Van beleid naar borging

Een onderzoek naar het privacybeleid van de gemeente Doetinchem

Onderzoekgegevens, bevindingen en aanbevelingen van de rekenkamercommissie Doetinchem

Augustus 2017

Rekenkamercommissie [gD] Doetinchem

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

PBLQ

verbinders in de informatiesamenleving

1. Inleiding

1.1 Aanleiding

Met de steeds groter wordende betekenis en invloed van digitale gegevensverwerking is in de samenleving de aandacht voor een goede bescherming van de privacy van de inwoners toegenomen. Overheden beheren veel, soms zeer gevoelige, gegevens van inwoners. Dat geldt bij uitstek voor gemeenten. Daar vindt de registratie in het bevolkingsregister plaats. Daar melden inwoners zich voor een vergunning, een uitkering of ondersteuning in het kader van de Wmo. Ook problemen in het gezin worden geregistreerd bij de gemeente. Bovendien vervullen gemeenten een belangrijke rol in het delen van dergelijke basisinformatie over de inwoners met andere instanties.

In de afgelopen jaren is meermalen gebleken dat niet alle gemeenten er in slagen om de vertrouwelijkheid van deze informatie te garanderen en te bewaren. Het belang van een adequaat privacybeleid door gemeenten is daarmee toegenomen. In dit licht heeft de rekenkamercommissie van de gemeente Doetinchem PBLQ gevraagd voor de ondersteuning bij een onderzoek naar het privacybeleid van deze gemeente.

Deze korte introductie op de achtergronden en doel van het onderzoek maakt toch al duidelijk dat dit onderzoek meer behelst dan louter een toets op een aspect van de uitvoering van gemeentelijk beleid. Natuurlijk moet de gemeente aan vereisten in de wet voldoen, maar vanuit het perspectief van de raad gaat het ook om een belangrijk maatschappelijk thema. Met de voortschrijdende invloed van ICT heeft de discussie over de privacy van inwoners aan urgentie gewonnen. Overheden worden steeds indringender geconfronteerd met de afweging tussen enerzijds de roep om een effectieve en efficiënte uitvoering van taken en verantwoordelijkheden en anderzijds de bescherming van de privacy van haar inwoners. Voor een effectieve en efficiënte uitvoering van taken kan het verleidelijk zijn om juist veel gegevens van inwoners te verzamelen en te bewaren.
De raad draagt dus niet alleen een verantwoordelijkheid voor een juiste invulling van het privacybeleid, maar moet ook een positie innemen in de afweging tussen enerzijds de belangen die de gemeente heeft en anderzijds de bescherming van de persoonlijke levenssfeer van inwoners.

Het onderzoek richt zich op de vraag of de gemeente de relevante wet- en regelgeving juist uitvoert. Dit beleid zal in de nabije toekomst enkele wezenlijke veranderingen ondergaan. Op basis van Europese afspraken treedt op 25 mei 2018 nieuwe regelgeving in werking: de Algemene Verordening Gegevensbescherming (AVG). In het onderzoek is er ook aandacht in hoeverre de gemeente zich thans al voorbereidt op de komst van de AVG.
Het privacybeleid kent verschillende risico's. Indien de gemeente in gebreke blijft bij het beschermen van de privacy van de inwoners, kan de gemeente geconfronteerd worden met forse boetes, op te leggen door de Autoriteit Persoonsgegevens. Ook dit risico maakt het onderzoek, mede vanuit het perspectief van de raad, van belang. Duidelijk moet zijn dat de gemeente in het beleid de nodige waarborgen heeft opgenomen om de privacy van de inwoners adequaat te beschermen.

1.2 Opdrachtformulering

De hoofdvraag voor dit onderzoek luidt:

In hoeverre is het privacybeleid bij de gemeente rechtmatig en doelmatig en in hoeverre is de privacy van inwoners geborgd?

Deze hoofdvraag is opgesplitst in deelvragen over het beleid, de uitvoeringspraktijk, betrokkenen en de raad:

Beleid

1) Welk beleid is er geformuleerd rond de privacy van gegevens van de inwoners?
2) Wat zijn de doelen van dit beleid?
3) Voldoet dit beleid aan de wet- en regelgeving?
4) Welke maatregelen neemt de gemeente om (tijdig) voorbereid te zijn op de komst van de nieuwe, scherpere privacyregelgeving (AVG)?

Uitvoering

5) Hoe is de bescherming van persoonsgegevens vormgegeven?
6) Op welke wijze wordt de regelgeving rondom bescherming persoonsgegevens nageleefd?
7) Heeft de gemeente een overzicht van de privacygevoelige gegevens die zij gebruikt en is duidelijk wie toegang heeft tot deze gegevens?
8) Heeft de gemeente een overzicht van de persoonsgegevens die worden gebruikt door buiten de gemeente geplaatste instellingen en organisaties? Is duidelijk wie toegang heeft tot deze gegevens en waar deze gegevens voor worden gebruikt?
9) Stelt de gemeente eisen aan bijvoorbeeld ICT-systemen en beveiligingsmaatregelen in de eigen organisatie en bij buiten de gemeente geplaatste instellingen en organisaties?
10) Beschikt de gemeente over een functionaris gegevensbescherming zoals bedoeld in de Wet bescherming persoonsgegevens (Wbp)? Heeft deze functionaris ook een rol bij de buiten de gemeente geplaatste instellingen en organisaties?
11) Is er in het privacybeleid van de gemeente aandacht voor welke acties ondernomen moeten worden in het geval zich een datalek voordoet?

Betrokkenen

12) Wordt aan inwoners toestemming gevraagd voor het uitwisselen van hun persoonsgegevens?
13) Hebben inwoners inzicht in de opslag van hun persoonsgegevens en voor welk doel deze zijn opgeslagen?
14) Is geregeld of en hoe inwoners een klacht kunnen indienen tegen opslag van hun gegevens en/of onjuistheden daarin?

Raad

15) Wordt er gerapporteerd aan de raad over privacy en zo ja op welke wijze?

1.3 Werkwijze en indeling rapport

Bij het uitvoeren van dit onderzoek is een aantal stappen doorlopen. De volgende activiteiten zijn uitgevoerd om de onderzoeksvraag te beantwoorden:

a. Bestuderen relevante documenten (zie bijlage);
b. Uitvoeren Interviews (zie bijlage);
c. Nader verkennen van twee praktijkcasus;
d. Uitvoeren convergentiesessie.

De onder a. en b. genoemde activiteiten zijn in onderzoeken gebruikelijk en behoeven geen nadere toelichting. Dat geldt minder voor de activiteiten onder c. en d:

Ad c. Casusbesprekingen
Het onderzoek richt zich in essentie op een inventarisatie en beoordeling van het beleid. In dat kader is van belang geacht om ook nadrukkelijk de uitvoeringspraktijk in het onderzoek te betrekken. Om die reden zijn twee beleidscasus verkend. Het betreft praktijksituaties waarbij sprake is van een relatief intensief gebruik van (mogelijk) privacygevoelige gegevens. Concreet gaat het om de praktijk in het klantcontactcentrum van de gemeente en om de gang van zaken binnen de uitvoering in het sociaal domein (jeugdhulp). Het praktijkonderzoek is uitgevoerd met behulp van de systematiek die PBLQ hanteert voor een ‘privacy impact assessment’. Dit is een methode van onderzoek waarbij de procesgang in de praktijk wordt gereconstrueerd en bij elke stap vervolgens met betrokken uitvoerende medewerkers wordt besproken hoe het waarborgen van de privacy van de ‘cliënten’ is ingericht.

Ad d. Convergentiesessie
Gedurende een onderzoek worden volgtijdelijk meningen, opvattingen en ervaringen van betrokkenen geïnventariseerd. Gaandeweg blijkt soms dat deze meningen en ervaringen van respondenten niet dezelfde zijn of op dezelfde wijze worden ervaren. Om die reden is ter afsluiting van de gegevensverzameling een sessie georganiseerd waar veel van de eerder geraadpleegde personen aanwezig waren. Tijdens die sessie zijn enkele voorlopige bevindingen gepresenteerd en is besproken of de betrokkenen zich daarin konden vinden. Deze activiteit nuanceert en verdiept de bevindingen.

Het feitenonderzoek is uitgevoerd in het voorjaar van 2017.

In dit onderzoek is, conform de verordening bij het functioneren van de rekenkamercommissie, sprake geweest van ambtelijk wederhoor. In afwijking echter van wat gebruikelijk is, heeft het ambtelijk wederhoor niet schriftelijk plaatsgevonden, maar heeft er een gesprek plaatsgevonden tussen medewerkers van de organisatie, de onderzoekers en de rekenkamercommissie. Hiervan is in bijlage verslag gedaan.

1.4 Leeswijzer

In het volgende hoofdstuk worden achtereenvolgens de beleidsdoelstellingen, de uitvoeringspraktijk, de monitoring en de rol van de raad behandeld. Per onderwerp worden de bevindingen beschreven en worden de bij dit onderwerp behorende deelvragen beantwoord. In hoofdstuk 3 zijn de bevindingen in verband gebracht met het in dit onderzoek gehanteerde normenkader. Hoofdstuk 4 bevat de conclusies en aanbevelingen.
In de bijlagen zijn opgenomen: een lijst van gehanteerde afkortingen, een overzicht van de geïnterviewde personen, de geraadpleegde documentatie en de georganiseerde bijeenkomsten. Tevens is in bijlage verslag gedaan van twee praktijkcasussen.
Ook het door de gemeente gehanteerde afwegingskader bij het borgen van de privacy in het sociaal domein als bijlage opgenomen.
In een laatste bijlage is het verslag opgenomen van het gesprek dat in het kader van het ambtelijk wederhoor heeft plaatsgevonden.

2. De balans opgemaakt

In dit hoofdstuk worden de onderzoeksvragen over de beleidsdoelstellingen, de uitvoeringspraktijk, de monitoring en de rol van de raad beantwoord. Per vraag wordt eerst de context en algemene bevindingen vanuit de documentstudie en interviews geschetst. Dit biedt het kader om tot een concrete beantwoording van de onderzoeksvragen te komen.

2.1 Beleid

2.1.1 Context en bevindingen

Bij aanvang van het rekenkameronderzoek beschikte de gemeente Doetinchem nog niet over een algemeen privacybeleidskader. Tijdens de onderzoeksperiode is het privacybeleidskader van de gemeente door het college vastgesteld en heeft de gemeenteraad op 12 april 2017 hiermee ingestemd.
Een belangrijke overweging om tot een gemeentelijk beleidskader te komen, was het feit dat er na de decentralisaties in het sociaal domein meer gevoelige persoonsgegevens in de organisatie aanwezig zijn en worden gedeeld. Weliswaar hebben zich geen grote privacyincidenten voorgedaan, maar ervaringen bij andere gemeenten maken duidelijk dat een privacybeleidskader kan helpen om het thema nog serieuzer op de agenda te zetten en om de bescherming van persoonsgegevens binnen de organisatie te borgen.
Met de constatering dat er voorheen geen privacybeleidskader beschikbaar was, is niet gezegd dat een zorgvuldige omgang met persoonsgegevens geen aandacht binnen de gemeente had. Er waren al stappen gezet. Ook waren voor Wmo en Jeugdzorg al richtlijnen en instructies opgesteld. Daarnaast is er al langere tijd sprake van richtlijnen voor gebruik en verstrekking van gegevens uit de Basisregistratie Personen.

2.1.2 Welk beleid?

In deze subparagraaf staat de beantwoording op de vraag centraal**:**

Vraag 1: Welk beleid is er geformuleerd rond de privacy van gegevens van de inwoners?

In deze subparagraaf is een beschrijving op hoofdlijnen van het privacybeleidskader opgenomen. Deze beschrijving vindt plaats aan de hand van thema's die onderdeel uitmaken van het toetsingskader. Per thema volgt een korte beschrijving van hetgeen hierover in het beleidskader is opgenomen. Vervolgens zijn onze bevindingen weergegeven. Voor een volledig beeld wordt verwezen naar het privacybeleidskader dat door de raad is vastgesteld.[1]

Generiek vs. specifiek
Het privacybeleidskader is een generiek kader dat richting en invulling geeft aan de manier waarop de gemeente met persoonsgegevens omgaat. Het sluit daarmee aan op de Wet bescherming persoonsgegevens (Wbp), maar geeft daar op sommige punten een verdieping of gemeentelijke invulling aan. Daarbij geeft het beleidskader aan dat er themabeleid moet komen op verschillende deelterreinen.

[1] http://besluitvorming.doetinchem.nl/Documenten/raadsbesluiten/Raadsbesluit-12-april-2017-Privacybeleidskader-gemeente-Doetinchem-2017-16.pdf

Het privacybeleidskader heeft daarmee een algemeen karakter.
Het beleidskader besteedt uitgebreid aandacht aan twee belangrijke aspecten: inhoud en proces. Enerzijds bevat het privacybeleidskader belangrijke juridische uitgangspunten en verplichtingen waar de gemeente zich aan dient te houden. Dat betreft het vereiste van een grondslag voor verwerking en het feit dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Anderzijds bevat het beleidskader een aanzet voor het invoeren van een zogenaamde 'Plan-do-check-act cyclus (PDCA-cyclus)' op het gebied van privacy. In het beleid worden actoren genoemd die verantwoordelijk zijn voor de uitvoering van het beleid. Tevens wordt voorgeschreven dat er processen ingericht moeten worden om de effectiviteit en doeltreffendheid van het beleid te evalueren.
Deze cyclus is nog niet volledig ingericht. Zo wordt er in het beleidskader gesteld dat de gemeente proactief privacybeleid op basis van dit privacybeleidskader voert. Hoe hier invulling aan wordt gegeven, is onduidelijk. Ook zijn sommige onderdelen van het beleid nog niet uitgewerkt, zoals het feit dat er themabeleid moet komen op de verschillende deelterreinen. Dit themabeleid is er al wel voor het sociaal domein en (voor een deel) voor de Basisregistratie personen. Op andere terreinen, zoals belastingheffing, subsidieverstrekking of vergunningen, toezicht en handhaving ontbreekt dit nog.

Organisatie, taken en verantwoordelijkheden
In het privacybeleidskader staat onder meer het volgende:
Het college van de gemeente is verantwoordelijk voor de naleving van privacywetgeving en handelt in dat kader proactief op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens zodat deze evenwichtig plaatsvindt. (….) Het college legt over de uitvoering van het privacybeleid periodiek verantwoording af aan de raad en betracht beleidstransparantie met behulp van publieksvoorlichting. (….) De algemeen directeur is verantwoordelijk dat de uitoefening van gemeentelijke taken binnen de grenzen van dit privacybeleidskader plaatsvindt. Afdelingshoofden geven hier invulling aan.

Hiermee zijn de taken en verantwoordelijkheden met betrekking tot de uitvoering van het privacybeleidskader, alsmede de verantwoording hierover, op papier belegd. Een heldere en duidelijke uitwerking van deze taken en verantwoordelijkheden is een belangrijk vereiste voor de bescherming van persoonsgegevens. Echter, bovenstaande passage bevat ook elementen waarvan op het eerste gezicht niet direct duidelijk is, hoe hier in de praktijk uitvoering aan wordt gegeven. Hoe wordt in de praktijk invulling gegeven aan beleidstransparantie door publieksvoorlichting, aan proactief handelingen op basis van afweging van belangen en risico's en hoe geven afdelingshoofden invulling aan de uitoefening van gemeentelijke taken binnen dit privacybeleidskader? Tijdens het onderzoek is duidelijk geworden dat de PDCA-cyclus nog niet op alle onderdelen volledig is uitgewerkt.

Juridische aspecten
In het privacybeleidskader staat wat dit betreft het volgende: *Proceseigenaren verwerken persoonsgegevens uitsluitend op basis van een wettelijke grondslag en zorgen ervoor dat persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (doelbinding). Proceseigenaren houden zich ook aan de beginselen van proportionaliteit[2] en subsidiariteit[3]. (….)*
Een proceseigenaar voert de regie over de verwerking van persoonsgegevens waar hij verantwoordelijk voor is. In dat kader kan hij zijn proces(sen), gegevensopslag en eventueel

[2] Proportionaliteit: de inperking of inbreuk op privacy moet in verhouding staan tot het daarmee te bereiken doel.
[3] Als er verschillende manieren zijn om een doel te realiseren, geniet het minst bezwarende middel de voorkeur.

gegevensuitwisseling onderwerpen aan een privacy impact assessment. Door middel hiervan wordt de impact van privacyschendingen voor de organisatie en betrokkene geanalyseerd.

In het privacybeleidskader is duidelijk opgenomen dat proceseigenaren zich aan de belangrijkste juridische verplichtingen en uitgangspunten dienen te houden. Zij mogen enkel handelen op basis van een grondslag, mogen niet meer gegevens verwerken dan dat noodzakelijk is en dienen zich te houden aan de beginselen van proportionaliteit en subsidiariteit. Dit is in lijn met wat de Wbp vereist.

Informatiesystemen en ICT
In het privacybeleidskader is het volgende opgenomen over informatiesystemen en ICT: *Het privacybeleid ondersteunt het informatiebeveiligingsbeleid (gebaseerd op de Baseline Informatiebeveiliging Gemeenten) door de nadrukkelijke aandacht voor het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de gemeentelijke informatievoorzieningen en opgeslagen persoonsgegevens. Het college draagt zorg voor privacybestendige informatievoorzieningen en gegevensopslag. Proceseigenaren dragen hieraan bij. Informatiebeveiliging wordt uitgevoerd vanuit het Informatiebeveiligingsbeleid Doetinchem 2015-2019.*

In het privacybeleidskader wordt nadrukkelijk aansluiting gezocht bij reeds bestaande informatiebeveiligingsbeleid. Hoe zich dit naar de praktijk vertaalt, wordt uit het kader niet duidelijk. Hetzelfde geldt voor de privacybestendige informatievoorzieningen en gegevensopslag.

Gegevens- en informatiestromen
In het privacybeleidskader staat onder meer het volgende: *In een aantal gevallen is de gemeente wettelijk verplicht verwerkingen met persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. De privacybeheerder houdt hiertoe een privacyregister bij. Dit is een inventarisatie van alle verwerkingen met persoonsgegevens binnen de gemeente. Om het privacyregister actueel te houden geven proceseigenaren mutaties door aan de privacybeheerder.*

Zowel de Wbp als de AVG vereisen van organisaties die persoonsgegevens verwerken, dat zij deze verwerkingen in kaart brengen en hiervan een register bij te houden. De gemeente beschikt over een dergelijk register.

Rechten van inwoners
In het privacybeleid is een hoofdstuk opgenomen over de rechten van inwoners. Volgens het kader hebben de inwoners van de gemeente er recht op dat:
- *de gemeente binnen deze privacybeleidskaders opereert;*
- *de gemeente informatie verschaft over de doelen van informatieverwerking en privacybeleidsvoering;*
- *zij inzage in hun eigen gegevens hebben;*
- *zij – in geval van fouten – hun gegevens kunnen (laten) verbeteren of verwijderen;*
- *zij tegen het gebruik van hun gegevens verzet kunnen aan tekenen hetgeen tot gevolg heeft dat de gemeente verplicht is tot het maken van een afweging;*
- *zij de gemeente bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.*

Onder de Wbp hebben betrokken inwoners bepaalde rechten. Deze rechten worden met de komst van de AVG verder uitgebreid. Het is goed om te zien dat hier met een paragraaf in het

privacybeleidskader duidelijk aandacht aan wordt besteed. Onze bevindingen ten aanzien van dit thema zullen verder worden beschreven bij de vragen 12, 13 en 14.

2.1.3 De beleidsdoelen

In deze subparagraaf wordt ingegaan op de gestelde doelen, gebaseerd op de volgende onderzoeksvraag:

Vraag 2: Wat zijn de doelen van dit beleid?

In het onderzoek is naar voren gekomen dat de doelen van het beleid zijn om te waarborgen dat de gemeente de privacywetgeving naleeft zodat er sprake is van een behoorlijke en zorgvuldige verwerking van persoonsgegevens. Het privacybeleidskader bevat een duidelijk doel en visie op gegevensverwerking. Dit heeft geleid tot de formulering van een aantal kernpunten:

1. Zorg voor privacy is een managementverantwoordelijkheid;
2. Het college voorziet in een team van professionals dat het college en de proceseigenaren ondersteunt in de privacybeleidsvoering;
3. Het college voorziet in faciliteiten voor bewustwording en training;
4. De gemeente hanteert een systeem voor privacy-incidentmanagement;
5. De gemeente evalueert met een zekere regelmaat de doeltreffendheid en de doelmatigheid van dit privacybeleidskader;
6. Het college informeert de raad periodiek over de privacybeleidsvoering;
7. Het college handhaaft het privacybeleid.

In het beleid staat ook dat de gemeente proactief handelt op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens zodat deze evenwichtig plaatsvindt. De gemeente is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden:

- voert de gemeente proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteert gemeente de uitoefening van rechten van haar inwoners;
- bewaakt de gemeente de nakoming van wet- en regelgeving op het gebied van privacybescherming.

Personen waaronder inwoners hebben er recht op dat zij tegen het gebruik van hun gegevens verzet kunnen aan tekenen hetgeen tot gevolg heeft dat de Gemeente Doetinchem verplicht is tot het maken van een afweging.

Een aantal kernpunten is in de praktijk terug te zien bij de jaarlijkse kennistest over gegevensbescherming en informatiebeveiliging. Dit illustreert dat er aan bewustwording en training wordt gedaan. Een aantal andere kernpunten is minder ver uitgewerkt. Het college 'voorziet' dan wel in een team, maar welke garantie is er dat dit team er komt, wie zitten erin en op welke termijn is het er? Hetzelfde geldt voor een periodieke evaluatie van de doeltreffendheid en de doelmatigheid van het systeem. In het kader van de PDCA-cyclus behoeven dergelijke kernpunten verdere uitwerking. Over het faciliteren van de uitoefening in de rechten van de inwoners van de gemeente, wordt aandacht besteed onder de vragen 12, 13 en 14.

2.1.4 Aansluiting bij wet- en regelgeving

In deze subparagraaf wordt de onderzoeksvraag behandeld

Vraag 3: Voldoet dit beleid aan de wet- en regelgeving?

In het algemeen kan worden gesteld dat het beleid momenteel voldoet aan de geldende landelijke wet- en regelgeving. In het privacybeleidskader zijn veel verplichtingen en beginselen voor de verwerking van persoonsgegevens terug te zien. Zo mogen persoonsgegevens enkel worden verwerkt als er sprake is van een wettelijke grondslag, doelbinding en de beginselen van proportionaliteit en subsidiariteit. Bepaalde handelingen die in strijd zijn met deze en andere privacybeginselen, zijn volgens het privacybeleidskader verboden.

Voor bepaalde beleidsvelden geldt dat, zover van toepassing, proceseigenaren tevens rekening moeten houden met bijzondere wettelijke voorschriften.

De AVG vertoont sterke overeenkomsten met de Wbp, maar bevat enkele aanvullende verplichtingen. Bij de beantwoording vraag 4 zal hier verder op worden ingegaan.

2.1.5 Voorbereiding op de AVG

De volgende onderzoeksvraag heeft betrekking op de voorbereidingen door de gemeente gericht op inwerkingtreding van de nieuwe Europese regelgeving, de AVG:

Vraag 4: Welke maatregelen neemt de gemeente om (tijdig) voorbereid te zijn op de komst van de nieuwe, scherpere privacyregelgeving (AVG)?

Op 25 mei 2018 zal de AVG in werking treden. Grote wijzingen ten opzichte van de Wbp zijn het verplicht aanstellen van een functionaris gegevensbescherming (FG) voor overheidsorganisaties, meer rechten voor betrokkenen en een meer uitgebreide verantwoordingsplicht (in het kader van accountability). Organisaties die persoonsgegevens verwerken moeten kunnen aantonen dat zij zich aan de privacywetgeving houden.

De Autoriteit Persoonsgegevens (AP) heeft tien stappen gepubliceerd waarmee organisaties zich kunnen voorbereiden op de AVG[4]. Op een aantal onderwerpen zet de gemeente al stappen, maar die zijn nu nog niet specifiek gericht op de komst van de AVG.
Uit gesprekken is gebleken dat de gemeente het voornemen heeft om samen met enkele regiogemeenten een FG aan te stellen. Een besluit hierover is nog niet genomen.
De AVG vereist dat organisaties zich niet alleen aan alle beginselen inzake de verwerking van persoonsgegevens houden, maar dit ook kan aantonen (accountability).[5] Organisaties die persoonsgegevens verwerken hebben dus een verantwoordingsplicht.
Binnen de gemeente is onduidelijk in hoeverre er aantoonbare documentatie aanwezig is waaruit blijkt dat de organisatie zich aan het privacybeleid houdt. Wel wordt in het privacybeleidskader gesproken over het uitvoeren van Privacy Impact Assessments (PIA). Een PIA draagt tevens bij aan accountability en wordt toegepast bij nieuw beleid en regelgeving of de invoering van nieuwe systemen.

[4] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/voorbereiding-op-de-avg
[5] Art. 5 lid 2 Avg.

De AVG gaat tevens gepaard met een versterking van een aantal bestaande rechten van betrokkenen (zoals toestemming) en een aantal nieuwe rechten, zoals dataportabiliteit (overdraagbaarheid van persoonsgegevens). Een andere verplichting is het bijhouden van een register van verwerkingen. Dit vraagt aanpassing van het bestaande privacyregister dat de gemeente nu al bijhoudt.

2.2 Uitvoering

2.2.1 Context en bevindingen

Het privacybeleidskader geeft aan op welke wijze de privacybescherming van inwoners moet worden geborgd. Het kader heeft een kapstokfunctie: het schrijft voor aan welke regels de gemeente zich dient te houden en hoe het privacybeleid moet worden uitgevoerd. Bij de uitvoering van het beleid zal in de volgende paragrafen worden stilgestaan.
Belangrijk uitgangspunt is dat de verantwoordelijkheid voor het nemen van maatregelen ter bescherming van de privacy gekoppeld is aan specifieke functionarissen binnen de organisatie (afdelingshoofden). Deze verantwoordelijkheden zijn weliswaar belegd, maar tijdens het onderzoek is niet vastgesteld of deze daadwerkelijk in de praktijk worden ingevuld. Met het toenemend belang van accountability in het kader van de AVG, is dit een aandachtspunt.

Een ander kernpunt van het privacybeleidskader is om met een zekere regelmaat de doeltreffendheid en doelmatigheid van het kader te evalueren. Op kleine schaal is hiervan sprake. Dit blijkt met name uit het vergelijken van de uitkomsten van de jaarlijkse privacytoets onder medewerkers. Op grotere schaal, in het kader van de PDCA-cyclus, moet dit nog verder worden uitgewerkt.

Op specifieke activiteiten of verwerkingen rondom bepaalde thema's zoomt het privacybeleidskader niet in. Voor zover dit speelt wordt via themabeleid en procesplannen nadere invulling aan het privacybeleidskader gegeven. Veel van de in het beleidskader aangekondigde procesplannen is nog geen sprake, met uitzondering voor het sociaal domein. Wel onderschrijft de aanwezigheid van het beleidskader de bevinding dat het thema privacybescherming leeft in de gemeente. Er is al veel aandacht besteed aan bewustwording en training.

Onder andere in het kader van de decentralisaties, heeft de gemeente een aantal uitvoerende (wettelijke) taken ondergebracht bij organisaties buiten de gemeente. Het privacybeleidskader is ook van toepassing op processen die de gemeente uitbesteedt, inkoopt of op een andere manier organiseert. Dat impliceert dat de gemeente voor wat betreft de verwerking van gegevens in het kader van de uitvoering van gemeentelijke taken kan worden aangemerkt als verantwoordelijke in de zin van de Wbp. De gemeente moet zorgen dat deze gegevens ook op rechtmatige en behoorlijke wijze worden verwerkt. De gemeente is hiervoor primair verantwoordelijk. Indien hiervan sprake is en de andere organisatie als bewerker (verwerker in de AVG) moet worden aangemerkt, moet een bewerkersovereenkomst worden afgesloten. De gemeente heeft inmiddels met enkele organisaties een dergelijke overeenkomst afgesloten (zie 2.2.3).

De gemeente heeft reeds maatregelen genomen rondom de verwerking van persoonsgegevens door bewerkers/derden. Hiervoor bevat het nieuwe privacybeleidskader een modelbewerkersovereenkomst. Of de overeengekomen maatregelen in bestaande contracten hieraan voldoen, wordt door de gemeente nog onderzocht. Ook vindt er geen duidelijke monitoring of controle plaats op de gegevensverwerking door bewerkers.

Casussen als verdieping van het onderzoek
Om te toetsen of het beleid en de gemaakte afspraken worden nageleefd en om te ervaren hoe er binnen de organisatie over een zorgvuldig gebruik van persoonsgegevens wordt gesproken en gedacht zijn twee casussen in aparte bijeenkomsten besproken:
1. Casus “Klantcontactcentrum”
2. Casus “Jeugdhulp”

Tijdens de bespreking is met direct betrokken gesproken over de manier waarop met persoonsgegevens wordt omgegaan. Voor de casus Jeugdhulp waren ook twee medewerkers van Buurtplein BV aanwezig. De besprekingen zijn gevoerd aan de hand van een aantal specifieke aandachtsvelden. Op basis daarvan is een oordeel gevormd en zijn risico’s benoemd.

Casus Klantcontactcentrum
Het KCC fungeert als frontoffice en handelt zelf eenvoudige vragen en meldingen af. Tegelijkertijd dient het KCC zoveel mogelijk gegevens te op te vragen, zodat de backoffice dat bij de afhandeling niet hoeft te doen. Hier is sprake van een spanning waar de medewerkers van het KCC zich zeer bewust van zijn. Daarom is er veel aandacht voor privacybescherming binnen het KCC. Nieuwe ‘gevallen’ en incidenten worden onderling besproken (awareness), er zijn werkinstructies (informatie moet ‘need to have’ in plaats van ‘nice to know’ zijn; gegevens mogen niet zomaar worden verstrekt zonder dat er identificatie en authenticatie heeft plaatsgevonden) en de KCC-medewerkers hebben slechts toegang tot de informatie in informatiesystemen die zij echt nodig hebben. Bovendien worden hun handelingen gelogd en vindt er monitoring plaats.

Casus Jeugdhulp
De uitvoering van de jeugdzorg is in Doetinchem zowel belegd bij de gemeente als bij de bij BV opgerichte uitvoeringsorganisatie Buurtplein. Bij het Buurtplein zijn de wijkteams en de jeugdcoaches ondergebracht. Signalen van mogelijke problemen met jeugdigen in de gemeente kunnen door veel verschillende mensen worden gegeven. Een deel van de meldingen leidt tot een concrete ondersteuningsvraag. De ondersteuningsvraag moet uiteindelijk door een jeugdconsulent van de gemeente worden beoordeeld, die voor de beslissing over een onderbouwd voorstel (gezinsplan) moet kunnen beschikken. De uitvoering wordt belegd bij Buurtplein of gespecialiseerde organisaties, waarbij natuurlijk ook weer overdracht van informatie plaatsvindt. Als uitvoeringsorganisatie van de gemeente zijn de regels en afspraken waar het Buurtplein zich aan dient te houden vastgelegd in de opdrachtgevers/opdrachtnemers-overeenkomst (OGON). Dat betreft ook privacy.

Binnen de gemeente is er aandacht voor doelbinding, autorisaties en veilige gegevensoverdracht doelbinding. Voor taken die buiten de gemeente zijn belegd maar waarvoor de gemeente wel een verantwoordelijkheid heeft, lijkt dit minder goed geregeld. Binnen het Buurtplein wordt deze aandacht momenteel gestimuleerd, maar moet het bewustzijn zeker nog toenemen. Ook de gemeente zal stappen moeten ondernemen, in lijn met haar verantwoordelijkheid, om ervoor te zorgen dat deze gegevens buiten de gemeente rechtmatig en behoorlijk worden verwerkt.

Zie bijlage E. voor de nadere uitwerkingen van de casusbesprekingen

2.2.2 Bescherming persoonsgegevens

De volgende vraag heeft betrekking op de wijze waarop de bescherming van persoonsgegevens is ingericht.

Vraag 5: Hoe is de bescherming van persoonsgegevens vormgegeven?

De verantwoordelijkheid voor het privacybeleid en het treffen van passende maatregelen ter bescherming van de privacy zijn conform het beleidskader belegd bij het college van B&W. De verantwoordelijkheid voor de uitvoering van de taken die hieruit voortvloeien ligt bij de afdelingshoofden, waarbij de gemeentesecretaris eindverantwoordelijk is.
Een aantal medewerkers heeft adviserende of controlerende taken gekregen. In dit kader is de *Chief Information Security Officer* (CISO)-rol van belang. Deze is belegd bij het hoofd services en bij de functie van informatiebeveiligings-coördinator/ privacybeheerder. De functie vervult een belangrijke aanjagende, faciliterende en controlerende rol als het gaat om het bewaken van de privacy. Echter deze functie heeft nu niet de bevoegdheden van een Functionaris Gegevensbescherming conform de AVG. Binnen de afdelingen zijn kwaliteitsmedewerkers medeverantwoordelijk voor maatregelen gericht op een zorgvuldige verwerking van persoonsgegevens.

In het privacybeleid wordt geen specifieke aandacht besteed aan specifieke activiteiten of verwerkingen rondom bepaalde thema's. Voor zover dit speelt moet dit via themabeleid en procesplannen nader worden ingevuld. Voor het sociaal domein is dit al gebeurd.

Zoals al aan de orde kwam, is het privacybeleidskader een algemeen kader, dat nog uitwerking nodig heeft. Onderwerpen die uitwerking vragen zijn onder meer:

- Taken en verantwoordelijken zijn in het beleidskader toebedeeld, maar voeren proceseigenaren daadwerkelijk de regie over de gegevens die zij verwerken? En in welke mate houden zij zich aan het privacybeleidskader?
- Welke afspraken zijn er gemaakt in een bewerkersovereenkomst of anderszins met partijen die in opdracht van de gemeenten persoonsgegevens verwerken? En kan de gemeente aantoonbaar maken dat deze partijen zich ook aan het privacybeleidskader houden?
- Concrete afspraken met betrekking tot transparantie en accountability, die met de komst van de AVG steeds belangrijker worden.

2.2.3 Naleving bescherming persoonsgegevens

Bij de bescherming van persoonsgegevens gaat het niet alleen om het beschreven beleid. Eveneens is relevant hoe dit beleid in de praktijk vorm wordt gegeven. Dit leidt tot de onderzoeksvraag:

Vraag 6. Op welke wijze wordt de regelgeving rondom bescherming persoonsgegevens nageleefd?

Controle op de naleving gebeurt op een aantal manieren. Enerzijds heeft de privacybeheerder de bevoegdheid om steekproeven te nemen om het gebruik van gegevens in systemen te controleren (bijvoorbeeld op basis van logfiles). Dergelijke steekproeven worden in de huidige praktijk ook uitgevoerd. Daarnaast wordt jaarlijks de kennistoets informatiebeveiliging georganiseerd, waar ook het gebruik van persoonsgegevens een element is. Deze toets is verplicht voor alle medewerkers. Er kunnen door de gemeentesecretaris maatregelen worden genomen bij het niet halen van of deelnemen aan de toets, maar daar is nog geen concrete aanleiding voor geweest.

Anderzijds vindt de controle op de naleving plaats binnen de afdelingen. De gemeente hecht aan onderling vertrouwen en elkaar aanspreken. Er wordt van medewerkers verwacht dat zij elkaar corrigeren als er te gemakkelijk met de privacy van inwoners wordt omgegaan.
Binnen het sociaal domein (Buurtplein) vindt dossiercontrole achteraf plaats.

Voor externe partijen die gemeentelijke taken uitvoeren en in het kader van die taak persoonsgegevens verwerken, vindt geen duidelijke monitoring of controle plaats door de gemeente. Uit de interviews blijkt dat gemeentelijke medewerkers nog geen antwoord hebben op de vraag wat hun verantwoordelijkheid is richting externe partijen als het gaat om de verwerking van persoonsgegevens. Voor zover in het onderzoek naar voren is gekomen, wordt hier niet op gestuurd. Evenmin vindt het gesprek daarover plaats.

Derden	Documentatie
Buha BV	bewerkersovereenkomst
Buurtplein	convenant
Laborijn	convenant
ODA	*Bewerkersovereenkomst in ontwikkeling*
Stichting inlichtingenbureau	bewerkersovereenkomst
Sité woondiensten	convenant (*wordt dit jaar vervangen door bewerkerso.k.)*
Veiligheidsregio	Gemeenschappelijke Regeling overeenkomst
Jeugdbescherming Gelderland	bewerkersovereenkomst

Met name daar waar (bijzondere) persoonsgegevens door externe partijen worden verwerkt in het kader van Wmo, Participatiewet en Jeugdzorg is er onzekerheid of onduidelijk hoe ver de gemeentelijke verantwoordelijkheid reikt.
Vanuit een strikt juridische invalshoek is dan de vraag relevant of deze partijen ‘verantwoordelijke’ of ‘verwerker’ in het kader van de privacywetgeving zijn. Is sprake van een externe partij als verwerker, dan is een bewerkersovereenkomst noodzakelijk. De gemeente heeft niet met alle externe partijen een bewerkersovereenkomst afgesloten, of op een andere wijze vastgelegd wat van andere partijen wordt verwacht. Dat laatste kan namelijk ook benaderd worden vanuit een meer algemeen besef dat de bescherming van de privacy op orde moet zijn bij organisaties die namens of voor de gemeente taken uitvoeren. Hierbij speelt dan dat (ook) de gemeente aangesproken zal worden als deze externe partijen de privacy niet op orde hebben, datalekken optreden, of de AP boetes uitdeelt. In de huidige situatie wordt niet altijd ervaren dat de gemeente zich verantwoordelijk voelt voor zorgvuldige gegevensverwerking door derden die namens de gemeente taken uitvoeren.

Om de effectiviteit van het privacybeleidskader vast te stellen en om deze constant te verbeteren, dient gestructureerde, periodieke evaluatie van het beleid plaats te vinden om het beleid bij te sturen of te corrigeren. In hoeverre er in de praktijk periodieke evaluatie van het beleid en de getroffen maatregelen plaatsvindt, is onduidelijk. In het kader van de PDCA-cyclus (in het bijzonder de check en act) moet dit nog verder worden uitgewerkt. Dit geldt ook voor verwerkers of derden die gegevens in opdracht van de gemeente verwerken.

2.2.4 Overzicht van en toegang tot privacygevoelige gegevens

In deze subparagraaf gaat het om de onderzoeksvraag:

Vraag 7: Heeft de gemeente een overzicht van de privacygevoelige gegevens die zij gebruikt en is duidelijk wie toegang heeft tot deze gegevens?

In het algemeen is voor het gebruik van specifieke applicaties een autorisatie-overzicht aanwezig. Voor medewerkers is bepaald welke functionaliteit en gegevens zij voor de uitvoering van hun werkzaamheden nodig hebben. Afhankelijk van de rol die zij vervullen, zijn autorisaties toegekend. Beleid (Het beleid Logische toegangsbeveiliging) is hiervoor al opgesteld, maar nog niet formeel door het management of het college van B&W vastgesteld.

Voor de uitvoering van werkprocessen in het sociaal domein, (met name Wmo en Jeugdzorg) voor het gebruik van Suwinet, en voor het beheer van de Basisregistratie Personen zijn processen gedocumenteerd. Voor andere processen zijn geen uitwerkingen aangetroffen.

2.2.5 Privacygevoelige gegevens in samenwerking met externe partijen

Er is niet alleen binnen de gemeentelijke organisatie sprake van privacygevoelige gegevens. Ook in samenwerking met externe partijen zijn dergelijke gegevens aan de orde.

Vraag 8: Heeft de gemeente een overzicht van de persoonsgegevens die worden gebruikt door buiten de gemeente geplaatste instellingen en organisaties? Is duidelijk wie toegang heeft tot deze gegevens en waar deze gegevens voor worden gebruikt?

De gemeente heeft een privacyregister waarin alle geautomatiseerde gegevensverwerkingen zijn gedocumenteerd. De verwerkingen zijn, tenzij vrijgesteld, ook gemeld aan de Autoriteit Persoonsgegevens en openbaar toegankelijk. Daar is tevens bij vermeld aan wie de gegevens worden verstrekt (zie voorbeeld hiernaast).

Uit de casus jeugdzorg kwam naar voren dat verantwoordelijkheden en autorisaties binnen de op afstand geplaatste organisaties ten behoeve van het sociaal domein soms worden gedeeld. Tegelijkertijd heeft de gemeente geen procedures of instrumenten om te controleren hoe binnen deze organisaties met persoonsgegevens wordt omgegaan.

Burgemeester van Doetinchem

Meldingsnummer	1533139
Naam verwerking	Uitvoering Wet Bijzondere Opname Psychiatrische Ziekenhuisen (Wet BOPZ)
Verantwoordelijke(n)	Naam Burgemeester van Doetinchem Bezoekadres Raadhuisstraat 2 7001EW DOETINCHEM NEDERLAND Postadres Postbus 9020 7000HA DOETINCHEM NEDERLAND
Doel(en) van verwerking	Administratieve afhandeling van een onvrijwillige opname in het kader van de Wet BOPZ
Betrokkene(n)	
Degene die de onvrijwillige opname moet ondergaan	Persoonsgegevens Omschrijving NAW gegevens, bevindingen psychiater Verzameldoel Identificatie en besluitvorming Omschrijving NAW van directe familie Verzameldoel Communicatie met familie over opname Bijzondere Gegevens betreffende de persoonsgegevens gezondheid
Ontvanger(s)	Geneeskundig inspecteur voor de Geestelijke Gezondheidszorg
	Officier van Justitie te Zutphen
	Wettelijk vertegenwoordiger van de in bewaring gestelde persoon
	Hoofd Arrondissementsparket
Doorgifte buiten EU	N
Doorgifte passend	

2.2.6 Systeemeisen en beveiligingsmaatregelen

In de subparagraaf staat onderzoeksvraag centraal:

Vraag 9: Stelt de gemeente eisen aan bijvoorbeeld ICT-systemen en beveiligingsmaatregelen in de eigen organisatie en bij buiten de gemeente geplaatste instellingen en organisaties?

Voor de gemeentelijke ICT is de Baseline Informatiebeveiliging Gemeenten (BIG) van toepassing. Alle gemeenten hebben zich in 2013 gecommitteerd om de BIG in te voeren. Daarbij heeft de gemeente een beveiligingsbeleid voor de periode 2015-2019 opgesteld[6]. Dit bevat algemene beleidsuitgangspunten over informatiebeveiliging. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. Op basis van dit beveiligingsbeleid kan de gemeente verdere in- en aanvulling geven aan de informatiebeveiliging. In het kader van dit onderzoek is inzage gegeven in het beveiligingsplan dat als doel heeft de maatregelen te implementeren. Hieruit blijkt hoe de gemeente met geconstateerde risico's omgaat en welke (rest-)risico's men accepteert. Het beveiligingsplan wordt jaarlijks geactualiseerd en door het college vastgesteld.

De uitgangspunten voor informatiebeveiliging zijn ook van toepassing op externe partijen. In het beleidsplan wordt gesteld: *De scope van dit beleid omvat alle gemeentelijke processen, onderliggende Informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.*

Tijdens het onderzoek is niet gebleken dat de gemeente het beveiligings- en privacybeleid direct bespreekt met externe partijen of hier specifiek invloed op uitoefent. Er worden geen eisen gesteld aan de ICT van externe partijen.

2.2.7 De functionaris gegevensbescherming

Voor het geven van invulling aan gegevensbescherming is het nuttig als deze verantwoordelijkheid belegd is bij een aanwijsbare persoon. De vraag luidt:

Vraag 10: Beschikt de gemeente over een functionaris gegevensbescherming zoals bedoeld in de Wbp? Heeft deze functionaris ook een rol bij de buiten de gemeente geplaatste instellingen en organisaties?

Vanaf 25 mei 2018, de datum waarop de AVG van kracht wordt, is het voor gemeenten verplicht een functionaris voor de gegevensverwerking (FG) te hebben. Belangrijk aan de FG is echter dat deze een onafhankelijke positie in de organisatie moet hebben[7]. De gemeente kent deze functionaris nog niet. Een aantal taken die straks onder de verantwoordelijkheid van de FG vallen worden nu al in meer of mindere mate uitgevoerd door de informatiebeveiligings-coördinator en privacybeheerder. Deze heeft geen formele taak of bevoegdheid in relatie tot externe partijen.

[6] In dit onderzoek is niet gekeken in hoeverre het beveiligingsbeleid voldoet aan de BIG

[7] Richtlijnen voor de FG zijn hier te vinden: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243_rev01_enpdf_0.pdf

2.2.8 Over datalekken

Datalekken krijgen volop de aandacht in de pers. Het is van belang dat de gemeente zich hier op voorbereidt.

Vraag 11: Is er in het privacybeleid van de gemeente aandacht voor welke acties ondernomen moeten worden in het geval zich een datalek voordoet?

Het privacybeleidskader bevat een regeling privacyincidenten: *De procedure bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorzieningen en gegevensopslag aantasten.*
Als uitwerking daarvan beschikt de gemeente over een “Handleiding melden datalek”. Deze bevat interne richtlijnen voor het melden van het datalek bij de Autoriteit Persoonsgegevens (AP), de rol van de privacybeheerder en de verantwoordelijkheid van het afdelingshoofd.

Daarnaast houdt de gemeente een register bij van opgetreden datalekken, waarbij naast de oorzaak van het incident ook is gedocumenteerd wat wordt gedaan om soortgelijke datalekken in de toekomst te voorkomen. Het privacyregister, dat sinds 2016 wordt bijgehouden, bevat nu vier gedocumenteerde incidenten. Het betrof hier menselijke fouten die gemeld zijn aan de AP. Uit interviews is gebleken dat de gemeente bij een datalek een onderzoek doet naar de oorzaak en maatregelen treft om herhaling te voorkomen.

2.3 De rechten van inwoners

In deze paragraaf zijn drie onderzoeksvragen aan de orde, die alle te maken hebben met de positie van de inwoners.

Vraag 12: Wordt aan inwoners toestemming gevraagd voor het uitwisselen van hun persoonsgegevens?

Een belangrijk juridisch uitgangspunt met betrekking tot privacy is dat de gemeente een grondslag moet hebben voor de verwerking van persoonsgegevens. In het privacybeleidskader wordt dit belang onderschreven.
Een gemeente zal voornamelijk persoonsgegevens verwerken voor publieke taken die bij of krachtens de wet aan haar zijn overgedragen.
De bepaling van de grondslagen voor de verwerking van persoonsgegevens bij de uitvoering van taken in het sociaal domein is echter vaak complex. Dat komt omdat hier vaak verschillende domeinen en wetten van toepassing zijn.[8] In het sociaal domein zal vaak sprake zijn van onvrije toestemming. Burgers hebben hier een afhankelijkheidsrelatie met de gemeente, waardoor het vragen om toestemming gecompliceerd ligt. Een goed beredeneerde gegevensverzameling en helderheid over de grondslag is dan nodig.
In de Werkinstructie '*Omgaan met privacy'. Kaders voor medewerkers van Buurtplein* dat door de gemeente is opgesteld wordt hier aandacht aan besteed. De gemeente hanteert een stroomschema (aangeduid als 'Zwitsers Zakmes') voor medewerkers om vast te stellen of gegevens mogen worden uitgewisseld (zie bijlage F).
Hoewel de gemeente hier in beginsel zorgvuldig mee om gaat (zie casus Jeugdhulp), gaven de medewerkers in de casusbespreking aan dat het maken van de afweging of gegevens uitgewisseld mogen worden, lastig blijft.

Vraag 13: Hebben inwoners inzicht in de opslag van hun persoonsgegevens en voor welk doel deze zijn opgeslagen?

In het privacybeleidskader wordt expliciet aandacht besteed aan deze en andere rechten van de inwoners (zie beantwoording onderzoeksvraag 4). Inwoners kunnen bij de gemeente een verzoek doen om een overzicht van hun persoonsgegevens die de gemeente heeft geregistreerd en voor welk doel. Een enkele keer wordt zo'n verzoek ook daadwerkelijk gedaan.

Specifiek voor het sociaal domein is er een folder over gegevensverwerking door de gemeente. Deze maakt onderdeel uit van het privacybeleidskader. In de folder wordt voor meer informatie over de privacyrechten verwezen naar de website van de gemeente. Daar levert zoeken via de zoekfunctie echter geen nadere informatie over privacy- of inzagerechten op. De website van de gemeente bevat wel een kort privacystatement. De rechten van de inwoners zijn daarin onvoldoende uitgewerkt en kenbaar gemaakt.

Vraag 14: Is geregeld of en hoe inwoners een klacht kunnen indienen tegen opslag van hun gegevens en/of onjuistheden daarin?

In het privacybeleidskader is opgenomen hoe de gemeente handelt bij vragen en klachten.
Bij schriftelijke of mondelinge vragen:

- *kunnen personen zich wenden tot het Klant Contact Centre (KCC) wat zodanig is ingericht dat vragen daadwerkelijk kunnen worden afgehandeld;*
- *vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld.*

[8] AP, De rol van toestemming in het sociaal domein, 2016, p. 2.

- *Een niet tot tevredenheid afgehandelde vraag geeft personen het recht om zich opnieuw te wenden tot klachtenfunctionaris van de gemeente;*
- *De klacht wordt geregistreerd;*
- *Klachten worden zo snel mogelijk maar uiterlijk binnen tien weken afgehandeld.*

Volgens het privacybeleidskader kunnen inwoners zich met klachten wenden tot het KCC. Echter, volgens de website is er geen aparte klachtenregeling voor privacy. En hoewel de gemeente weliswaar een klachtenregeling kent, wordt nergens duidelijk gemaakt dat deze ook voor privacyklachten is.

Al met al heeft de gemeente als het gaat om de privacyrechten van inwoners niet alleen de nodige goede bedoelingen waarvan er enkele zijn vastgelegd in het beleid, alleen blijkt dat die rechten niet tot nauwelijks op te vragen of in te zien zijn door de betrokkenen zelf.

2.4 Raad

Privacy is een politiek beladen thema, de gemeenteraad hoort hierover geregeld geïnformeerd te worden, zodat het zijn kaderstellende en controlerende rol goed waar kan maken.

Vraag 15: Wordt er gerapporteerd aan de raad over privacy en zo ja op welke wijze?

Er vindt geen structurele verantwoording over privacy (-incidenten) plaats aan de gemeenteraad. Dit jaar is het beleidskader privacy vastgesteld in de raad. In de periode hieraan voorafgaand is een informele sessie georganiseerd voor raadsleden. Enkele raadsleden hebben daar aan deel genomen.

3. Toetsing aan het normenkader

Voor dit onderzoek is gebruik gemaakt van een normenkader. Het normenkader is voorafgaand aan het onderzoek opgesteld door PBLQ en vastgesteld door de Rekenkamercommissie. Het is opgesteld aan de hand van de onderwerpen die centraal staan in dit onderzoek (beleid, uitvoering, monitoring en verantwoording). Het oordeel wordt geformuleerd aan de hand van verwachtingen (de normen) die er zijn ten aanzien van deze onderwerpen. Aangegeven is in welke mate wordt voldaan aan de norm: wel (groen), niet/onvoldoende (rood), of gedeeltelijk/op de goede weg (oranje).

Beleid	Oordeel	
[1] Er is een privacybeleidskader, waarin staat op welke wijze aan de vigerende privacywetgeving wordt voldaan (rechtmatigheid, behoorlijkheid en zorgvuldigheid), hoe privacybescherming organiek is ingebed (inclusief de benodigde middelen en rapporteringslijnen), hoe risico's en passende maatregelen worden vastgesteld en of er sprake is van een PDCA-cyclus, zodat het beleid kan worden bijgestuurd en gecorrigeerd		Belangrijk voor een goed privacybeleidskader zijn inhoud (juridische verplichtingen en uitgangspunten m.b.t. privacybescherming) en proces (het borgen van privacy door taken en verantwoordelijkheden te beleggen en een PDCA-cyclus te volgen. Met de aandacht voor privacymanagement, noodzakelijke gegevensverwerking, gedragsnormen voor proceseigenaren, privacyservices en een privacy-programma, voldoet het beleidskader op papier aan deze normen. Wel heeft het privacybeleidskader een algemeen karakter heeft. Het zoomt niet in op de spelregels die kunnen gelden voor specifieke beleidsterreinen.
[2] In het beleid wordt zowel aandacht besteed aan de rechten van de burger als aan het belang van de gemeente. Tussen deze belangen is bij het formuleren een afweging gemaakt.		In het beleidskader staat dat de gemeente een aantal kernpunten hanteert en proactief handelt op basis van een afweging van belangen en risico's bij de verwerking van persoonsgegevens, zodat deze evenwichtig plaatsvindt. Verder wordt in het beleid noodzakelijke gegevensverwerking als uitgangspunt gehanteerd, dat wil zeggen dat er altijd sprake moet zijn van grondslag, doelbinding, proportionaliteit en subsidiariteit. In de praktijk blijkt echter dat sommige van deze (kern)punten nog verdere uitwerking behoeven.
[3] Het beleid voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld (Generiek aan de Wbp en de AVG en specifiek voor bepaalde beleidsvelden). Hierbij is in het bijzonder gekeken naar de rechtmatigheid, de behoorlijkheid en zorgvuldigheid van de verwerking, alsmede de rechten van betrokkenen.		Veel beginselen inzake gegevensverwerking uit de Wbp en de AVG zijn opgenomen in het privacybeleidskader. Echter, niet aan alle eisen uit de AVG wordt voldaan. Zo heeft de gemeente geen nog FG aangesteld. Ook moet de gemeente aantonen dat zij aan alle wettelijke privacy-verplichtingen voldoet (accountability /verantwoordingsplicht. Ten aanzien van bepaalde beleidsvelden dienen proceseigenaren tevens rekening houden met bijzondere wettelijke voorschriften.
[4] De gemeente is bekend met de komst van nieuwe privacywetgeving (AVG) en bereidt zich er op voor om hieraan tijdig te voldoen		Het is bij de privacybeheerder en andere betrokkenen bekend dat de AVG per 25 mei 2018 van kracht is. Deelgenomen wordt aan voorbereidingsbijeenkomsten die vanuit de VNG worden georganiseerd. Met regiogemeenten wordt gesproken over een gezamenlijke FG. Er is nog geen project- of invoeringsplan als het gaat om de implementatie van de AVG.

Uitvoering	Oordeel	
[5] Bij de bescherming van de persoonsgegevens is aandacht besteed bij de toewijzing van verantwoordelijkheden, in de relevante werkprocessen, bij de inrichting van informatiesystemen en bij de inrichting van de uitwisseling van gegevens.		Taken en verantwoordelijkheden zijn op papier duidelijk belegd. Met betrekking tot informatiesystemen ondersteunt het privacybeleid het informatiebeveiligingsbeleid. Echter, hoe hier in de praktijk invulling aan wordt gegeven, is niet helemaal duidelijk. Rondom bepaalde thema's, zoals het sociaal domein, zijn uitgewerkte procesplannen/werkinstructies. Voor andere thema's zijn deze er echter (nog) niet. Een aantal uitvoerende (wettelijke) taken is ondergebracht bij organisaties buiten de gemeente. De verantwoordelijkheden en verplichtingen van de gemeente en de 'bewerkers' van deze gegevens, zijn voor de betreffende partijen niet altijd even duidelijk. Op papier staat het netjes uitgewerkt, in de praktijk moet nog een en ander worden uitgewerkt.
[6] In de praktijk wordt gehandeld naar de wijze waarop aan bescherming van de persoonsgegevens aandacht is besteed in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen en de inrichting van de uitwisseling van gegevens.		Toezicht op naleving vindt op verschillende wijzen plaats: enerzijds voert de privacybeheerder steekproefsgewijs controles uit, anderzijds geschiedt naleving binnen de afdeling zelf. Of dit voldoende is voor het college om haar bestuurlijke verantwoordelijkheid uit te oefenen, is onduidelijk. Verdere verantwoordingsprocedures en mechanismen ontbreken. Hetzelfde geldt voor afspraken over periodieke toetsing van het uitgevoerde beleid (een kernpunt volgens het privacybeleidskader) en gegevensverwerking buiten de gemeente. Wat dit laatste betreft bestaat er in het sociale domein soms onduidelijkheid over de taken en verantwoordelijkheden van de betrokken partijen. Ook moeten er nog convenanten naar bewerkersovereenkomsten worden omgezet en moet er monitoring en/of controle op de naleving van deze overeenkomsten worden verbeterd.
[7] Binnen de gemeente bestaat een overzicht van de door de gemeente gebruikte privacygevoelige gegevens. Er is vastgelegd wie toegang heeft tot de privacygevoelige gegevens.		Aandachtspunt is het aanpassen van het privacyregister aan de nieuwe eisen vanuit de AVG.
[8] Binnen de gemeente bestaat een overzicht van de persoonsgegevens die worden gebruikt door buiten de gemeente geplaatste instellingen en organisaties. Er is vastgelegd wie toegang heeft tot de privacygevoelige gegevens en waar deze voor worden gebruikt.		Binnen de gemeente bestaat weliswaar een dergelijk overzicht, maar periodiek toezicht en controle op wie er binnen de buiten de gemeente geplaatste instellingen en organisaties in het sociaal domein daadwerkelijk toegang heeft tot deze gegevens in het sociale domein, ontbreekt.
[9] De gemeente heeft eisen gesteld aan en beveiligingsmaatregelen geformuleerd ten aanzien van de ICT-systemen waarin persoonsgegevens worden gebruikt.		Binnen de gemeente wordt de BIG en de NCSC-normen gehanteerd. Van bewerkers (ketenpartners) is niet bekend of de wettelijke verplichtingen ten aanzien van beveiliging worden nageleefd. Dit terwijl de Wbp vereist dat de verantwoordelijke ook moet bedingen dat de bewerker de beveiligingsverplichtingen nakomt die op verantwoordelijke rusten op grond van de Wbp, en dat de verantwoordelijke daadwerkelijk moet

		toezien op naleving van deze beveiligingsverplichtingen.
[10] Binnen de gemeente is de gegevensbescherming belegd bij een functionaris. Daarbij is ook omschreven welke verantwoordelijkheden en bevoegdheden deze functionaris bij de buiten de gemeente geplaatste instellingen en organisaties heeft.		Er is een privacybeheerder met beperkte bevoegdheden. Richting externe organisaties heeft de privacybeheerder geen bevoegdheden. Op grond van de AVG zullen overheidsinstanties en publieke organisaties verplicht worden om een FG aan te stellen. Uit gesprekken is gebleken dat de gemeente heeft het voornemen om samen met enkele regiogemeenten een FG aan te stellen, maar een besluit hierover is nog niet genomen.
[11] De gemeente heeft beleid dat betrekking heeft op de omgang met datalekken. Dit beleid voldoet aan de wettelijke vereisten en dit beleid is bekend onder medewerkers.		Beleid met betrekking tot datalekken is opgenomen in het beleidskader. Uit gesprekken is gebleken dat er procedures zijn waarmee medewerkers bekend zijn.

Betrokkenen	**Oordeel**	
[12] Aan de inwoners is expliciet toestemming gevraagd voor het uitwisselen van hun persoonsgegevens.		De noodzaak van een wettelijke grondslag wordt in het privacybeleidskader onderschreven. In veel gevallen wordt om toestemming gevraagd. Echter toestemming is niet altijd de juiste grondslag, zeker in het sociale domein. De AP adviseert daarom een overzicht op te stellen van de doelen, grondslagen en persoonsgegevens in het sociaal domein. Dit overzicht is onder meer noodzakelijk om de taken in het sociaal domein te onderkennen die niet wettelijk zijn geregeld. Hier is toestemming mogelijk wel de enige grondslag.
[13] Op de website van de gemeente is terug te vinden welke persoonsgegevens door de gemeente zijn opgeslagen en met welk doel dit gebeurt.		In het privacybeleidskader staan de rechten van betrokkenen onder de Wbp vermeld. Communicatie over deze rechten en het faciliteren ervan verdient echter nog enige aandacht. Er is alleen een folder over gegevensverwerking door de gemeente specifiek gericht op het sociale domein. Deze maakt onderdeel uit van het privacybeleidskader. In de folder wordt voor meer informatie over de privacyrechten verwezen naar de website van de gemeente. Daar levert zoeken via de zoekfunctie echter geen resultaten op
[14] Op de website van de gemeente is terug te vinden hoe inwoners een klacht kunnen indienen tegen opslag van hun gegevens en/of onjuistheden daarin. Eventuele klachten worden in behandeling genomen en daarover wordt gemotiveerd en onderbouwd een besluit genomen.		Volgens het privacybeleidskader kunnen inwoners zich met klachten wenden tot het KCC. Echter, volgens de website is er geen aparte klachtenregeling voor privacy. Hoewel de gemeente weliswaar een algemene klachtenregeling kent, wordt nergens duidelijk gemaakt dat deze ook voor privacyklachten geldt.

Raad	**Oordeel**	
[15] Aan de raad wordt gerapporteerd over privacybescherming. Tenminste één keer per jaar wordt hierover schriftelijk verslag aan de raad uitgebracht.		Er wordt niet structureel, bij de jaarrekening/jaarverslag of anderszins over privacybescherming gerapporteerd.

4. Conclusies en aanbevelingen

In dit hoofdstuk worden het antwoord op de hoofdvraag van dit onderzoek en de conclusies die hierop zijn gebaseerd geformuleerd. De conclusies leiden tot een aantal aanbevelingen. De basis voor dit hoofdstuk zijn de bevindingen en beantwoording van de deelvragen uit hoofdstuk 2 en de beoordeling aan de hand van het vooraf geformuleerde normenkader uit hoofdstuk 3.

4.1 Conclusies

De hoofdvraag die bij dit onderzoek centraal stond, luidt: *In hoeverre is het privacybeleid bij de gemeente rechtmatig en doelmatig en in hoeverre is de privacy van inwoners geborgd?*

Doelmatigheid en rechtmatigheid
Ten aanzien van het eerste deel van deze vraag betreffende de doelmatigheid en rechtmatigheid beantwoordt de rekenkamercommissie de hoofdvraag als volgt:

Qua inhoud (grondslag, doelbinding, dataminimalisatie, rechten van betrokkenen etc.) en qua proces (onder andere een duidelijke verdeling van taken en verantwoordelijkheden, evaluatieprocessen en een PDCA-cyclus) bevat het privacybeleidskader op papier veel elementen die de wet voorschrijft.
In het onderzoek is gebleken dat de gemeente aandacht besteedt aan het waarborgen van de privacy van inwoners. Een aantal maatregelen is, en was, al van kracht, zoals incidentele controles, het bijhouden van een register met verwerkingen, een overzicht van datalekken en er wordt veel aandacht besteed aan bewustwording onder de medewerkers. Ook al is het privacybeleidskader recentelijk vastgesteld, privacybescherming leeft op de werkvloer en in de organisatie.
In die zin is het beleidskader rechtmatig en in algemene zin ook doelmatig.

Borging
In het tweede deel van de hoofdvraag staat de vraag centraal of inwoners er op kunnen rekenen dat hun privacy is geborgd.
De rekenkamercommissie stelt in het algemeen dat met de aandacht die privacy binnen Doetinchem krijgt en de stappen die zijn gezet, de gemeente op de goede weg is. Echter, de uitdagingen op dit gebied blijven toch groot en de eisen die gesteld worden, worden in de toekomst steeds strenger. Privacybescherming zal voortdurende aandacht blijven vragen. Daarmee concludeert de rekenkamercommissie het volgende:

- Het privacybeleidskader is recent vastgesteld en moet op onderdelen verder uitgewerkt worden. Hiervoor bestaan geen concrete plannen;
- Er zijn geen afspraken gemaakt om de effectiviteit van het privacybeleid vast te stellen en gestructureerd, periodiek te evalueren en bij te stellen.
- De gemeente geeft beperkt invulling aan haar verantwoordelijkheid voor de verwerking van persoonsgegevens voor gemeentelijke taken die zijn belegd bij organisaties buiten de gemeente.
- De gemeente is zich bewust van de komst van de AVG (ingangsdatum 25 mei 2018) maar heeft geen impactanalyse uitgevoerd of invoeringsplan uitgewerkt.
- Privacy heeft nauwelijks aandacht van de gemeenteraad. Daarbij wordt de raad op dit moment beperkt geïnformeerd.

4.2 Aanbevelingen

Op basis van de conclusies komt de rekenkamercommissie tot de volgende aanbevelingen:

- Kom tot een concreet uitvoerings- en implementatieplan van het privacybeleidskader waarmee het beleid daadwerkelijk, volledig en consequent wordt uitgevoerd.
- Besteed expliciet aandacht aan het evalueren, leren en bijstellen van het beleid.
- Geef invulling aan de organisatie en naleving van privacywaarborgen in de relatie met ketenpartners/bewerkers en zie toe op de nalevering daarvan.
- Geef, in aanloop naar de invoering van de AVG in 2018, invulling aan de strengere eisen op het gebied van verantwoording en transparantie. Maak inzichtelijk welke afwegingen daarbij gemaakt worden (niet alleen qua beleid, maar ook in de praktijk) en leg dit ter besluitvorming voor aan de gemeenteraad.
- Geef als gemeenteraad aan waarover en op welke wijze het college moet rapporteren.

Bijlage A Gebruikte afkortingen

Afkorting	Betekenis
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIG	Baseline Informatiebeveiliging Gemeenten
CISO	Chief Information Security Officer
FG	Functionaris Gegevensbescherming
PIA	Privacy Impact Assessment
Wbp	Wet bescherming persoonsgegevens
Wmo	Wet maatschappelijke ondersteuning

Bijlage B Geïnterviewde personen

#	Datum	Naam	Functie
1	22 februari 2017	H. Legebeke	Hoofd Services
2	22 februari 2017	G. Verbeek	Regisseur Sociaal Domein
3	22 februari 2017	R. Ruiterkamp S. Gries	Hoofd KCC Teamleider KCC
4	22 februari 2017	K. Telder	Wethouder
5	22 februari 2017	P. Fuijk	Juridisch adviseur
6	23 februari 2017	N. Rensink	Coördinator Informatiebeveiliging
7	23 februari 2017	N. van Waart	Gemeentesecretaris
8	23 februari 2017	R. Frerix	Directeur Bedrijfsvoering
9	23 februari 2017	H. van Dijk	Team beleid en kwaliteit Zorgplein

Bijlage C Georganiseerde bijeenkomsten

#	Type bijeenkomst	Datum	Deelnemers
1	Startbijeenkomst	25 januari 2017	Direct betrokkenen van de gemeente
2	Casusbespreking KCC	29 maart 2017	Medewerker en afdelingshoofd KCC, coördinator informatiebeveiliging
3	Casusbespreking Jeugdhulp	29 maart 2017	Medewerkers gemeente en medewerkers Buurtplein, coördinator informatiebeveiliging
4	Convergentiesessie	20 april 2017	Medewerkers gemeente en medewerkers Buurtplein, coördinator informatiebeveiliging, juridisch medewerker

Bijlage D Bestudeerde documentatie

#	Document	Datum
1	Adviesrapport Privacybeleid Gemeente Doetinchem, Stappenplan privacybescherming voor het sociaal domein (PrivacyManagementPartners)	8 oktober 2015
2	Beleid logische toegangsbeveiliging	2017
3	Convenant met Buurtplein voor het gebruik van gegevens uit de basisregistratie personen	7 oktober 2015
4	Convenant met Laborijn voor het gebruik van gegevens uit de basisregistratie personen	31 mei 2016
5	Handleiding melden van een datalek	29 juni 2016
6	Incident managementproces meldplicht datalekken (inclusief overzicht datalekken)	gestart op 1 januari 2016 (dynamisch document)
7	Informatiebeveiligingsbeleid 2015-2019 (Gemeente Doetinchem) versie 1.0	21 april 2015
8	Klachtafhandeling doorgifte persoonsgegevens (brief, geanonimiseerd)	27 november 2015
9	Onderzoek Veilig gebruik Suwinet 2016 (brief van inspectie SZW)	25 oktober 2016
10	Opdrachtovereenkomst 2017 Buurtplein b.v. - gemeente Doetinchem	6 juni 2017
11	Privacybeleidskader gemeente Doetinchem met bijlagen	Januari 2017
12	Procedure verstrekking van gegevens aan organen van de gemeente *gemeente Doetinchem) versie. Versie 2.1	1 mei 2014
13	Stroomschema Zwitsers zakmes	25 februari 2016
14	Suwinet Handboek met bijlagen	12 maart 2014
15	Werkinstructie ‘Omgaan met privacy’, Kaders voor medewerkers van het Zorgplein	Januari 2017
16	Email “overzicht partijen uitwisseling persoonsgegevens” doorgestuurd aan PBLQ t.b.v. onderzoek	1 februari 2017

Bijlage E Praktijkonderzoek

Om te toetsen of het beleid en de gemaakte afspraken worden nageleefd en om te ervaren hoe er binnen de organisatie over een zorgvuldig gebruik van persoonsgegevens wordt gesproken en gedacht zijn twee casussen in aparte bijeenkomsten besproken:

1. Casus “Klantcontactcentrum”
2. Casus “Jeugdhulp”

Tijdens de bespreking is met direct betrokken gesproken over de manier waarop met persoonsgegevens wordt omgegaan. Voor de casus Jeugdhulp waren ook twee medewerkers van Buurtplein BV aanwezig.
De besprekingen zijn gevoerd aan de hand van een aantal specifieke aandachtsvelden. Op basis daarvan is een oordeel gevormd en zijn risico’s benoemd.

Casus Klantcontactcentrum

Beschrijving Casus
Het KCC ontvangt dagelijks vele veelzijdige meldingen. Elke nieuwe melding wordt verwerkt in het zaaksysteem, waarbij diverse persoonsgegevens uit de BRP op basis van postcode-huisnummer aan de melding worden toegevoegd. Het is de verantwoordelijkheid van medewerkers van het KCC om zoveel mogelijk gegevens uit te vragen, zodat bij afhandeling de backoffice dat niet apart hoeft te doen. Voorheen werd daardoor eigenlijk teveel informatie uitgevraagd. Nu is er meer aandacht voor ‘need to have’ en het voorkomen van ‘nice to have’.

Eenvoudige meldingen worden direct afgedaan, andere vragen worden doorgezet naar de relevante backoffices. Medewerkers van de KCC houden inzage in de status van de melding zodat ze daarover informatie kunnen verstrekken als ze daarnaar worden gevraagd. Dat betekent dat ze toegang hebben tot diverse andere gemeentelijke systemen, waarbij ze in beginsel (en zeker voor gegevens uit het sociaal domein) alleen statusinformatie kunnen inzien. Voor sommige systemen geldt dat ook inhoudelijke informatie toegankelijk is, zoals voor gemeentebelastingen.

Medewerkers van het KCC ondertekenen bij aanstelling een geheimhoudingsverklaring. Er is veel aandacht voor bewuste omgang met gegevens, zoals in teamoverleggen en overleggen met de leidinggevende. Alle medewerkers van de gemeente moeten jaarlijks slagen voor de digitale kennistoets informatiebeveiliging. Verder draagt de privacybeheerder van de gemeente zorg voor presentaties en voorlichting en controleert actief op mogelijke misstanden.

Handelingen, zoals het raadplegen van gegevens, worden gelogd en steeksproefgewijs worden deze logbestanden gecontroleerd. Bij opmerkelijke patronen worden medewerkers daarop aangesproken. De leidinggevende moet toezicht houden op autorisaties en de toekenning van inzagerechten. Deze worden ook jaarlijks structureel gecontroleerd.

Juridisch kader

- Gemeentewet of andere wetgeving waar i.i.g. de taken van de gemeente staan opgenomen
- Wbp/Avg
- Wet BRP

Bevindingen

	Wat gaat goed	Risico's
Positie van de burger	In beleid veel aandacht voor privacy van de burger	Inzage- en correctierecht zijn in het algemeen wel geregeld, maar worden niet gecommuniceerd. Kans bestaat dat de burger niet bekend is met zijn rechten.
Werkprocessen	Veel aandacht voor bescherming privacy burger. Uitgangspunt is 'need to know'	Als gevolg van zoveel mogelijk zelfstandig afhandelen door KCC constante spanning tussen *nice to have* en *need to know*
Taken en verantwoordelijkheden	Duidelijk belegd, medewerkers kennen hun verantwoordelijkheid.	Onduidelijk is wie de 'leidinggevende' controleert
ICT en informatiesystemen	Op orde en worden up-to-date gehouden	Het is niet precies duidelijk welke gegevens beschikbaar zijn. Het systeemeigenaarschap en daarmee de verantwoordelijkheid voor (met name) generieke applicaties, zoals het zaaksysteem, is niet duidelijk.
Informatiebehoefte	Aandacht voor doelbinding	Neiging tot 'overvragen' Bewaartermijn niet duidelijk

Casus Jeugdhulp

Beschrijving Casus

De uitvoering van de jeugdzorg is in de gemeente zowel belegd bij de gemeente als bij de BV opgerichte uitvoeringsorganisatie Buurtplein. Bij Buurtplein zijn de wijkteams en de jeugdcoaches ondergebracht. Signalen van mogelijke problemen met jeugdigen in de gemeente kunnen door veel verschillende partijen worden gedaan, zoals professionals in het veld, mensen in de omgeving, betrokkenen zelf als door hulpverleners van Buurtplein of medewerkers van de gemeente. Er zijn daarmee veel verschillende 'intakemogelijkheden' voor een vraag. Dat betreft onder meer de website, het KCC, gemeentelijke loketten, de wijkteams, etc.

Meldingen worden geregistreerd in het systeem van de gemeente, WIZ. Zowel medewerkers van de gemeente als van het Buurtplein hebben toegang tot WIZ. Op basis van de melding (postcode) worden gegevens aan de melding toegevoegd. Het Burgerservicenummer (bijzonder persoonsgegeven) van de betrokken jongere en eventueel diens ouders worden alleen toegevoegd als de ouders (c.q. wettelijk vertegenwoordiger) daar toestemming voor hebben gegeven. De dossiers worden opgebouwd in de gemeentelijke systemen, nu CORSA, in de toekomst vermoedelijk GWS. Er is vastgelegd wie geautoriseerd is om toegang te krijgen tot de dossiers.

Een deel van de meldingen leidt tot een concrete ondersteuningsvraag. De ondersteuningsvraag moet uiteindelijk door een jeugdconsulent van de gemeente worden beoordeeld, die voor de beslissing over een onderbouwd voorstel (gezinsplan) moet kunnen beschikken. De uitvoering wordt belegd bij buurtplein of gespecialiseerde organisaties, waarbij natuurlijk ook weer overdracht van informatie plaatsvindt.
Het gezinsplan wordt door een jeugdcoach van de wijkteams opgesteld. Dit gezinsplan vormt ook de basis van de af te geven beschikking. In de praktijk is een goedgekeurd gezinsplan, de beschikking, die als zodanig ook geregistreerd en gearchiveerd moet worden en waartoe dan zowel medewerkers van de gemeente als van het buurtteam toegang hebben.

Hoewel de gemeente beschikt over een veilige manier om persoonsgegevens uit te wisselen (Owncloud) bleek tijdens de bespreking dat het ook voorkomt dat gezinsplannen via Email- in PDF-formaat- worden gedeeld tussen betrokkenen. Medewerkers kiezen voor het gebruik van email omdat zij het gebruik van de Owncloud als lastig wordt ervaringen, c.q. het te tijdrovend is om zich te verdiepen in het gebruik van deze veilige toepassing.

In principe is het gezinsplan het eigendom van het gezin. Het gezin moet expliciet de toestemming geven dat het plan met anderen gedeeld kan worden. In de praktijk wordt die toestemming vrijwel altijd verleend, omdat het gezin anders verstoken zal blijven van ondersteuning.
Als uitvoeringsorganisatie van de gemeente zijn de regels en afspraken waar het Buurtplein zich aan dient te houden vastgelegd in de opdrachtgevers/opdrachtnemers-overeenkomst (OGON). Dat betreft ook privacy. Binnen de gemeente is veel aandacht voor autorisatie, en doelbinding van op te vragen informatie. Binnen Buurtplein wordt deze aandacht momenteel gestimuleerd, maar moet het bewustzijn zeker nog toenemen. Buiten hetgeen er vastgelegd is in de OGON, is er nog geen sprake van een specifieke bewerkersovereenkomst. Hier wordt nu wel over nagedacht.

Juridisch kader
- Gemeentewet of andere wet
- Jeugdwet
- Wet BSN
- Wbp/AVG

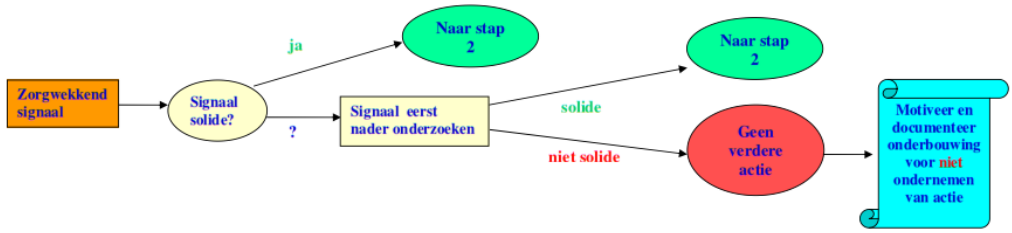
Bevindingen

	Wat gaat goed	Risico's
Positie van de burger	In principe voert de burger de regie op de gegevens	De burger heeft eigenlijk geen keuze dan om de gegevens te delen, in dat geval zou sprake zijn van onvrije toestemming, wat geen grondslag vormt voor gegevensverwerking; Inzage- en correctierecht zijn niet duidelijk geregeld. Burger kan lastig overzicht houden wie inzage heeft in welke gegevens
Werkprocessen	Er is aandacht voor doelbinding, autorisaties en veilige gegevensoverdracht; Sprake van controles, zowel op het beleid als geheel als op concrete processen. Zo worden er logbestanden bijgehouden. Ook is er binnen de gemeente sprake van een procedure voor datalekken;	Het bewustzijn binnen de gemeente is verder ontwikkeld dan bij Buurtplein. De indruk bestaat dat procedures, processen en beveiliging bij Buurtplein minder strikt worden gecontroleerd dan bij de gemeente. Zo bestaat er bij Buurtplein geen vaste procedure hoe om te gaan met datalekken. De gemeente heeft nog niet zo lang de verantwoordelijkheid over het jeugdbeleid. Afspraken en procedures over archivering (en vernietiging, 'het recht om vergeten te worden') zijn nog niet uitgekristalliseerd

Taken en verantwoordelijkheden	m.b.t. primaire proces binnen betrokken organisaties zijn taken en verantwoordelijkheden belegd. E.e.a. is vastgelegd in de OG-ON-overeenkomst tussen gemeente en Buurtplein	Gegevensuitwisseling tussen organisatie, uitvoering van privacybeleid en maatregelen en ICT(ondersteuning) is minder goed geregeld.
ICT en informatiesystemen	Binnen de systemen zijn autorisaties ingeregeld en kan worden gelogd wanneer functionarissen informatie toevoegen of ontlenen aan de dossiers	Er wordt gewerkt met systemen die niet altijd zijn ontwikkeld voor deze specifieke taken en verantwoordelijkheden. Zo is logging en monitoring niet voor alle systemen mogelijk. Vooral de overdracht van gezinsplannen via Email is kwetsbaar en moet voorkomen worden.
Informatiebehoefte	Er is aandacht voor doelbinding van op te vragen informatie	In de praktijk bestaat de neiging meer informatie te verzamelen dan wellicht nodig

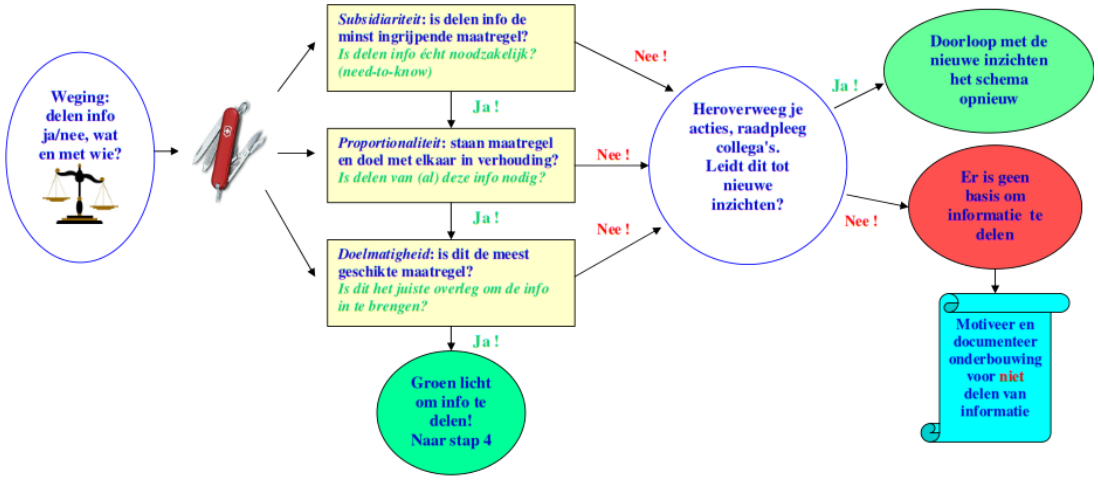
Bijlage F Het 'Zwitsers zakmes': afwegingskader voor het sociaal domein

1. EEN ZORGSIGNAAL KOMT BINNEN, WAT DOE JE HIERMEE?

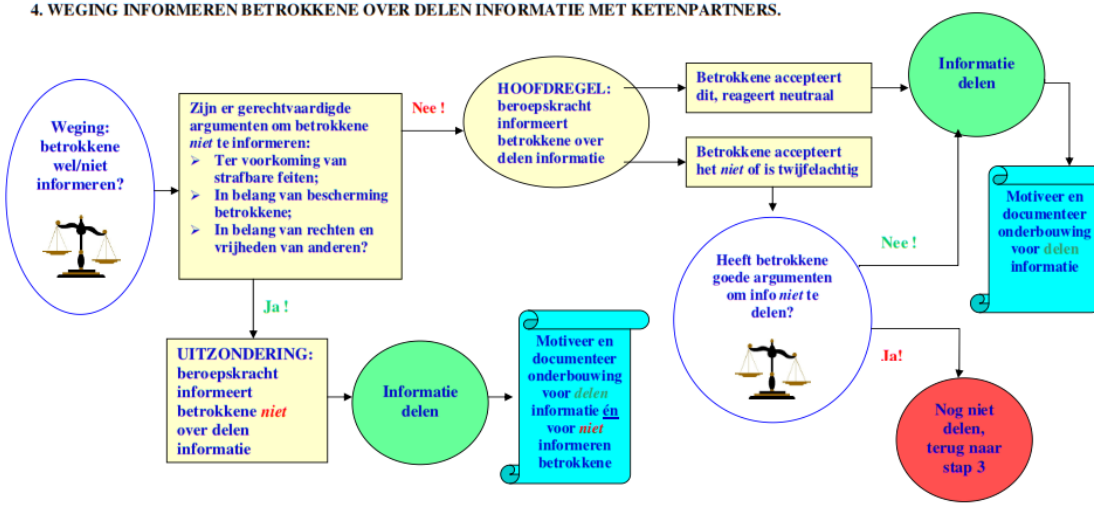


2. BEOORDELING DOEL UITWISSELEN INFORMATIE MET KETENPARTNERS.

3. WEGING UITWISSELEN INFORMATIE, TOEPASSING ZWITSERS ZAKMES.



4. WEGING INFORMEREN BETROKKENE OVER DELEN INFORMATIE MET KETENPARTNERS.



Bijlage G Ambtelijk wederhoor

Mede op initiatief van de ambtelijke organisatie en met enthousiaste instemming van zowel de rekenkamercommissie als het uitvoerend bureau, is bij dit onderzoek sprake geweest van een mondelinge bespreking van het ambtelijk wederhoor. Het voordeel daarvan is dat ter plekke opmerkingen en commentaar toegelicht en genuanceerd kunnen worden.
Op 13 juli 2017 heeft dit gesprek plaatsgevonden. Het bleek dat er nauwelijks feitelijke onjuistheden in het rapport waren aangetroffen, behoudens een enkele omschrijving van de functie van respondenten. Tevens is gesproken over de achtergronden van de keuze voor een specifieke kleur van de 'stoplichten' in hoofdstuk 3. Dit leidde overigens tot de vaststelling dat de kleuren ongewijzigd konden blijven. Verder is bij een enkel punt door de ambtelijke organisatie om verduidelijking van de tekst gevraagd.
Na de feitelijke bespreking van de rapportage is met de aanwezigen nog van gedachten gewisseld over mogelijke conclusies en aanbevelingen die aan de bevindingen verbonden zouden kunnen worden.
De deelnemers stelden unaniem vast dat de keuze om het ambtelijk commentaar gezamenlijk te bespreken hun zeer is bevallen. Zij deden dan ook de suggestie om dit ook bij volgende onderzoeken zo in te richten.