Oktober 2018

Privacybeleid

Onderzoek naar privacybeleid in Pijnacker-Nootdorp

Voorwoord

In de periode maart tot juli 2018 heeft PBLQ, in opdracht van de rekenkamercommissie (RKC) Pijnacker-Nootdorp onderzoek gedaan naar het privacybeleid van de gemeente. Het onderzoek beoogt inzicht te bieden in de doeltreffendheid en de doelmatigheid van de beveiliging van persoonsgegevens van inwoners en mogelijke verbeteringen, rekening houdend met de invoering van de AVG. Het resultaat van het onderzoek treft u aan in het voorliggende rapport 'Privacybeleid in Pijnacker-Nootdorp'.

In afwijking van eerdere onderzoeken door de rekenkamercommissie heeft het ambtelijk wederhoor niet schriftelijk plaatsgevonden. Op basis van de ervaring van de onderzoekers van PBLQ is het ambtelijk wederhoor vorm gegeven door het organiseren van een gesprek tussen de onderzoekers en de relevante vertegenwoordigers van de gemeente. Het gesprek bood alle mogelijkheden voor verduidelijking van bevindingen en formuleringen enerzijds en de opvattingen en reacties daarop anderzijds en is dan ook in Pijnacker-Nootdorp positief ervaren door de onderzoekers.

Ten aanzien van het privacy beleid stellen wij samen met het college van Burgemeester en Wethouders vast, dat er de afgelopen jaren binnen de gemeente Pijnacker-Nootdorp al sprake was van kennis over en aandacht voor privacy en informatiebeveiliging. De gemeente heeft het beleid op papier in orde en het traject ingezet voor de implementatie van de AVG.
In het onderzoek is wel geconstateerd dat er nog een aantal elementen mist en/of verbeterd kan en dient te worden in de vertaling en implementatie van het beleid naar de werkpraktijk. Kennis, informatie, continuïteit en communicatie zijn cruciaal voor de overdracht én het blijvend vasthouden van de aandacht voor het onderwerp in de gehele organisatie Hierbij dient er ook expliciet aandacht te zijn voor de positie en de informatievoorziening aan de inwoners en het meenemen van de gemeenteraad in de ontwikkelingen.
In het licht van de AVG en de huidige uitvoering binnen de gemeentelijke organisatie legt de rekenkamercommissie de gemeenteraad daarom ter besluitvorming acht aanbevelingen voor die na bestuurlijk wederhoor ongewijzigd zijn gebleven.

De RKC bedankt het college van Burgemeester en Wethouders, de gemeentelijke organisatie en de Adviesraad Sociaal Domein voor de constructieve samenwerking bij de totstandkoming van dit rapport. Wij vertrouwen erop dat de uitkomsten van dit rapport een positieve bijdrage leveren aan de verdere vertaling van het privacybeleid naar de praktijk.

Namens de rekenkamercommissie Pijnacker-Nootdorp,

Hans Lesscher, voorzitter

Privacybeleid in Pijnacker-Nootdorp

15 oktober 2018

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Overheden beheren veel gegevens van burgers. Dat geldt bij uitstek voor gemeenten. Daar vindt de registratie in het bevolkingsregister plaats, melden inwoners zich voor een vergunning, een uitkering of andere vragen om zorg of ondersteuning.
Na de decentralisatie hebben meer burgers met een hulpvraag te maken met de gemeente. Het betreft veelal mensen in een kwetsbare positie die afhankelijk zijn van de ondersteuning door de gemeente. Daarmee is het gegevensverkeer binnen de gemeente complexer geworden: meer cliënten, meer gevoelige gegevens, zoals die over gezondheid, inkomen, justitiecontacten, verhoudingen binnen een gezin en dergelijke, die ook nog eens gedeeld moeten worden met veel meer externe partijen zoals zorgaanbieders.

Burgers moeten ervan uit kunnen gaan dat hun gegevens, zeker persoonlijke gegevens, bij elke gemeente in veilige handen zijn. Gemeenten moeten dat vertrouwen verdienen, zowel in de directe contacten met de burger als in verantwoordingen achteraf. Bescherming van persoonsgegevens is immers een grondrecht. Wordt dit recht, en daarmee het vertrouwen in de overheid, geschaad, dan kan dat ernstige gevolgen hebben voor de relatie tussen gemeente en burger.

Veel gemeenten worstelen met het vraagstuk privacy. Bovendien leeft, met name in het sociaal domein, bij veel gemeenten het idee dat privacy en dienstverlening elkaar in de weg zitten. Daarnaast is de regelgeving aangescherpt en zijn de implicaties van de Algemene Verordening Gegevensbescherming (AVG) voor de gemeentelijke bedrijfsvoering nog niet overal helder. Wel is duidelijk dat gemeenten risico's lopen in het geval zij niet conform de geldende normen de beveiliging van persoonsgegevens op orde hebben. In het uiterste geval zouden gemeenten boetes kunnen worden opgelegd.

Het belang van een adequaat privacybeleid en een strikte uitvoering is daarmee toegenomen. Gezien deze context en ontwikkelingen heeft de rekenkamercommissie van de gemeente Pijnacker-Nootdorp begin 2018 het initiatief genomen tot een onderzoek naar de wijze waarop deze gemeente uitvoering geeft aan de bescherming van persoonsgegevens. In deze rapportage wordt verslag gedaan van de inzichten die tijdens dit onderzoek zijn opgedaan en de conclusies die daaruit kunnen worden afgeleid. De rapportage wordt afgesloten met enkele aanbevelingen.

1.1 Opdrachtformulering

Privacy en een correcte omgang met persoonsgegevens worden vaak louter als juridische en ICT-technische onderwerpen gezien. De aandacht daarvoor beperkt zich dan tot de afdeling Juridische Zaken en de afdeling ICT. Voor dit onderzoek is uitgangspunt dat een zorgvuldige omgang met persoonlijke gegevens een kernwaarde dient te zijn van elke medewerker van de gemeente. Daarmee is de menselijke factor en de dagelijkse uitvoeringspraktijk een gemeente- en organisatiebreed aandachtspunt. Het betekent dat het beleid aan iedereen bekend moet zijn, omdat je immers 'de

regels niet kunt naleven als je ze niet kent'.[1] De ervaring is dat kennis over de regelgeving, zowel de Wbp/AVG als de informatieparagrafen in de materiewetten, nog niet in elke gemeente voldoende aanwezig is. Het schort er vervolgens aan om de regelgeving te vertalen naar kaders en praktische instructies voor de uitvoering. Bovendien zit de noodzaak om zorgvuldig met persoonsgegevens om te gaan niet bij medewerkers van elke gemeente in het DNA. Dat betreft in het bijzonder het sociaal domein waar privacy soms wordt gezien als een belemmerende factor om integraal te werken.

In het uitgevoerde onderzoek staat de vraag centraal in hoeverre de gemeente Pijnacker-Nootdorp in de dagelijkse praktijk correct omgaat met de persoonlijke gegevens van burgers. In dit verband is extra aandacht besteed aan de omgang met persoonsgegevens in het sociaal domein.

In het onderzoek is gesteld dat respect voor privacy onderdeel is van integere dienstverlening. Daarvoor moeten medewerkers de geldende regels kennen, de betekenis daarvan hebben geïnternaliseerd, ze weten te vertalen naar processen, organisatie en techniek, en de wijze waarop de burger wordt bejegend. In feite begint het niet met regels, maar met bewustwording van het feit dat bescherming van persoonsgegevens een grondrecht is dat gerespecteerd moet worden. Zeker door gemeenten waar burgers van afhankelijk zijn en alleen in uiterste nood aankloppen.

Een en ander heeft geresulteerd in de volgende doelstelling van het ondernomen onderzoek:

> **De rekenkamercommissie wil inzicht krijgen in de doeltreffendheid en de doelmatigheid van de beveiliging van persoonsgegevens van inwoners en mogelijke verbeteringen, rekening houdend met de invoering van de AVG.**

De centrale probleemstelling van het onderzoek is als volgt geformuleerd:

> ***Hoe is in het licht van de decentralisaties in het sociaal domein en de verdergaande digitalisering de privacy van inwoners juridisch en in de praktijk geborgd en op welke punten behoeft dit eventueel aanpassingen?***

Deze centrale probleemstelling is uitgewerkt in tien deelvragen, die gegroepeerd zijn rond de thema's beleid, leren en verbeteren, de positie van de burger en de kaderstellende en controlerende rol van de raad. Deze deelvragen staan in onderstaande tabel.

Deelvragen

Beleid
1. Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de juridische borging van de privacy van de inwoners?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Gemeenten (BIG), aan de Wet bescherming persoonsgegevens (Wbp) en vanaf 25 mei 2018 aan de algemene verordening gegevensbescherming (AVG)?
3. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?
4. Zijn er casussen waarin sprake is van schending van de privacy van inwoners en hoe is daarmee omgegaan?

[1] Privacy is een mensenrecht. Met mensenrechten hoor je niet te experimenteren. Y. Bommeljé, R. van Oostrom in Sociaal Bestek, 2015- nr 1.

Leren en Verbeteren
5. Hoe worden medewerkers betrokken bij en getraind in het borgen van de privacy van de inwoners? 6. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop de privacy van de inwoners is geborgd binnen de gemeente? 7. Hoe ziet de gemeente erop toe dat de borging van de privacy van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven en juridische ontwikkelingen?
Positie van de burger
8. Hoe communiceert de gemeente naar inwoners over de wijze waarop zij omgaat met persoonsgegevens?
Kaderstellende en controlerende rol van de raad
9. Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid en informatieveiligheid in het sociaal domein betrokken geweest? 10. Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?

1.2 Werkwijze

Het onderzoek is langs de volgende stappen ingericht:

- **Vaststellen normenkader**
  In dit rekenkameronderzoek worden de bevindingen getoetst aan een normenkader. In een eerste bespreking met de rekenkamercommissie is dit normenkader vastgesteld. Dit normenkader is opgenomen in bijlage D.
- **Documentenstudie**
  Ten behoeve van het onderzoek is kennisgenomen van relevante documenten. Naast beleidsdocumenten betreft dat ook overzichten van de binnen de organisatie geldende afspraken en procedures. Ook is kennisgenomen van eerdere verkenningen en beoordelingen van de uitvoeringspraktijk, zoals audits. Een overzicht van alle geraadpleegde documenten is opgenomen in bijlage C.
- **Interviews en groepssessies**
  Vervolgens hebben interviews plaatsgevonden met personen binnen de organisatie die betrokken zijn bij het beleid of in hun uitvoerende activiteiten direct te maken hebben met het privacybeleid. In bijlage B is vermeld met welke personen interviews hebben plaatsgevonden.
  Om meer zicht te krijgen in de vraag hoe in de dagelijkse praktijk de medewerkers van de gemeente omgaan met privacy zijn er bovendien twee groepssessies georganiseerd om werkprocessen door te lopen op privacyaspecten. Dat is uitgevoerd voor het proces 'vergunningverlening', in het bijzonder de vergunningen voor kinderdagverblijven, en voor processen in het sociaal domein: de 'aanvraag van een uitkering Participatiewet', 'aanvraag voor een Wmo-voorziening' en het proces 'melding en intake kernteam'.
- **Convergentiesessie**
  Op basis van de voorgaande stappen hebben de onderzoekers zich een beeld kunnen vormen over het privacybeleid en hoe daar in de praktijk inhoud aan wordt gegeven. Om dat beeld scherper te stellen hebben we een convergentiesessie georganiseerd. Hierin zijn de voorlopige bevindingen gepresenteerd en bediscussieerd. Op die manier was het mogelijk om de bevindingen te toetsen, te verdiepen en aan te scherpen of te nuanceren. Aan deze sessie is deelgenomen door het merendeel van medewerkers die we eerder hadden geïnterviewd.

- **Sessie met de raad**
  Een belangrijke vraag uit het onderzoek is de betrokkenheid van de gemeenteraad. Tijdens het onderzoek vonden de gemeenteraadsverkiezingen plaats en is de raad van samenstelling veranderd. Met een aantal raadsleden heeft een bijeenkomst plaatsgevonden. Aan de hand van een fictieve casus over een mogelijk datalek in het sociaal domein is bediscussieerd waar risico's voor privacy zich in de praktijk voordoen en wat de mogelijke bemoeienis van de raad daarbij kan zijn. Vervolgens is dat vertaald naar Pijnacker-Nootdorp en is door de aanwezigen een lijst aandachtspunten opgesteld waarover zij geïnformeerd wil worden, en voor de wijze waarop zij haar kaderstellende, controlerende en vertegenwoordigende taak wil gaan uitvoeren. Deze bijeenkomst leverde een belangrijk deel van de informatie voor het beantwoorden van de onderzoeksvragen over de rol van de raad.
- **Opstellen rapportage**
  Op basis van de verzamelde informatie is de uiteindelijke rapportage opgesteld. Daarin zijn de antwoorden op de onderzoeksvragen opgenomen en zijn de bevindingen getoetst aan het normenkader. Het feitelijk deel van de rapportage is aan de organisatie voorgelegd, zodat ze eventuele onjuistheden konden aangeven. In afwijking van de gebruikelijke procedures heeft dit ambtelijk wederhoor plaatsgevonden op basis van een gesprek tussen de onderzoekers en vertegenwoordigers van de organisatie. Na het definitief vaststellen van het feitelijk deel heeft de rekenkamer conclusies en aanbevelingen geformuleerd. Het college van B&W van Pijnacker-Nootdorp is de mogelijkheid geboden om een reactie te geven op deze conclusies en aanbevelingen. Dit ‘bestuurlijk wederhoor’ is toegevoegd aan de rapportage.

Het merendeel van de verzamelde informatie door middel van documenten en interviews heeft plaatsgevonden tot de zomer van 2018. Sindsdien heeft de ontwikkeling van het beleid binnen de gemeente Pijnacker-Nootdorp niet stilgestaan en zijn verdere maatregelen doorgevoerd en instrumenten toegepast. Waar relevant wordt hiervan melding gemaakt.

Tijdens dit onderzoek zijn geen persoonsgegevens in de zin van art. 1 AVG verwerkt anders dan de namen en contactgegevens van de geïnterviewde functionarissen.

1.3 Indeling rapport

In het volgende hoofdstuk wordt verslag gedaan van de opgedane inzichten. Hoofdstuk 2 is opgebouwd analoog aan de groepering van deelvragen. Dat betekent dat in hoofdstuk 2 eerst inzichten met betrekking tot het gemeentelijk beleid worden beschreven, gevolgd door de inzichten die betrekking hebben op de wijze waarop de gemeente invulling geeft aan het proces van leren en verbeteren in het privacybeleid. Daarna wordt aandacht besteed aan de positie van de burger. De bevindingen in hoofdstuk 2 worden afgesloten met een korte beschrijving van de positie van de raad.

Het derde hoofdstuk begint met een korte samenvatting van de bevindingen. Daarna worden alle onderzoeksvragen beantwoord. Met gebruikmaking van een beoordeling van de bevindingen, door gebruikmaking van het normenkader, worden vervolgens enkele conclusies geformuleerd. Het hoofdstuk wordt afgesloten met enkele aanbevelingen.

Een overzicht van in dit rapport veelgebruikte afkortingen is opgenomen in bijlage A.

2. Bevindingen

2.1 Het gemeentelijk beleid

Binnen de gemeente Pijnacker-Nootdorp bestaat al sinds enkele jaren aandacht voor zowel privacybescherming als informatieveiligheid. Bij processen en handelingen waar veel persoonsgegevens aan de orde zijn (zoals de basisregistratie personen BRP) bestaan er van oudsher al (landelijke) afspraken om daar correct mee om te gaan. Ook wordt door middel van audits regelmatig getoetst of afgesproken procedures en afspraken worden nageleefd. Bij gebleken tekortkomingen worden er verbeteringen doorgevoerd. Later werden ook elders binnen de organisatie initiatieven ontwikkeld om het privacybeleid een meer structurele basis te geven, onder andere binnen het sociaal domein met het oog op de decentralisaties. Er zijn toen afspraken en overeenkomsten vastgelegd voor het delen van (persoons-)gegevens binnen de gemeentelijke organisatie of met samenwerkingspartners (persoons-)gegevens.

In de loop van 2016 is de aandacht voor privacybeleid (en informatieveiligheid) verbreed naar de gehele organisatie. Het groeipad leidde er toe dat het onderwerp gaandeweg in 2017 hoger op de bestuurlijke agenda kwam. Dit werd mede gestimuleerd door het gegeven dat de gemeente zich diende voor te bereiden op de voorziene inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) in mei 2018. Sindsdien zijn diverse betrokkenen binnen de organisatie gestructureerd te werk gegaan om er voor te zorgen dat de gemeente op 25 mei 2018 gereed zou zijn om aan de basisvereisten van de AVG te voldoen. Het directieteam (DT) heeft hiervoor in november 2017 de governance rond informatieveiligheid en privacy in de vorm van elf voorstellen vastgesteld. Dit is gevolgd door het *Projectplan Implementatie AVG* (december 2017). Dit implementatieplan bevat een overzicht van de zaken die op dat moment nog geregeld moeten worden. In het voorjaar van 2018 zijn in dat verband op tijdelijke basis een Chief Information Security Officer (CISO) en een Functionaris Gegevensbescherming (FG) aangesteld. Over de zomer van 2018 heen hebben zij het beleid verder doorontwikkeld.

In mei 2018 heeft het college van B&W het *Privacybeleid gemeente Pijnacker-Nootdorp* (het privacybeleidsdocument) ter kennisname aan de raad gestuurd. In dit document wordt ingegaan op de visie van de gemeente over privacy, de rechtmatigheid van verwerkingen binnen de gemeente (waaronder relevante grondslagen), de governance en organisatie binnen de gemeente ten aanzien van privacy en nieuwe ontwikkelingen. Ook kent de gemeente een beleidsdocument informatiebeveiliging, dat ten tijde van het onderzoek werd vernieuwd. Dit beleidsdocument beschrijft hoe informatiebeveiliging binnen de gemeente beheerst dient te worden, hoe de (informatie)beveiligingsorganisatie er uit ziet en het behandelt de beheersmaatregelen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Met de toezending van dit document aan de raad kan worden gesteld dat sinds begin mei 2018 de gemeente een privacybeleid kent dat recht doet aan wettelijke eisen en richtlijnen. Voor specifieke domeinen heeft de gemeente soms aanvullend privacybeleid. Dat betreft onder meer landelijk beleid, zoals voorgeschreven Suwinet-controles en de ENSIA-verantwoording[2]. Met de decentralisaties heeft

[2] Dit is de verantwoording over de informatieveiligheid van de gemeentelijke basisregistraties en kernregistraties o.a. de BRP, Basisregistratie Adressen en Gebouwen (BAG), paspoortuitvoeringsregelingen, digitale persoonsidentificatie ed.

de gemeente tevens een privacyprotocol opgesteld over de omgang met persoonsgegevens in de kernteams en het regieteam.

De onderlinge samenhang en de werking van de verschillende onderdelen van het privacybeleid vormden in de praktijk nog een aandachtspunt. Zo bleek rond de zomer dat er onder andere nog een verwerkingenregister, een datalekregister en een privacyverklaring moesten worden opgesteld. Aan deze acties is sindsdien door de FG en de CISO invulling gegeven.

Op de werkvloer (bijvoorbeeld in het sociaal domein) zijn de medewerkers zich op globaal niveau bewust van privacy van burgers en de privacyrisico's die bij het werk van de gemeente horen. Dat laat onverlet dat er nog verschillende complexe vragen zijn over hoe in de praktijk gehandeld moet worden en welke afwegingen er gemaakt moet worden ten aanzien van de bescherming van persoonsgegevens en de uitvoering van de primaire taken van de gemeente. Een voorbeeld hiervan is het gebruik van toestemming in het sociaal domein. In het privacybeleidsdocument wordt over toestemming gesteld dat er een grote kans is dat deze vanwege een afhankelijkheidsrelatie niet in vrijheid gegeven wordt. Echter, in de praktijk wordt er wel om toestemming gevraagd in de kernteams en is dit ook opgenomen als voorwaarde voor de verstrekking en uitwisseling van gegevens in het privacyprotocol. Het is het voornemen van de gemeente dat in het eerste kwartaal van 2019 voor dergelijke complexe vraagstukken antwoorden beschikbaar zullen zijn.

In het kader van de implementatie van het beleid verdienen de autorisaties voor enkele systemen en applicaties aandacht. Zo is geconstateerd dat meer medewerkers dan nodig inzage hebben in het systeem voor de vergunningen. Medewerkers die uitvoering geven aan de Participatiewet kunnen in het systeem bij de dossiers van alle cliënten. Ook de dossiers van reïntegratiecliënten staan op een gezamenlijk gedeelde schijf. Het regieteam, dat de complexe (gezins-)situaties begeleidt, werkt met een systeem waarmee medewerkers toegang hebben tot alle cliëntdossiers.
Verder moeten de ontwikkeling en uitvoering van Privacy Impact Assessments (PIA's), het verwerkingenregister, en zoals gezegd het opstellen van instructies voor complexe privacy vraagstukken (met name in het sociaal domein) nog plaatsvinden.

Wat het sociaal domein betreft, een specifiek aandachtspunt in dit rekenkameronderzoek, bleken Het uitgangspunt in het uitgevoerde onderzoek is de vraag in hoeverre de gemeente Pijnacker-Nootdorp in de dagelijkse praktijk correct omgaat met de persoonlijke gegevens van burgers. In dit verband is extra aandacht besteed aan de omgang met persoonsgegevens in het sociaal domein. En tijde van het onderzoek andere risico's, zoals:

- het gebruik van de zelfredzaamheidsmatrix en de daaraan ten grondslag liggende toestemming die cliënten dienen te geven;
- de wijze waarop de situatie en achtergronden van cliënten worden besproken in de kernteams en de kernteams;
- de toegang tot de systemen;
- dossiervorming; wat mag wel in een dossier worden opgenomen en wat niet;
- het gebruik van het BSN.

Een aantal van deze risico's zijn sinds de zomer opgelost, zoals met name het gebruik van de zelfredzaamheidsmatrix en het gebruik van het BSN.

In ons onderzoek hebben we geen uitwerkingen van werkprocessen aangetroffen waarin is beschreven welke persoonsgegevens wanneer en door wie mogen worden verwerkt. Het

privacyprotocol voor de kernteams en het regieteam gaan weliswaar in op de kaders met betrekking tot de verwerking van persoonsgegevens in het sociaal domein, maar geeft geen gedetailleerde beschrijving van de verwerking van persoonsgegevens in verschillende processtappen.

In het privacybeleidsdocument is aandacht besteed aan de inrichting en het functioneren van een 'team datalekken' alsmede op de verantwoordelijkheden van de FG bij het afhandelen en evalueren van datalekken. In de praktijk is er, zo blijkt uit interviews, een werkende procedure datalekken, maar deze was ten tijde van het veldwerk nog niet op papier vastgelegd. Na de zomer is dat alsnog gebeurd.

2.2 Leren en verbeteren

In het *Beleidsdocument informatiebeveiliging* wordt ruim aandacht besteed aan personele aspecten, de maatregelen die nodig zijn om de medewerkers veilig te laten omgaan met persoonsgegevens en wie daarvoor verantwoordelijk is. Bewustwording en periodiek agenderen in werkoverleggen maakt daarvan onderdeel uit. In de nota *Privacybeleid* zijn in een apart hoofdstuk bewustwording en training genoemd als belangrijke voorwaarden voor het slagen van privacybescherming.

Vanaf eind 2017 is gewerkt aan het overbrengen van kennis over de AVG aan medewerkers en bewustwording van het belang van bescherming van persoonsgegevens inherent aan integere dienstverlening. Concreet zijn er organisatiebrede workshops I-bewustzijn gegeven en hebben medewerkers een e-learning module over informatiebeveiliging moeten volgen. Met de komst van de CISO en de FG in april jl. is de training geïntensiveerd. Zo is de FG per afdeling in gesprek met medewerkers over de betekenis van privacy en wat dat concreet betekent voor de uitvoering van de werkprocessen. De medewerkers worden in deze sessies uitgedaagd om vragen te stellen en in discussie te gaan. Dit heeft geleid tot een informatiepagina op het intranet over privacy die onder andere Frequently Asked Questions (FAQ's) bevat. Daarnaast ontwikkelen de FG en CISO een nieuwe e-module specifiek gericht op privacy. Deze moet in het najaar door de medewerker worden gevolgd. Nieuwe ontwikkelingen (landelijk en eigen beleid) worden consequent door de FG bij de afdelingen over het voetlicht gebracht. Volgens de FG en de CISO leeft het onderwerp en wordt het serieus genomen.

Privacy moet tot de kernwaarden van de organisatie gaan behoren (*Privacybeleid*) en de gemeente wil in control zijn (*Beleidsdocument informatiebeveiliging*): weten welke maatregelen genomen moeten worden, een planning daarvoor hebben en het geheel verankeren in een PDCA-cyclus. De gemeente is voor de komst van de AVG al begonnen met het uitvoeren van risicoanalyses en het nemen van beveiligingsmaatregelen.
Medewerkers zijn al eerder in aanraking gekomen met de verplichting zorgvuldig met persoonsgegevens om te gaan. Bijvoorbeeld door middel van de eed/belofte die nieuwe medewerkers bij hun indiensttreding afleggen of door algemene geheimhoudingsverklaringen. Voor specifieke systemen (Basisregistraties, Suwinet) gelden aparte procedures en moet ook een aparte verklaring worden getekend. Ook zijn eerder regels gesteld aan 'clean desk'-werken, het werken met gemeentelijke middelen buiten de kantooromgeving, moet e-mail met (bijlagen met) gevoelige informatie versleuteld verstuurd worden en is de werkwijze bij datalekken uitgelegd. Uit het onderzoek blijkt dat deze maatregelen zijn al behoorlijk zijn ingeburgerd. Wel blijft regelmatige herhaling van belang om de maatregelen te laten beklijven. Medewerkers hebben verteld dat zij elkaar er ook op aanspreken als de zorgvuldigheidseisen niet in acht worden genomen.

De trainingen die nu worden gegeven vallen volgens betrokkenen in een vruchtbare bodem. Het bewustzijn en de nieuwsgierigheid zijn er. Dat heeft er bijvoorbeeld toe geleid dat gedurende onze gespreksronde er bij medewerkers nieuwe vragen zijn gerezen over de uitvoering van hun werk. Met name was dit het geval bij de medewerkers sociaal domein. Zij hebben behoefte aan duidelijke werkinstructies voor specifieke stappen in het werkproces. Op het intranet wordt informatie over privacybeleid en informatieveiligheid gepubliceerd. Aldaar worden ook FAQ's – en de antwoorden daarop - bijgehouden.

Naast de vragen op de FAQ-lijst spelen er regelmatig ook complexere vraagstukken, bijvoorbeeld het gebruik van toestemming of de zelfredzaamheidsmatrix binnen het sociaal domein of privacyaspecten bij flexibel werken. Op ad hoc basis worden deze vragen opgepakt (ook met gespecialiseerde functionarissen van de gemeente buiten het sociaal domein), maar is er nog geen gestructureerde aanpak om beleid te formuleren voor deze kwesties. Naar verwachting wordt dat begin van 2019 gerealiseerd.

Voor het werken met vitale systemen zoals de BRP en het Suwinet zijn er voorschriften en wordt er gecontroleerd op naleving door middel van log-bestanden. Daarnaast vinden voor deze systemen aparte onderzoeken (audits, zelfevaluaties) plaats naar beveiliging en gebruik. Ook zijn er autorisatieformulieren voor deze processen/systemen waar ook wordt ingegaan op de (privacy)regels met betrekking tot het gebruik van het systeem door medewerkers.

Verder kan worden genoemd dat de gemeente zogenaamde ENSIA-audits uitvoert. Dit is een verantwoordingssystematiek voor een aantal kernregistraties en risicogevoelige systemen. ENSIA ondersteunt gemeenten in het verantwoording afleggen over informatieveiligheid, waarvoor de BIG (Baseline Informatiebeveiliging Nederlandse Gemeenten) de basis verschaft.

Buiten de gangbare aandacht voor vitale systemen en de ENSIA-audits bestond er vooralsnog geen (gemeente-brede) leer- of verantwoordingssystematiek, waarbij er vanuit de directiestaf (stuur)informatie verzameld wordt en het beleid en/of de inspanningen voor het vergroten van bewustzijn en veilig gedrag op basis daarvan wordt aangepast. Deze aanpak is naar verluid gedurende de zomer van 2018 ingericht.

Privacy als onderwerp leeft op dit moment in de organisatie en medewerkers nemen dit onderwerp serieus en tonen nieuwsgierigheid en betrokkenheid. Dit blijkt uit de vele vragen die er bij de FG terecht komen en blijkt ook uit de gesprekken die wij voerden. Na implementatie van de AVG hoort dit punt op de reguliere agenda van de werkoverleggen te komen. Naar mening van de FG dient dit de verantwoordelijkheid van het lijnmanagement te worden.

2.3 Positie van de burgers

In de AVG zijn bepaalde rechten van burgers aangescherpt, zoals het recht op informatie (art. 15 t/m 22 AVG). Burgers moeten van tevoren worden geïnformeerd over het feit dat er gegevens worden opgevraagd, bij welke bronnen, met welk doel dat is, wat ermee gebeurt. Ook moeten burgers duidelijk worden geïnformeerd over onder meer hun recht op inzage, correctie en verwijdering van hun persoonsgegevens en over de bezwaarprocedure. Deze rechten moeten ook daadwerkelijk uitgeoefend kunnen worden. Dat wil zeggen dat de informatie daarover vindbaar en begrijpelijk moet zijn, en dat wordt aangewezen hoe de toegang tot de rechten mogelijk is: waar kan ik mijn gegevens corrigeren, wat moet ik daarvoor doen. Daarnaast moeten de contactgegevens van de FG bekend zijn.

De burger heeft recht op informatie, de gemeente heeft dus een actieve informatieplicht jegens de burger (art. 12, 13 en 14 AVG). Hoe gevoeliger de gegevens des te meer de gemeenten in detail de burger moet informeren over het hoe en waarom van de gegevensverwerking.

De algemene rechten van betrokkenen (recht op informatie) en de algemene informatieplichten van de gemeente zijn opgenomen in het privacybeleidsdocument. Deze is kort na de start van ons onderzoek verschenen. Een concrete uitwerking van de algemene informatieplicht is aangetroffen in de vorm van de *Privacyverklaring* op de website, opgenomen in de rubriek Algemene Informatie - Privacy. Deze privacyverklaring is tijdens het onderzoek door de FG op de website gezet (mei 2018). Ze bevat informatie over de algemene informatierechten van de burger en het emailadres van de FG voor vragen en verzoeken.

Verder zijn er in het *Privacyprotocol kernteams en regieteam* verwijzingen naar de algemene informatierechten van betrokkenen opgenomen. In artikel 15 wordt verwezen naar het recht op informatie, correctie en wijziging cf. 'de wet', dat een schriftelijk verzoek daartoe moet worden ingediend bij 'de verantwoordelijke'. Dat geldt ook voor het indienen van een klacht. Onduidelijk is of dit voor de medewerkers concreet is gemaakt. Verwacht kon worden dat in het *Privacyprotocol* (of in een aparte gedragscode) ook een verwijzing zou staan naar de actieve informatieplicht jegens betrokkene over de gegevensverwerking en over de wijze waarop de medewerkers van het kernteam en regieteam daar invulling aan moeten geven. Zeker gezien het feit dat er in deze teams gegevens over personen, ook bijzondere gegevens, breed worden gedeeld. In de *Samenwerkingsovereenkomst kernteams en regieteam* is wel een verwijzing opgenomen naar geheimhoudingsplicht. Maar verder wordt niet ingegaan op informatierechten van burgers en -plichten van de medewerker.

Sinds mei jl. kan de burger algemene informatie vinden over verwerking van persoonsgegevens door de gemeente op de website onder Algemene Informatie - Privacy - Privacyverklaring.

Gebleken is dat er geen folders of instructies zijn voor het gesprek met de cliënt om hem specifiek te informeren over de gegevensverwerking. Deze verplichting staat niet specifiek genoeg in de documenten, is niet uitgewerkt in instructies en staat (daarom) ook niet op het netvlies van medewerkers met cliënt-contacten.

Medewerkers hebben aangegeven dat 'de cliënt door zijn aanvraag al toestemming heeft gegeven om zijn gegevens te gebruiken'. Hij tekent namelijk een algemene toestemming voor de opvraag van gegevens. Dit is ook zo verwoord in paragraaf 2.2 van het privacybeleidsdocument: 'In het algemeen geldt dat degene die een beroep doet op de gemeente.... door die aanvraag al toestemming verleent voor de verwerking van persoonsgegevens die nodig zijn voor dat doel.' Dit laat onverlet dat de burger ook specifiek geïnformeerd moet worden over de gegevensverwerking die samenhangt met de behandeling van zijn hulpvraag. Overigens wordt ook in het rapport *Privacy Impact Assessment (Jeugdzorg)* geconcludeerd dat met hoge prioriteit het proces zo in te richten dat de cliënt op het juiste moment actief en transparant wordt geïnformeerd en om toestemming wordt gevraagd om gegevens door te leveren (pg. 6 PIA).

De FG is bezig met het ontwerpen van een procedure voor inzagerecht, correctierecht en dergelijke. Het ontwerp is gebaseerd op de procedure die nu voor inzage in de BRP geldt. Inzage in de eigen gegevens is natuurlijk altijd al mogelijk geweest op grond van de Wbp. Het is voor zover bekend bij de medewerkers nog maar een paar keer voorgekomen dat een burger inzage heeft gevraagd. In de

periode 2016-2018 zijn er vier klachten geweest over schending van privacy, waarvan er één gegrond is verklaard en twee ongegrond. Eén is door de klager aan de Nationale Ombudsman voorgelegd.

Perspectief van de betrokkene
Vanuit de *Adviesraad Sociaal Domein* is opgemerkt dat betrokkenen (cliënten) geen informatie krijgen over de gegevensverwerking en hun rechten daarbij. Betrokkenen moeten bij de aanvraag ondertekenen dat ze akkoord gaan met het opvragen en verder verwerken van gegevens. Voor zover bekend wordt daar geen verdere uitleg aan gegeven. Voor betrokkenen is het dan ook niet altijd duidelijk waarom er zoveel gegevens worden opgevraagd. Daarnaast maken zij zich zorgen over het grote aantal medewerkers dat die gegevens te zien of te horen krijgen. Dat begint al aan de telefoon, waar doorgevraagd wordt terwijl betrokkenen soms hun zaken liever alleen bespreken met consulenten. Betrokkenen hebben het gevoel dat hun verhaal door een hele reeks medewerkers gaat voordat de consulent wordt bereikt of er iemand de zaak op zich neemt (of dit gevoel ook altijd klopt is niet geverifieerd in dit onderzoek).

Recent heeft de Adviesraad vragen gekregen uit de achterban over de (proactieve) huisbezoeken van schuldhulpverleners in het kader van vroegsignalering: hoe de gemeente weet dat ze betalingsachterstanden hebben en hoe ze aan hun adressen komt. Dit is kennelijk niet duidelijk aan betrokkenen bekend gemaakt; niet van te voren in algemene zin, niet door de betrokken schuldeiser[3], en niet 'voor de deur'. De Adviesraad is overigens ook niet geïnformeerd over het (nieuwe) privacybeleid van de gemeente en de ontwikkelingen daarin, en wordt ook niet op de hoogte gehouden over de uitvoering en naleving. Zonder deze informatie kan zij haar rol in deze niet vervullen. Overigens kan de Adviesraad ook zelf hierin initiatief nemen.

2.4 De rol en positie van de raad

Privacy en de AVG zijn niet als specifieke onderwerpen in de raad aan de orde geweest. Wel heeft de raad vragen gesteld over de beveiliging van persoonsgegevens door de gemeente: een keer naar aanleiding van algemene berichtgeving in de media over het gebruik van het Suwinet (vragen Partij van de Dieren, 2016) en een keer naar aanleiding van berichtgeving op RTL over een datalek bij de aanbesteding van het leerlingenvervoer (VVD, PvdA, GroenLinks, D'66 september 2017).

Inmiddels zijn de verkiezingen geweest en is de raad van samenstelling gewijzigd. In het 'opleidingsprogramma' voor de raadsleden is privacy niet opgenomen als een apart onderdeel. Vanuit de medewerkers basisregistraties is opgemerkt dat daarin helaas ook geen ruimte is gereserveerd om over de functie van de basisregistraties te informeren. De FG heeft aangekondigd om na de vakantie in een raadsvergadering het onderwerp 'privacy in Pijnacker- Nootdorp' aan de orde te stellen.
Op gezette tijden heeft de raad wel kennisgenomen van diverse ‘formele’ documenten die in het kader van de voorbereiding op de AVG van belang waren. Dat geldt in het bijzonder voor het privacybeleidsdocument, in mei 2018.

Op 11 juli jl. is in het kader van dit onderzoek een discussiebijeenkomst met raadsleden georganiseerd. Aan de hand van een fictieve casus is gesproken over de rol en verantwoordelijkheid

[3] In algemene zin: door een aankondiging de gemeente van de aanpak vroegsignalering, bijvoorbeeld op de website van de gemeente en in het huis-aan-huisblad, in folders voor vindplaatsen. En meer specifiek door de betrokken schuldeiser die de adressen levert: die kan een melding doen in een brief, in een nieuwsbrief, op de website en./of in het contract met de burger. Zie voor de wijze van informeren van de burger over vroegsignalering: Handreiking vroegsignalering schulden en de AVG. PBLQ dec. 2017.

van de raad met betrekking tot het onderwerp privacy. Aandacht is besteed aan zowel de kaderstellende, de controlerende als de volksvertegenwoordigende rollen van de raad.
Uit de bijeenkomst kwam naar voren dat de aanwezige raadsleden, waarvan sommige pas sinds maart zitting hebben in de raad, allereerst behoefte hebben aan meer achtergrondkennis en algemene informatie over privacy en privacybeleid, om zo goede invulling te kunnen geven aan hun verantwoordelijkheden. Tevens is aangegeven dat zij behoefte hebben aan uitgebreider inzicht in de uitvoering van het beleid. De bijeenkomst is afgesloten met de conclusie dat de raad gevoed moet worden met informatie vanuit de gemeentelijke organisatie, maar ook zelf initiatief moet nemen om dit onderwerp te agenderen en te volgen.

3. Conclusies en aanbevelingen

3.1 Beantwoording van de onderzoeksvragen

Binnen de gemeente Pijnacker-Nootdorp was de afgelopen jaren al sprake van kennis over en aandacht voor privacy en informatiebeveiliging. De kennis over privacy was echter vooral geconcentreerd bij enkele functionarissen en de aandacht, voorschriften en instrumenten waren er slechts bij enkele afdelingen. De direct betrokkenen werden zich meer en meer bewust van het belang en de urgentie om hier bredere aandacht voor te krijgen. In de loop van 2016 heeft het Directieteam van de gemeente de ruimte gecreëerd om privacy en informatiebeveiliging gestructureerd aan te pakken, vooral met het oog op de inwerkingtreding van de AVG per mei 2018. Gedurende 2017 is gewerkt aan de voorbereidingen en eind 2017 is een Plan van Aanpak uitgebracht met de onderdelen die nog voor datum inwerkingtreding afgerond zouden moeten worden. Op dat moment is geconstateerd dat er veel bouwstenen gereed waren of in voorbereiding, maar dat de verbinding daartussen nog gelegd moest worden. Met name het privacybeleid moest nog verder worden ontwikkeld en op papier worden gezet, en de privacy-organisatie moest verstevigd worden. Voor deze taken zijn in april 2018 een FG en een CISO aangesteld, vooralsnog op tijdelijke basis. Deze hebben ervoor gezorgd dat sinds het voorjaar van 2018 er sprake is van de inrichting van coherent gemeentelijk beleid op het gebied van privacy en informatiebeveiliging. Er wordt nu gewerkt aan de vertaling van het beleid naar de praktijk. Er functioneert al een privacy-organisatie. CISO en FG hebben gezamenlijk een concrete werkplanning gemaakt, waarin de nog relevante acties zijn benoemd.

Met het vaststellen van beleid is de gemeente er natuurlijk nog niet. In het onderzoek is geconstateerd dat de vertaling en implementatie van het beleid naar de werkpraktijk nog verbeterd moet worden. Allereerst is geconstateerd dat bepaalde systemen 'open' staan voor alle medewerkers van een team, in plaats van een beperking van de autorisatie tot de behandelend uitvoerder en bijvoorbeeld een teamleider. Het uitvoeren van PIA's staat in de planning; op moment van onderzoek was er alleen voor de uitvoering van de Jeugdwet een PIA uitgevoerd. Er zijn nog geen procesbeschrijvingen die in detail beschrijven wie wanneer welke persoonsgegevens mag verwerken. De verwerkingenregisters moeten nog verder worden ontwikkeld.

Voor de uitvoeringspraktijk moeten er meer handreikingen en instructies komen om richting te geven aan het dagelijks handelen. Zo is uit onze gesprekken gebleken dat door de intensieve overleggen van de FG met de afdelingen, de kennis en het bewustzijn van de medewerkers is vergroot, met als (positief) gevolg dat er steeds vragen rijzen over de praktijk. Dat geldt voor zowel het handelen in het individuele geval van de cliënt, als in casus-overleggen in bijvoorbeeld het kernteam. Ook de informatieverstrekking aan de inwoners over de omgang met persoonsgegevens moet worden verbeterd, zowel op papier (zowel interne procedures voor bijvoorbeeld inzage en correctie, als voor informatie aan burgers) als in de gesprekken van de uitvoerend medewerkers met de burger. Er moet een compleet overzicht worden opgesteld van de nog noodzakelijke verwerkingsovereenkomsten. Deze punten zijn overigens opgenomen in de werkplanning van de FG en de CISO.

De raad is via beleidsdocumenten op verschillende momenten geïnformeerd over het privacy- en informatiebeveiligingsbeleid van de gemeente. Tegelijkertijd geldt dat de raad niet systematisch is betrokken bij dit beleid en evenmin op eigen initiatief hiernaar heeft geïnformeerd. Er heeft geen integrale bespreking en afweging van het beleid in de raad plaatsgevonden.

Deze korte samenvatting verschaft het uitgangspunt voor de beantwoording van de geformuleerde deelvragen in dit onderzoek. Deze antwoorden zijn in onderstaande tabel opgenomen.

Beleid

1.	**Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de juridische borging van de privacy van de inwoners?**
	De gemeente beschikt over verschillende beleidskaders, regels en richtlijnen met betrekking tot de (juridische) borging van de privacy van inwoners. Het belangrijkste beleid op het gebied van privacy is tot stand gekomen als onderdeel van het implementatieproject AVG. Voor specifieke (meer risicovolle) domeinen heeft de gemeente aanvullende regels opgesteld. De procedure voor datalekken is rond de zomer van 2018 pas op papier gezet. Voor de informatierechten van de burger / informatieplicht van de gemeente jegens de burger moet dit nog gebeuren.
2.	**Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Gemeenten (BIG), aan de Wet bescherming persoonsgegevens (Wbp) en vanaf 25 mei 2018 aan de algemene verordening gegevensbescherming (AVG)?**
	In het algemeen voldoet het beleid aan de wettelijke vereisten zoals gesteld in Wbp en AVG. Dat geldt eveneens voor de bepalingen in de BIG. Op onderdelen is een nadere uitwerking en implementatie nog nodig. De samenhang tussen verschillende beleidsonderwerpen ontbrak, maar daar wordt momenteel structureel aan gewerkt.
3.	**Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?**
	In het onderzoek zijn geen uitwerkingen van werkprocessen aangetroffen waarin is beschreven welke persoonsgegevens wanneer en door wie mogen worden verwerkt. PIA's en de verwerkingenregisters staan nog op de planning. Er zijn enkele verwerkersovereenkomsten, een check op compleetheid is noodzakelijk. Op de risicogevoelige systemen zoals BPR en Suwinet vinden geregeld audits plaats. Er zijn autorisatieprocedures, maar wat urgent geregeld moet worden is een strakkere (beperktere) autorisatie voor de systemen in het sociaal domein. Overigens is daar recent door de FG op ingegrepen. Voor de uitvoering, in ieder geval het sociaal domein, zijn ook meer instructies nodig voor de uitvoeringspraktijk.
4.	**Zijn er casussen waarin sprake is van schending van de privacy van inwoners en hoe is daarmee omgegaan?**
	Jaarlijks zijn er enkele kleinere zogenaamde datalekken. Er bestaat een ‘team datalekken’, die reageert op dergelijke incidenten. Ook zijn de verantwoordelijkheden van de FG bij het afhandelen en evalueren van datalekken beschreven. In de praktijk is er een werkende procedure datalekken, die onlangs op papier is vastgelegd. Ook het feit dat sommige systemen 'open' staan is een risico voor schending van de privacy van burgers/cliënten.

Leren en Verbeteren

5.	**Hoe worden medewerkers betrokken bij en getraind in het borgen van de privacy van de inwoners?**
	Medewerkers worden getraind in kennis over de AVG en de betekenis daarvan voor hun werk. Kennisoverdracht gebeurt onder andere door e-learning. De FG houdt per afdeling met medewerkers gesprekken om de vereisten te vertalen naar de uitvoering van hun dagelijks werk. Privacy als onderwerp leeft op dit moment in de organisatie en medewerkers nemen dit

	onderwerp serieus en tonen nieuwsgierigheid en betrokkenheid.
6.	**Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop de privacy van de inwoners is geborgd binnen de gemeente?**
	Mogelijke risico's zitten in het ontbreken van specifieke werkinstructies, enkele 'open' systemen, het niet actief burgers informeren over hun rechten en de tijdelijke aanstelling van de FG en CISO. Voor de laatste twee functionarissen geldt dat zij vervangen moeten worden door een vaste medewerker. Kennisoverdracht en continuïteit zijn cruciaal voor de overdracht en het vasthouden van de belangstelling voor het onderwerp in de organisatie. Deze risico's zijn bekend binnen de organisatie en daar wordt op geanticipeerd.
7.	**Hoe ziet de gemeente erop toe dat de borging van de privacy van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven en juridische ontwikkelingen?**
	Naleving van het beveiligingsbeleid is in de PDCA-cyclus van het beveiligingsbeleid opgenomen en is ook onderwerp van risico-analyses of PIA's die nog in de planning staan. Daarnaast ontwikkelt de FG een privacy kwaliteitsmanagementsysteem. Onderdeel daarvan is een checklist voor het uitvoeren van audits die al worden toegepast. Voor het werken met vitale systemen zoals de basisregistraties en Suwinet worden al langer op gestructureerde wijze controles uitgevoerd op naleving van de vereisten. Het voornemen bestaat dat de onderwerpen privacy en informatieveiligheid regelmatig worden geagendeerd in de reguliere werkoverleggen.

Positie van de burger

8.	**Hoe communiceert de gemeente naar inwoners over de wijze waarop zij omgaat met persoonsgegevens?**
	Sinds mei jl. kan de burger algemene informatie vinden over verwerking van persoonsgegevens door de gemeente op de website onder Algemene Informatie - Privacy - Privacyverklaring. Meer specifieke en gerichte informatie is echter niet beschikbaar. Ook zijn er nog geen instructies voor de medewerkers die met burgers contact hebben.

Positie van de raad

9.	**Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid en informatieveiligheid in het sociaal domein betrokken geweest?**
	De raad is tot nu toe betrokken door het beoordelen/kennis nemen van de verschillende (beleids-)nota's die over dit onderwerp aan haar zijn voorgelegd. De raad wordt geïnformeerd over datalekken. Daarnaast heeft de raad op twee momenten vragen gesteld aan het college over zaken die in de media aan de orde werden gesteld: het gebruik van Suwinet en het datalek bij de aanbesteding van het leerlingenvervoer. De raad heeft geen actieve bemoeienis gehad bij het ontwikkelen van het privacybeleid en het controleren daarvan.
10.	**Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?**
	De raad heeft de mogelijkheid om te sturen door de (beleids)nota's over dit onderwerp te beoordelen en achteraf te controleren via verantwoordingsrapportages voor zover het onderwerp privacy daarin aan de orde komt. Het ontbreekt de raad op dit moment nog aan concrete handvatten: kennis, inzicht in de ontwikkelingen die binnen de gemeente plaatsvinden en informatie over naleving. Raadsleden hebben aangegeven op dit onderwerp bijgeschoold te willen worden en over het onderwerp structureel geïnformeerd te willen worden om hun taken

te kunnen uitvoeren.

3.2 Conclusies

In de voorgaande hoofdstukken zijn de bevindingen verwoord en van context voorzien. Dit verschafte de basis voor de beantwoording van de onderzoeksvragen. Vervolgen toetsen wij nu de bevindingen aan het normenkader dat voorafgaand aan het onderzoek is vastgesteld door de Rekenkamercommissie. Het normenkader is gebaseerd op wettelijke eisen en uitgangspunten en de voorschriften zoals die door de gemeente in het lokale beleid zijn vastgelegd. Onze bevindingen hebben voornamelijk betrekking op de periode voor juni 2018. Vermeld moet worden dat aan het eind van de onderzoeksperiode de CISO en FG in dienst zijn gekomen en hebben gezorgd voor een versnelde aanpak van zaken die nog geregeld moesten worden.

GEMEENTELIJK BELEID

Gestelde Norm	Beoordeling
Het gemeentelijk beleid voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld: generiek aan de AVG, en specifiek voor de genoemde materiewetten.	Deels positief
In het gemeentelijk beleid wordt ingegaan op: • Juridische aspecten op basis van de AVG en de materie wetten zoals: Suwi (en onderliggende regelgeving), Participatiewet, Wmo, Jeugdwet, Wet gemeentelijke schuldhulpverlening. • Vertaling naar de beleidskaders privacy. • Organisatie, taken en verantwoordelijkheden. • Inrichting werkprocessen. • De toepassing van informatiesystemen en ICT. • De gegevens- en informatiestromen. • De positie van en communicatie met de burger.	Deels positief
De gemeente hanteert landelijke standaarden, zoals de Baseline Informatiebeveiliging Gemeenten, routering via het GGK e.d.	Positief
De gemeente is bekend met de AVG, de impact daarvan en heeft een plan van aanpak voor de noodzakelijke aanpassingen die voor mei 2018 gerealiseerd moeten zijn.	Positief
In de procesbeschrijvingen en instructies (waaronder sociaal domein) is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag.	Neutraal
De gemeente heeft beleid voor incidenten waarbij sprake is van schending van de privacy van inwoners. Dit beleid voldoet aan de wettelijke vereisten.	Neutraal

Met het traject dat de gemeente heeft ingezet voor de implementatie van de AVG is het beleid over het algemeen op orde, maar er missen nog een aantal elementen. Zo is er (nog) geen sprake van een samenhangend privacybeleid en een volledig uitgewerkte systematiek om de bescherming van persoonsgegevens te beheersen en borgen. Dit resulteert in een neutrale tot positieve beoordeling ten opzichte van de normen.

Het beleid kan nog meer uitgewerkt en gedetailleerd worden op het gebied van materiewetten en procesbeschrijving. Het systeem van beleid, werkprocessen, systemen, autorisaties, controle, informatierechten en -plichten is nog niet dekkend voor de gehele gemeente en evenmin volledig sluitend. De gemeente moet nog veel PIA's uitvoeren, dat zijn belangrijke bouwstenen in zo'n systeem. Als laatste is er pas sinds kort een formeel vastgestelde procedure voor de afhandeling van datalekken, hoewel er in de praktijk al geruime tijd een werkende procedure bestaat.

LEREN EN VERBETEREN

Norm	Beoordeling
De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in / er aandacht besteed wordt aan het onderwerp privacy.	Positief
De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt.	Neutraal
Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen en persoonsnamen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt.	Deels positief
Het controleplan sluit aan op het gemeentelijk beveiligingsplan en op het Integriteitsbeleid.	Deels positief
In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.	Positief
De medewerkers zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens (waaronder het privacybeleid het sociaal domein).	Positief
De gemeente heeft een routine voor het meten en verbeteren van de bescherming persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd.	Deels positief

De gemeente beschikt pas kort over een gestructureerde leer- en verbetercyclus, hetgeen leidt tot de neutrale beoordeling op deze norm.

De beoordeling van de overige normen is overwegend positief. De gemeente kent de nodige initiatieven om het personeel te trainen in het belang van privacybescherming en informatieveiligheid, bijvoorbeeld door middel van een e-learning module voor informatiebeveiliging (en in tweede helft 2018 voor privacy) en presentaties en/of discussies over privacy en de AVG. In de gemeente is daarnaast ruimte om privacy-vraagstukken te bespreken en in gevallen te beleggen bij de juiste functionarissen (zoals juristen en de FG). Een gestructureerde en expliciete afweging met betrekking tot deze vraagstukken en een koppeling met het beleid is niet aanwezig, maar dit vindt nu nog ad-hoc plaats.

Er bestaan controleplannen voor vitale systemen zoals de BRP en Suwinet. De CISO werkt aan uitbreiding van deze procedures over alle gegevensverwerkingen binnen de gemeente. De hele PDCA-cyclus wordt daarmee inzichtelijk. Zonder een dekkend systeem van verantwoording en bijsturing kan niet worden vastgesteld of er wordt gehandeld conform het beleid (en de AVG).

Voor de basisregistraties en Suwinet zijn procedures (autorisatie, gegevensverwerking, controle) goed geregeld en ook ingesleten. Controle en onderzoek op naleving laat zien dat in deze domeinen conform de vereisten wordt gewerkt en/of dat verbeterpunten geborgd zijn.

Van een aantal systemen is bekend dat deze geen strak ingeregelde autorisaties hebben, maar dat alle dossiers toegankelijk zijn voor het hele team of de hele afdeling.

Ook moeten de privacyrisico's en maatregelen van werkprocessen nog in kaart worden gebracht en zijn er werkinstructies nodig. De PIA's die hiervoor de basis zouden moeten zijn, zijn echter voor het merendeel nog niet uitgevoerd.

POSITIE VAN DE BURGERS

Norm	Beoordeling
De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.	Neutraal
De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.	Neutraal

Er moet meer aandacht zijn voor de positie van de burger en zijn recht op informatie over de verwerking van zijn persoonsgegevens. De gemeente heeft een algemene privacyverklaring op de website geplaatst waarin de belangrijkste informatie ten aanzien van de rechten van betrokkenen (burgers), zoals contactgegevens, wordt weergegeven. Echter, in hun directe contact met de gemeente worden burgers niet altijd expliciet geïnformeerd over hun rechten. Dit resulteert in de neutrale beoordeling op dit punt.

KADERSTELLENDE EN CONTROLERENDE ROL VAN DE RAAD

Norm	Beoordeling
In de bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.	Neutraal
Bij de ontwikkeling van het gemeentelijk beleid, bijvoorbeeld op het gebied van de decentralisaties in het sociaal domein, heeft privacy als punt op de agenda van de Raad gestaan.	Negatief

De gemeenteraad is tot nu toe ad hoc geïnformeerd over ontwikkelingen in het privacybeleid van Pijnacker-Nootdorp. De raad is niet in de positie gesteld om integraal kennis te nemen van dit beleid en zich daar een mening over te vormen.

3.3 Beantwoording centrale onderzoeksvraag en aanbevelingen

Bij de aanvang van het onderzoek is de volgende centrale onderzoeksvraag geformuleerd:

> ***Hoe is in het licht van de decentralisaties in het sociaal domein en de verdergaande digitalisering de privacy van inwoners juridisch en in de praktijk geborgd en op welke punten behoeft dit eventueel aanpassingen?***

Nu de deelvragen zijn beantwoord en de bevindingen zijn getoetst aan het normenkader kan deze vraag als volgt worden beantwoord:

> *De gemeente Pijnacker-Nootdorp is goed op weg om de privacy van inwoners juridisch en in de praktijk te borgen. Op onderdelen is dat al conform wettelijke vereisten volledig geïmplementeerd. Dit beleid moet nog wel volledig dekkend voor de gehele gemeente worden geïmplementeerd. Verder verdienen de informatievoorziening aan de inwoners en de betrokkenheid van de raad nog aandacht.*

Hieruit zijn de volgende aanbevelingen af te leiden:

- *1 Borg de samenhang in het beleid*
  Zorg voor samenhang in beleid. Maak duidelijk hoe de PDCA-cyclus voor privacy concreet in elkaar steekt. Expliciteer daarbij welke sturingsinstrumenten en -momenten er zijn (bijvoorbeeld in de vorm van rapportages, presentaties, (management)reviews, etc).

- *2 Verbeter de informatie aan burgers, maak werk van de actieve informatieplicht.*
  Verbeter de informatievoorziening aan de burgers. In dat verband kan allereerst worden gewezen op het uitbrengen van een folder in eenvoudige (B1-)taal. Daarnaast moet informatie op schrift worden gegeven voor specifieke procedures, zoals in het sociaal domein of bij het opvragen van eigen gegevens door inwoners uit de BRP. Tenslotte moeten medewerkers met cliënten-contacten worden geïnstrueerd in het actief verschaffen van maatwerk-informatie over de rechten van de betrokkene en op welke manier hun informatie gedeeld wordt. Raadpleeg de Adviesraad Sociaal Domein of cliëntenpanels voor de manier waarop cliënten het beste geïnformeerd kunnen worden.

- *3 Ga in gesprek met burgers / cliënten*
  Investeer actief in het verkrijgen van een goed beeld van ervaringen, vragen en zorgen van burgers met betrekking tot privacy. Ga tevens na wat de gemeente kan doen om daar op een goede manier mee om te gaan. Neem het onderwerp op in cliëntervaringsonderzoeken en bevraag hierover de cliëntenvertegenwoordiging.

- *4 Maak werkinstructies voor de uitvoering*
  Tijdens de gesprekken met medewerkers sociaal domein zijn verschillende vragen gerezen over de wijze waarop in sommige situaties gehandeld moet worden. Licht daarom samen met medewerkers de processen door op privacy-aspecten, breng in kaart waar die vragen leven en borg de antwoorden waar nodig in (specifiek) beleid. Wij bevelen aan om te beginnen met het uitvoeren van PIA's en daarna maatregelen uit te werken en werkinstructies op te stellen of aan te passen. Deze dienen vervolgens geïmplementeerd te worden, bijvoorbeeld door ze toe te lichten tijdens werkoverleggen.

- *5 Regel autorisaties en controle*
  Autorisaties van medewerkers dienen zo strak mogelijk ingeregeld te worden, met de werkbaarheid in acht genomen. De gemeente moet voorkomen systemen volledig open te zetten voor alle medewerkers van een team of afdeling enkel en alleen omdat dit handig is; er moet een duidelijke noodzaak zijn voor ruime autorisaties. De regels voor wie wanneer persoonsgegevens mag inzien moeten duidelijk worden opgenomen in de werkinstructies. Wanneer er noodzaak is voor ruimte in de autorisaties dan is het van belang om de toegang tot informatie periodiek en/of steekproefsgewijs te controleren. Op deze manier kan de naleving van het privacybeleid en de genomen maatregelen getoetst worden.

- *6 Laat zien wat je doet*
  Laat zien waarom privacy belangrijk is en een kernwaarde van de gemeentelijke organisatie is.. Geef aan wat de uitgangspunten van het beleid zijn en hoe het uitgevoerd en gecontroleerd wordt. Maak van dit hele stelsel een begrijpelijk overzicht voor de gemeenteraad, Adviesraad Sociaal

Domein, belangstellende burgers en de eigen medewerkers. Betrek ook op die manier de gemeenteraad bij dit onderwerp.

- *7 Houd privacy levend in de organisatie*
  Houd privacy hoog op de agenda bij medewerkers en maak een plan om dat *gestructureerd* te doen. Dat kan bijvoorbeeld door het onderwerp met enige regelmaat te agenderen in werkoverleggen en daar casussen en ‘lastige situaties’ te bespreken. Of door geplande organisatiebrede opfrisacties. Dat gebeurt nu, in het kader van de AVG, maar moet onderdeel worden van de leer- en verbetercyclus. Het is belangrijk dat medewerkers *automatisch* aan het onderwerp toekomen en dat zij zo ruimte krijgen om hun professionele aanpak te borgen. Zorg dat privacy leeft! Ook een volgroeide boom heeft aandacht nodig.

- *8 Betrek de gemeenteraad*
  Stel de raad in de gelegenheid kennis te nemen van de volle breedte van het privacy- en informatiebeveiligingsbeleid, en geef daarbij aan welke afwegingen er zijn gemaakt, bijvoorbeeld tussen enerzijds het belang van privacy en anderzijds dienstverlening. Ga daarbij vooral in op hoe privacy is geregeld in het sociaal domein en bij andere vitale onderdelen zoals de BRP. Laat zien hoe de 'governance', de privacy-organisatie, werkt. Laat zien hoe de rechten van de burgers zijn geregeld. Maak van zaken aangaande privacy en beveiliging een paragraaf in de bestuursrapportages. Geef de nieuwe raad de gelegenheid zich op dit onderwerp bij te scholen. Geef de raad tevens handvatten voor het invullen van de controlerende verantwoordelijkheden bij het privacybeleid en informatiebeveiliging, in het bijzonder op het sociaal domein.

Bijlage A Lijst van 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
P-wet	Participatiewet
Wgs	Wet gemeentelijke schuldhulpverlening
ENSIA	Eenduidige Normatiek Single Information Audit

Bijlage B Geïnterviewde personen

Naam	Organisatie
L. Hanssen	ENSIA-coördinator (tot 1/4/2018)
J. Poels	Informatiemanager
C. Vreugde	(Interim) FG
C. Deben	(Interim) CISO
E. Weststeijn	Concerncontroller / lid DT
F. van Ravestein	Burgemeester / portefeuillehouder
J.P. Woudstra	Gemeentesecretaris
F. van Manen	Jurist / beleidsmedewerker privacy
A. Koster	Jurist (inkoop-, aanbestedings- en contractmanager
H. van Vliet	Afdelingshoofd RBG
N. van Dam	Teamleider basisregistraties
J. Groenewegen	Gegevensbeheerder BRP
M. van der Scheer	Teammanager Sociaal Domein
C. de Koning J. Arends	Adviesraad Sociaal Domein

Deelnemers mini-Privacy Impact Assessment Vergunningen	
J. van Hemert	Strategisch adviseur, teamleider Ruimte a.i.
H. Roeten	Frontofficemedewerker
G. Stam	Teamleider Milieu/Handhaving
H. van Vliet	Afdelingshoofd RBG

Deelnemers mini-Privacy Impact Assessment Sociaal Domein	
L. Suijker	Teamleider participatie
I. van Gaasbeek	Kwaliteitsmedewerker bedrijfsbureau
M. Dernee	Gedragswetenschapper, lid kernteam
L. de Keijzer	Administratief Medewerker
A. Nandpersad	Consulent W&I

Deelnemers Convergentiesessie	
C. Vreugde	(Interim) FG
C. Deben	(Interim) CISO
F. van Manen	Jurist / beleidsmedewerker privacy
L. Hanssen	ENSIA-coördinator (tot 1/4/2018)
J. Groenewegen	Gegevensbeheerder BRP
L. Suijker	Teamleider participatie
I. van Gaasbeek	Kwaliteitsmedewerker bedrijfsbureau
S. Somai	Directiestaf

De RKC onderzoekt het beleid van de gemeente en kijkt hierbij of de gestelde doelen zijn bereikt, tegen welke kosten en of de regelgeving wordt nageleefd. In het kader van de Algemene Verordening Gegevensbescherming (AVG) merken we het volgende op. Voor het onderzoek zou het soms nodig kunnen zijn persoonsgegevens te verwerken. Mocht dat het geval zijn dan vragen we betrokkenen hiervoor expliciete toestemming. In dit onderzoek zijn, naast een overzicht van geinterviewden geen persoonsgegevens verwerkt.

Bijlage C Bestudeerde documentatie

#	Documentnaam	Versie	Datum
	ALGEMEEN		
	Informatieveiligheid en privacy – voorstel governance (inclusief oplegmemo DT)		14 november 2017
	Privacybeleid	1.0	mei 2018
	Addendum bij het Privacybeleid		2 aug. 2018
	Projectopdracht en -plan Implementatie Algemene Verordening Gegevensbescherming	0.1	6 december 2017
	Beleidsdocument informatiebeveiliging	1.0	november 2013
	Basisniveau informatiebeveiliging	1.0	november 2013
	Informatiebeveiliging: Strategie en beleid	Concept	18 december 2017
	Samenwerkingsovereenkomst kernteams en regieteam	Definitief	11 november 2014
	Privacy-protocol kernteams en regieteam	Definitief	11 november 2014
	Privacy Impact Assessment Jeugdzorg	Definitief	15 februari 2017
	Onderzoek Veilig gebruik Suwinet 2016 (Inspectie SZW)		11 oktober 2016
	Accountantsrapport jaarrekening 2015 t.b.v. de gemeenteraad	Definitief	12 juli 2016
	Accountantsverslag uitkomsten controle en overige informatie 2016, t.b.v. de gemeenteraad	Definitief concept	16 januari 2016
	Controleplan verbijzonderde interne controles 2017	1.1	februari 2017
	Resultaten verbijzonderde interne controles Jeugdzorg	1.0	november 2017
	Resultaten verbijzonderde interne controles Wmo	1.0	september 2017
	PROCEDURES		
	Procedure Autorisatie tot de gemeentelijke voorziening (GBA-V)	2.0	18 augustus 2014
	Procedure Gegevensverwerking (BRP)	3.0	19 juni 2017
	Procedure Verstrekken gegevens aan organen van de gemeente (BRP)	2.0	18 augustus 2014
	Procedure Verstrekken gegevens uit de BRP	2.0	9 mei 2014
	Procedure Verstrekkingsbeperking (BRP)	2.0	18 augustus 2014
	BEWERKERSOVEREENKOMSTEN		
	Bewerkersovereenkomst Metaobjects (leerlichtenadministratie)		
	Bewerkersovereenkomst Inlichtingenbureau	getekend	9 december 2014
	Bewerkersovereenkomst Vecozo	getekend	24 november 2014
	Bewerkersovereenkomst Solviteers	getekend	16 december 2014
	Bewerkersovereenkomst Stichting Jeugdbescherming West		18 december 2015
	Bewerkersovereenkomst Effectory BV	getekend	23 februari 2017
	AUTORISATIEFORMULIEREN		
	Formulier aanvraag thuiswerken met de BRP		
	Formulier autorisaties t.b.v. GBA-V		

Formulier autorisaties Key2Burgerzaken	
GEMEENTERAAD	
Beantwoording vragen raad persoonsgegevens leerlingenvervoer	19 september 2017
Beantwoording vragen raad veiligheid privacy gevoelige informatie	15 maart 2016
Beantwoording vragen uitwerking privacyregels sociaal domein	31 mei 2016
Kennisgeving resultaten veilig gebruik Suwinet 2016	21 december 2017

Bijlage D Gehanteerd normenkader

Normen

Gemeentelijk beleid (onderzoeksvragen 1, 2, 3 en 4)
◥ Het gemeentelijk beleid voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld: generiek aan de Wbp/AVG, en specifiek voor de genoemde materiewetten. ◥ In het gemeentelijk beleid wordt ingegaan op: – Juridische aspecten op basis van de Wbp/AVG en de materie wetten zoals: Suwi (en onderliggende regelgeving), Participatiewet, Wmo, Jeugdwet, Wet gemeentelijke schuldhulpverlening. – Vertaling naar de beleidskaders privacy. – Organisatie, taken en verantwoordelijkheden. – Inrichting werkprocessen. – De toepassing van informatiesystemen en ICT. – De gegevens- en informatiestromen. – De positie van en communicatie met de burger. ◥ De gemeente hanteert landelijke standaarden, zoals de Baseline Informatiebeveiliging Gemeenten, routering via het GGK e.d. ◥ De gemeente is bekend met de AVG, de impact daarvan en heeft een plan van aanpak voor de noodzakelijke aanpassingen die voor mei 2018 gerealiseerd moeten zijn. ◥ In de procesbeschrijvingen en instructies (waaronder sociaal domein) is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag. ◥ De gemeente heeft beleid voor incidenten waarbij sprake is van schending van de privacy van inwoners. Dit beleid voldoet aan de wettelijke vereisten.
Leren en verbeteren (Onderzoeksvragen 5, 6 en 7)
◥ De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in / er aandacht besteed wordt aan het onderwerp privacy. ◥ Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan, waarin onder meer staat: hoe dit proces verloopt, de periodiciteit van de controles, wie daarbij betrokken zijn (functienamen en persoonsnamen), wie controles uitvoert, aan wie wordt gerapporteerd, hoe de resultaten worden vastgelegd, wat de criteria zijn voor vervolgstappen, welke de vervolgstappen kunnen zijn en wie die neemt. ◥ Het controleplan sluit aan op het gemeentelijk beveiligingsplan en op het Integriteitsbeleid. ◥ De medewerkers zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens (waaronder aangaande het sociaal domein). ◥ In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming. ◥ De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt. ◥ De gemeente heeft een routine voor het meten en verbeteren van de bescherming persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd.
Positie van de burgers (onderzoeksvraag 8)
◥ De gemeente verschaft aan burgers schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt. ◥ De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.
Kaderstellende en controlerende rol van de raad (onderzoeksvragen 9 en 10)
◥ In de bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles. ◥ Bij de ontwikkeling van het gemeentelijk beleid, bijvoorbeeld op het gebied van de decentralisaties in het sociaal domein, heeft privacy als punt op de agenda van de Raad gestaan.

gemeente Pijnacker-Nootdorp

adres Oranjeplein 1, Pijnacker
post Postbus 1, 2640 AA Pijnacker
telefoon 14 015
e-mail info@pijnacker-nootdorp.nl
internet www.pijnacker-nootdorp.nl

Rekenkamercommissie Pijnacker-Nootdorp
t.a.v. de heer H.A. Lesscher
d.t.k.v. griffie

behandeld door	W.J. Niermeijer	uw brief van		ons kenmerk	18UIT14550	datum	2-10-2018
telefoon	14 015	uw kenmerk		bijlagen	--	verzonden	5-10-2018

onderwerp bestuurlijke reactie op rekenkamerrapport privacy beleid

Geachte heer Lesscher,

Met interesse hebben wij kennis genomen van uw rapport over het privacy beleid in de gemeente Pijnacker-Nootdorp. Wij zijn verheugd over uw beantwoording van de centrale onderzoeksvraag:

> "de gemeente Pijnacker-Nootdorp is goed op weg om de privacy van inwoners juridisch en in de praktijk te borgen. Op onderdelen is dat al conform wettelijke vereisten volledig geïmplementeerd. Dit beleid moet nog wel volledig dekkend voor de gehele gemeente worden geïmplementeerd. Verder verdienen de informatievoorziening aan de inwoners en de betrokkenheid van de raad nog aandacht".

Met belangstelling hebben wij dan ook de beantwoording van de onderzoeksvragen, de conclusies en de aanbevelingen gelezen en onderschrijven in grote lijnen uw betoog. In deze brief geven wij u graag een reactie op de conclusies en aanbevelingen. Wij zullen hierbij de indeling van uw rapport volgen.

U heeft in de periode januari – mei 2018 onderzoek gedaan, bent gekomen tot bevindingen en heeft conclusies getrokken. Wij hebben in die periode hard gewerkt aan onder andere implementatie van de AVG. Uiteraard staat de wereld na mei 2018 niet stil en zijn wij doorgegaan met de uitvoering van het plan van aanpak rond privacy en informatiebeveiliging. Op enkele punten in uw rapport blijkt dan ook dat de door u beschreven situatie niet (meer) de huidige situatie is.

Gemeentelijk beleid
U constateert dat de gemeente Pijnacker-Nootdorp het beleid rond privacy van burgers over het algemeen op orde heeft. U merkt echter op dat de eindsituatie – een samenhangend privacy beleid – nog niet is bereikt. Uw aanbeveling 1 luidt dan ook zorg te dragen voor samenhang in het privacy beleid. In uw rapport maakt u melding van het feit dat wij hier mee bezig zijn. Om deze samenhang te bereiken, hebben wij onder andere een 'Informatie Security Management Systeem' (ISMS) aangeschaft. Verschillende vervolgstappen worden nu uitgevoerd. Dit leidt ertoe dat in het eerste kwartaal van 2019 de samenhang in het beleid optimaal is. Dat u terughoudend bent in uw beoordeling leiden wij af uit de score 'neutraal' op de procedure datalekken. Deze procedure is juni 2018 vastgesteld en hoefde tot op heden nog niet te worden gebruikt.

Leren en verbeteren
Het is prettig te lezen dat de beoordeling op het onderdeel over de scholing van de ambtelijke organisatie overwegend positief is. De leer- en verbetercyclus, met daarin een apart privacy onderdeel, beoordeelt u als 'neutraal'. Omdat wij deze cyclus afgelopen zomer hebben ingevoerd, menen wij ook aan deze norm te voldoen. Uw aanbeveling 4, over het maken van werkinstructies voor de uitvoering, zijn wij aan het implementeren in het AVG werkplan dat in 2019 volledig uitgevoerd zal zijn.

Het levend houden van het onderwerp 'privacy', aanbeveling 7, onderschrijven wij. Wij realiseren ons dat dit punt te allen tijde aandacht behoeft.

Positie van de burgers
Ook bij de conclusie die u trekt ten aanzien van de positie van de burgers speelt het onderzoeksmoment een rol. U komt tot het oordeel dat hier – op het moment van onderzoek – meer aandacht voor nodig was. Een privacyverklaring stond al vermeld op de website, vervolgactiviteiten om inwoners expliciet te informeren over privacyrechten waren er op het moment van uw onderzoek nog niet. Hier is ondertussen mee gestart. Aanbeveling 2 en 3 onderschrijven wij dan ook en voeren wij uit.

Aanbeveling 5 over autorisaties en controle zien wij als een managementvraagstuk. Het gaat om meer dan alleen een ICT oplossing ('dichtzetten van computersystemen'). Het heeft namelijk ook te maken met de inrichting van bedrijfsprocessen. Aanbeveling 5 sluit dan ook aan bij de eerste aanbeveling over samenhang in het beleid. Dit vraagstuk heeft uiteraard onze aandacht.

Kaderstellende en controlerende rol van de gemeenteraad
In de afgelopen jaren hebben wij op verschillende momenten de gemeenteraad geïnformeerd over relevante onderwerpen op privacy beleid. Het is correct dat dit niet gebeurt op basis van een vooraf met de gemeenteraad afgesproken planning. Uw aanbeveling 6 en 8 kunnen bijdragen de gemeenteraad te betrekken bij dit onderwerp. Het is aan de gemeenteraad om aan te geven of men bij geschoold wenst te worden op dit onderwerp. Mocht die wens bestaan, dan zullen wij daar gehoor aan geven. Ditzelfde geldt uiteraard voor de Adviesraad Sociaal Domein en andere gremia.

Pilot ten aanzien van het ambtelijke hoor en wederhoor
Ten aanzien van de wijze waarop u dit onderzoek uit zou willen voeren, heeft u voorgesteld een andere vorm van ambtelijk hoor en wederhoor dan gebruikelijk toe te passen. Uw voorstel was het ambtelijke hoor en wederhoor niet schriftelijk te laten plaatsvinden, maar door middel van het voeren van een open gesprek tussen ambtenaren en het onderzoeksbureau, om te kijken of het onderzoeksrapport geen feitelijke onjuistheden bevat.

Uiteraard staan wij open voor een dergelijke pilot. Wij hebben begrepen dat het gesprek positief is verlopen. Wat echter opviel, was dat het onderzoeksbureau er voor gekozen heeft de antwoorden op de onderzoeksvragen niet te vermelden in de concept rapportage.

Wij vernemen graag uw ervaringen met deze vorm van ambtelijk hoor en wederhoor en zijn benieuwd of de pilot heeft gebracht wat u wilde bereiken.

Conclusie
De aanbevelingen in uw rapport zijn in lijn met het beleid dat wij voorstaan. Op enkele punten in het rapport zijn wij nog bezig de beoogde doelen te realiseren. Wij danken u voor het uitgevoerde onderzoek, waarmee wij bevestigd zien dat wij op de goede weg zijn.

Hoogachtend,
het college van Pijnacker-Nootdorp,

de secretaris,

drs. J.P.R. Woudstra

de burgemeester,

mw F. Ravestein

Rekenkamercommissie **Pijnacker-Nootdorp**

bezoek Oranjeplein 1, 2641 EZ Pijnacker

post Postbus 1, 2640 AA Pijnacker

telefoon 14 015

e-mail info@pijnacker-nootdorp.nl

internet www.pijnacker-nootdorp.nl