016
De heer J. Beks	Juridisch concern controller, Functionaris Gegevensbescherming	21 oktober 2016
Mevrouw E. Jansen van Doorn	Eenheidsmanager sociale wijkteams	2 november 2016
De heer M. Hulshoff	Strategisch controller sociaal domein, opdrachtgever bedrijfsvoering sociaal domein	2 november 2016
Mevrouw C. Tönissen Mevrouw R. van Gerwen De heer D. Steens	Teamleider sociale wijkteams Schuytgraaf en Elderveld Wijkteamcoach Malburgen Wijkteamcoach Rijkerswoerd, Kronenburg, Vredenburg	2 november 2016
De heer S. Does De heer C. Deben De heer L. Klein Holte	Chief Information Officer Chief Information Security Officer Informatiemanager	7 november 2016
Mevrouw A. van Pommeren	Relatiebeheerder van o.a. Zorg-Lokaal	17 november 2016
Mevr. A. Haga	Wethouder, portefeuillehouder Wmo	2 december 2016

Groepsbijeenkomst zorgpartners

Naam	Organisatie	Datum
Mevrouw P. Baars Mevrouw M. de Bruyn Mevrouw S. Aleman	Lindenhout Pro Persona Praktijk Rigtering	17 november 2016

Mevrouw M. van Goinga	Basisschool Jongleren	
De heer A. Moerman	Rijnstad	
De heer R. Angenent	Krekel Autismecoaching	
Mevrouw S. Krekel	Krekel Autismecoaching	
De heer R. Voet	Yes We Can Clinics	
De heer R. Wieten	Werk naar Waarde	
De heer G. Rozema	Buurtpastor Klarendal	

Groepsbijeenkomst raadsleden

Naam	Partij	Datum
De heer L. de Groot	Partij voor de Dieren	21 november 2016
Mevrouw K. Kalthoff	VVD	
De heer M. Venhoek	D66	
Mevrouw L. Manders	Arnhem Centraal	
De heer P. Kusters	SP	
Mevrouw R. Peters	GroenLinks	
De heer D. Becker	ChristenUnie	
Mevrouw H. van Nuenen	PvdA	

Bijlage 3. Begrippenlijst

AP – Autoriteit Persoonsgegevens (tot 1 januari 2016 College bescherming persoonsgegevens). De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AWBZ – Algemene Wet Bijzondere Ziektekosten (sinds 1 januari 2015 ondergebracht bij Wet langdurige zorg, Wet maatschappelijke ondersteuning en Zorgverzekeringswet).

BIG – Baseline Informatiebeveiliging Nederlandse Gemeenten; gemeentelijke basisnormenkader voor informatieveiligheid.

BKWI − Bureau Keteninformatisering Werk & Inkomen.

CAK − een publiekrechtelijk zelfstandig bestuursorgaan, belast met de uitvoering van wettelijke taken in het domein van zorg en welzijn, in opdracht van het ministerie van Volksgezondheid, Welzijn en Sport.

CIO – Chief Information Officer, verantwoordelijke ambtenaar voor de informatietechnologie en digitale systemen binnen de gemeente.

CISO – Chief Information Security Officer; specialist op het gebied van de Informatie Beveiligingsfunctie, genoemd in het BIG.

CBP – College bescherming persoonsgegevens (sinds 1 januari 2016 Autoriteit Persoonsgegevens (zie AP).

CVS – Cliëntvolgsysteem.

EDP-auditor – Electronic Data Processor-auditor.

FG – Functionaris voor de Gegevensbescherming. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp).

GAP-analyse – Analyse van verschillen tussen de gewenste en de huidige situatie. In het kader van de privacy bij decentralisaties is het doel van de GAP-analyse om gemeenten te controleren of en in welke mate de maatregelen uit de tactische variant van de BIG zijn geïmplementeerd. Hierbij gaat het om gemeenten die het onderzoek uitvoeren of laten uitvoeren.

GeVS – Gezamenlijke Elektronische Voorzieningen Suwinet. Het Normenkader GeVS wordt gebruikt door de Inspectie Sociale Zaken en Werkgelegenheid om toezicht te houden op de toepassing van deze normen.

GWS – Registratiesysteem; gemeentelijk klant-volgsysteem.

Jeugdwet – Sinds 1 januari 2015 zijn gemeenten verantwoordelijk voor de jeugdhulp. Zij kunnen de zorg dichter bij de inwoners organiseren, maar ook eenvoudiger en goedkoper. De nieuwe organisatie van de jeugdhulp is vastgelegd in de Jeugdwet.

IBD – Informatiebeveiligingsdienst.

Participatiewet – Iedereen die kan werken maar daarbij ondersteuning nodig heeft, valt sinds 1 januari 2015 onder de Participatiewet. De wet is er om zoveel mogelijk mensen met of zonder arbeidsbeperking werk te laten vinden. De Participatiewet vervangt de Wet werk en bijstand (Wwb), de Wet sociale werkvoorziening (WSW) en een groot deel van de Wet werk en arbeidsondersteuning jonggehandicapten (Wajong).

PIA – Privacy Impact Assessment.

Proportionaliteitsbeginsel – Beslissingen van de staat gaan vaak in tegen het belang of de rechten van individuele burgers, ten bate van het algemeen belang. Het proportionaliteitsbeginsel stelt dat de mate van inbreuk op het individueel belang vanuit een bepaalde maatregel proportioneel moet zijn ten opzichte van het beoogde legitieme doel van die maatregel. In het bijzonder dient de inbreuk nooit groter te zijn dan noodzakelijk is voor het beoogde doel.

Subsidiariteitsbeginsel – Organisatiewijze of regel in taakverdeling tussen 'hogere' en 'lagere' openbare overheden. Het houdt in algemene zin in dat hogere instanties niet iets moeten doen wat door lagere instanties kan worden afgehandeld.

Suwinet – Registratiesysteem; systeem van informatie-uitwisseling in de keten van werk en inkomen. Uitvloeisel van de Wet structuur uitvoeringsorganisatie werk en inkomen.

Suwi – Wet Structuur uitvoeringsorganisatie werk en inkomen.

Transparantie – In de context van politiek en bestuurszaken duidt dit begrip op openheid binnen een bestuurlijk of juridisch orgaan, zoals een overheid of een internationale instelling.

Triage – Hulpmiddel bij het goed inregelen van privacy in de werkprocessen van de gemeenten voor de decentralisaties. Het is het proces van verhelderen, routeren en escaleren van vragen en casussen waarbij tevens bepaald wordt welke informatie daarbij nodig is. Triage is erop gericht om op een gestructureerde en gestandaardiseerde manier de mate van integraliteit vast te stellen.

Vecozo – Vecozo, een beveiligde omgeving waarin onderling en met zorgpartners gecommuniceerd kan worden.

Wbp – Wet bescherming persoonsgegevens.

Wmo – Wet maatschappelijke ondersteuning; Gemeenten moeten ervoor zorgen dat mensen zo lang mogelijk thuis kunnen blijven wonen. De gemeente geeft ondersteuning thuis via de Wet maatschappelijke ondersteuning (Wmo). Officieel heet deze wet Wmo 2015.