Rekenkamercommissie **Pijnacker-Nootdorp**

November 2020

Privacy en informatieveiligheid

Vervolgonderzoek naar de omgang met privacy en de beveiliging van informatie door de gemeente

Voorwoord

Beste lezer,

In 2018 liet de Rekenkamercommissie Pijnacker-Nootdorp (RKC) rondom de invoering van de AVG een onderzoek uitvoeren naar het privacy- en informatieveilgheidsbeleid van de gemeente. Hier kwam uit dat er in de voorgaande jaren al sprake was van kennis over en aandacht voor privacy en informatiebeveiliging. Het beleid was op papier op orde en het traject voor invoering van de AVG was ingezet. Wel werd geconstateerd dat er nog een aantal elementen misten of verbeterd konden worden. In de afgelopen twee jaar heeft de gemeente hieraan gewerkt.

In het kader van opvolging ligt nu voor u een vervolgonderzoek naar de omgang met privacy en informatieveiligheid. Tussen april en september 2020 heeft onderzoeksbureau PBLQ, in opdracht van de RKC, onderzocht welke stappen de gemeente heeft gezet. Daarbij is vooral gekeken naar of, en zo ja, hoe de aanbevelingen uit 2018 zijn opgevolgd.

Het uitgevoerde onderzoek laat zien dat de gemeentelijke organisatie hard aan de weg heeft getimmerd; de omgang met persoonsinformatie en het privacybeleid zijn goed op orde. Op veel plaatsen staan de spreekwoordelijke seinen op groen. Tegelijk heeft de RKC ook zes nadere aanbevelingen geformuleerd, die na wederhoor door het college van B&W niet zijn aangepast. Deze luiden als volgt:

1. Maak het toelichten en benadrukken van privacy en informatieveiligheid een expliciet onderdeel van het inwerkprogramma van nieuwe medewerkers;
2. Blijf de communicatie naar inwoners via de website, middels folders, op het gemeentekantoor en in contacten met inwoners continu verbeteren. Ga daarbij ook in gesprek met (vertegenwoordigers van) inwoners om er achter te komen welke vragen er bij hen leven, om de communicatie-uitingen daar op aan te passen;
3. Verkrijg routine in het uitvoeren van ‘privacy-impact assessments’ (PIA’s) door meer PIA’s uit te voeren. Begin daarbij met de processen waar veel en/of gevoelige persoonsgegevens verwerkt worden;
4. Geef de eigenaren van de betreffende processen een rol bij de planning en totstandkoming van de PIA’s;
5. Houdt standaard een PIA bij nieuwe of veranderende wet- en regelgeving en/of uitvoeringsprocessen;
6. Voer de ‘check’ en ‘act’ fase, gericht op het evalueren en bijstellen van beleid, gestructureerder en explicieter uit. Geef dit voor privacy en informatiebeveiliging handen en voeten door de privacy-risico’s die in uitgevoerde PIA’s zijn geïnventariseerd centraal te stellen.

De Rekenkamercommissie bedankt onderzoeksbureau PBLQ, het college van B&W en de ambtelijke organisatie voor de goede samenwerking bij de totstandkoming van het onderzoek. Tevens spreekt de commissie de hoop uit dat de uitkomsten van het rapport zullen bijdragen aan het verder verbeteren van de omgang met privacy en de beveiliging van persoonsinformatie.

Namens de Rekenkamercommissie Pijnacker-Nootdorp,

Sigrid Bueving
voorzitter

PBLQ

Quickscan Privacy en Informatieveiligheid

project 7181
versie 1.0
9 oktober 2020

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

In 2018 heeft PBLQ onderzoek gedaan voor de Rekenkamer Pijnacker-Nootdorp (hierna: Rekenkamer) naar het privacybeleid van deze gemeente. In die rapportage (hierna: Rapport 2018) is geconstateerd dat het relevante privacy- en informatiebeveiligingsbeleid van de gemeente voldeed. Tegelijkertijd was er sprake van een aantal voornemens waarvan in het stadium van het toenmalige onderzoek niet vastgesteld kon worden of de gemeente daar adequaat invulling aan zou gaan geven. Er was verder sprake van nog enkele tekortkomingen in het beleid. Zowel met het oog op de geconstateerde tekortkomingen als op de toekomstige eisen die aan het beleid zouden worden gesteld, is de toenmalige rapportage afgesloten met verschillende aanbevelingen.

Aan het begin van 2020 heeft de Rekenkamer aan PBLQ gevraagd een vervolgonderzoek uit te voeren naar de opvolging van de aanbevelingen van het rapport uit 2018 in de vorm van een Quickscan.

1.2 Opdrachtformulering

Deze Quickscan richt zich op de vraag in hoeverre de gemeente Pijnacker-Nootdorp daadwerkelijk invulling heeft gegeven aan de toenmalige voornemens. Daarnaast is in het onderzoek vastgesteld in welke mate opvolging is gegeven aan de door de rekenkamercommissie geformuleerde aanbevelingen. Tevens is het relevant om te toetsen of de gemeente adequaat heeft geanticipeerd op nieuwe eisen die op diverse beleidsterreinen zijn gesteld aan het privacybeleid van de gemeente.

De doelstelling van de quickscan is als volgt geformuleerd:

> *De rekenkamercommissie wil inzicht krijgen in de wijze waarop invulling is gegeven aan de adviezen betreffende de beveiliging en gegevensbescherming van persoonsgegevens uit 2018 en waar nog ruimte voor verbetering zit.*

Het onderzoek richt zich op drie thema's, namelijk:

- het actuele **beleid** van de gemeente met betrekking tot de bescherming van persoonsgegevens;
- de wijze waarop **uitvoering** wordt gegeven aan dit beleid;
- de **cultuur** binnen de organisatie met betrekking tot de bescherming van persoonsgegevens.

Met het oog op deze thema's is de volgende centrale probleemstelling voor de quickscan opgesteld:

Centrale probleemstelling

Hoe is in het licht van de adviezen van 2018 de privacy van inwoners geborgd zowel in juridische, beleidstechnische en culturele zin en op welke punten behoeft dit eventueel aanpassingen?

Deze probleemstelling is uitgewerkt in de volgende deelvragen:

Deelvragen
Beleid
1. in hoeverre zijn de relevante beleidsvoornemens (voortkomend uit de aanbevelingen uit het onderzoek, de eigen voornemens van de gemeente of nieuwe wet- en regelgeving) opgenomen in het beleid van de gemeente?
Uitvoering
2. In hoeverre wordt in de dagelijkse uitvoeringspraktijk van de gemeente gevolg gegeven aan de relevante beleidsvoornemen; in hoeverre is deze uitvoering geborgd in procedures, werkinstructies en overige afspraken; 3. In hoeverre wordt het privacybeleid meegenomen bij het uitvoering geven aan nieuwe werkprocessen?
Cultuur
4. Op welke manier is privacy als kernwaarde in de cultuur van de organisatie verankerd? 5. 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? 6. Hoe wordt er intern en naar inwoners gecommuniceerd over privacy?

1.3 Aanbevelingen 2018

Het onderzoek richt zich, zoals eerder beschreven, onder meer op de aanbevelingen uit het rapport uit 2018. Ook deze zijn te ordenen aan de hand van de drie thema's in het onderzoek; beleid, uitvoering en cultuur. Dit geeft het volgende beeld:

Aanbevelingen uit het Rekenkameronderzoek 2018
Aanbevelingen met betrekking tot beleid
◥ 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.
Aanbevelingen met betrekking tot de uitvoering van beleid:
◥ Verbeter de informatie aan burgers, maak werk van de actieve informatieplicht ◥ 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. ◥ Licht 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 zogenaamde Privacy Impact Assessments (PIA's') en daarna maatregelen uit te werken en werkinstructies op te stellen of aan te passen. ◥ Regel autorisaties en controle. Autorisaties van medewerkers dienen zo strak mogelijk ingeregeld te worden, met de werkbaarheid in acht genomen.
Aanbevelingen met betrekking tot de cultuur in de organisatie m.b.t. de bescherming van persoonsgegevens:
◥ Laat zien waarom privacy belangrijk is en een kernwaarde van de gemeentelijke organisatie is. ◥ 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. ◥ 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.

1.4 Referentiekader

Ook in dit opvolgingsonderzoek heeft de rekenkamercommissie een normenkader gehanteerd, om daarmee de bevindingen mee te beoordelen. Dit is het volgende:

Normenkader
Beleid
◥ De gemeente heeft verschillende beleidskaders, regels en richtlijnen met betrekking tot de (juridische) borging van de privacy van inwoners aantoonbaar aangepast conform de AVG. Voor specifieke (meer risicovolle) domeinen heeft de gemeente aanvullende regels opgesteld. ◥ In de verschillende beleidskaders 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 gemeente hanteert landelijke standaarden, zoals de Baseline Informatiebeveiliging Gemeenten. ◥ 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 en hoe en wanneer vastgestelde processen worden geëvalueerd en aangepast.
Uitvoering
◥ 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. ◥ 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. ◥ De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling. ◥ 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.
Cultuur
◥ De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens en worden van aanpassingen op de hoogte gehouden. ◥ In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk privacybeleid na te leven.

1.5 Werkwijze

Het onderzoek is begonnen met een startbijeenkomst met de direct betrokken ambtenaren.[1] In deze bijeenkomst is ingegaan op de inrichting van het onderzoek en zijn afspraken gemaakt over het verkrijgen van de relevante documenten en het interviewen van de relevante functionarissen.

[1] Dat betrof de zogenoemde Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG) en de privacy jurist.

Om inzicht te krijgen in het **beleid** hebben wij kennisgenomen van de relevante beleidsdocumenten van de gemeente. Wij hebben ons daarbij specifiek gericht op de vraag hoe de eerder gegeven adviezen zijn verwerkt in het huidige beleid. Deze korte documentenanalyse is aangevuld met een klein aantal gesprekken met functionarissen binnen de gemeente die betrokken zijn bij het opstellen van de relevante beleidsdocumenten en het doorvoeren van de aanpassingen. Een overzicht van de geïnterviewde personen is opgenomen in Bijlage A.

Om inzicht te krijgen in de **uitvoering** is kennisgenomen van relevante werkinstructies en procedures en eventuele andere relevante documenten (zoals verslagen van audits e.d.). Ook deze documentenanalyse is aangevuld met een aantal gesprekken met functionarissen die een rol hebben in het borgen van de uitvoeringspraktijk. Een overzicht van de personen met wie het gesprek is gevoerd, is opgenomen in Bijlage A.

Om zowel meer inzicht te krijgen in de heersende **organisatiecultuur** met betrekking tot privacy als ook om meer inzicht te krijgen in de dagelijkse **uitvoeringspraktijk** hebben wij twee zogenaamde mini-Privacy Impact Assessments (hierna: mini-PIA) in de vorm van een workshop georganiseerd. In deze mini-PIA's wordt de omgang met vertrouwelijke gegevens binnen een proces of werkgebied (met de betrokken functionarissen) geïnventariseerd en beoordeeld. In overleg met de gemeente is gekozen voor de onderwerpen fraudebestrijding en een proces dat voortvloeit uit de Wvggz. De mini-PIA's concentreren zich op beleidsterreinen waar vanwege recente wet- en regelgeving verwacht kan worden dat de omgang met privacygevoelige gegevens is veranderd. De Wvggz is per 1 januari dit jaar in werking getreden. Binnen de bestrijding van fraude zijn verschillende ontwikkelingen gaande. Wij hebben gekeken naar hoe privacy rondom zo'n onderwerp is meegenomen en besproken, zowel intern als in de relatie met inwoners.

1.6 Indeling rapport

Het rapport is als volgt ingedeeld. In de eerstvolgende drie hoofdstukken presenteren we de bevindingen met betrekking tot respectievelijk het beleid, de uitvoering van het beleid en de cultuur. Het onderzoek kijkt daarbij in het bijzonder in hoeverre relevante beleidsvoornemens (voortkomend uit de aanbevelingen uit het onderzoek, de eigen voornemens van de gemeente of nieuwe wet- en regelgeving) zijn ingevuld door de gemeente. Hoofdstuk 2 gaat in op het beleid van de gemeente ten aanzien van de bescherming van persoonsgegevens. Zowel in hoofdstuk 3 (uitvoering van het beleid) als in het hoofdstuk 4 (de cultuur met betrekking tot de bescherming van persoonsgegevens) inventariseren en beschrijven wij hoe in de in de dagelijkse uitvoeringspraktijk van de gemeente gevolg wordt gegeven aan de relevante beleidsvoornemens. Daarbij is tevens van belang in hoeverre de uitvoering is geborgd in procedures, werkinstructies en overige afspraken. Op basis van een beoordeling van de bevindingen formuleren wij in hoofdstuk 5 de conclusies en doen wij tevens enkele aanbevelingen.

2. Het gemeentelijk beleid

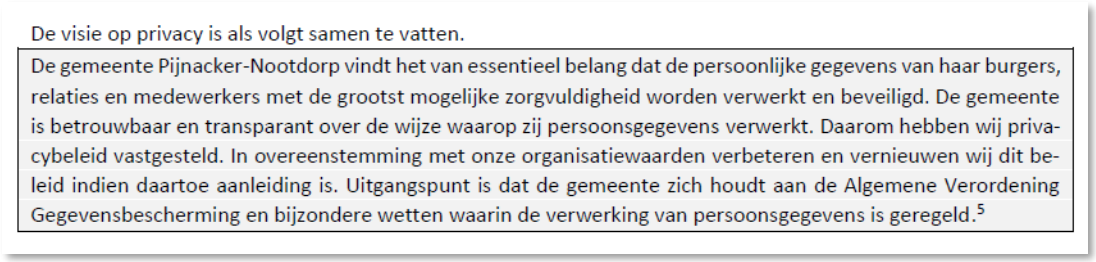
2.1 Inleiding

Het door ons uitgevoerde onderzoek richt zich onder meer op (de ontwikkelingen in) het gemeentelijk beleid. In de desbetreffende deelvraag gaat het er om in hoeverre de relevante beleidsvoornemens (voortkomend uit de aanbevelingen uit het Onderzoek 2018, de eigen voornemens van de gemeente of nieuwe wet- en regelgeving) zijn opgenomen in het huidige beleid van de gemeente. In deze paragraaf wordt verslag gedaan van de relevante bevindingen met betrekking tot het gemeentelijk beleid.

2.2 Bevindingen

De gemeente Pijnacker-Nootdorp heeft sinds 2016 haar aandacht voor privacy en informatieveiligheid structureel opgeschaald. Het privacy en informatieveiligheid-beleid voldeed in 2018 aan de wettelijke eisen en richtlijnen. Voor sommige domeinen was aanvullend beleid geformuleerd.[2] Dit onderzoek richt zich op de ontwikkeling van het privacy en informatieveiligheid-beleid in de periode 2019 tot en met heden. Wij zullen hier toelichten hoe beleid zich sindsdien heeft ontwikkeld, wat de huidige beleidskaders zijn, wat zij inhouden en wat de belangrijkste ontwikkelingen zijn geweest op het gebied van privacy en informatieveiligheid-beleid sinds 2018.

In het privacybeleid is de visie van de gemeente op de bescherming van persoonsgegevens als volgt omschreven:


De visie op privacy is als volgt samen te vatten.

De gemeente Pijnacker-Nootdorp vindt het van essentieel belang dat de persoonlijke gegevens van haar burgers, relaties en medewerkers met de grootst mogelijke zorgvuldigheid worden verwerkt en beveiligd. De gemeente is betrouwbaar en transparant over de wijze waarop zij persoonsgegevens verwerkt. Daarom hebben wij privacybeleid vastgesteld. In overeenstemming met onze organisatiewaarden verbeteren en vernieuwen wij dit beleid indien daartoe aanleiding is. Uitgangspunt is dat de gemeente zich houdt aan de Algemene Verordening Gegevensbescherming en bijzondere wetten waarin de verwerking van persoonsgegevens is geregeld.[5]

Figuur 1 Visie op privacy zoals beschreven in het privacybeleid

Het beleid ten aanzien van privacy en informatieveiligheid wordt onder andere geactualiseerd door de Functionaris Gegevensbescherming (FG) en de Chief information security officer (CISO). De FG is aangesteld om binnen de gemeente toezicht te houden op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). Overheidsinstanties zijn verplicht een FG aan te stellen.[3] Hoewel in dienst van de gemeente, opereert een FG onafhankelijk.

Een CISO concentreert zich met name op het implementeren van informatiebeveiligingsbeleid. De CISO is tevens ENSIA[4]-coördinator. De ENSIA-coördinator houdt zich bezig met het faciliteren en coördineren van het horizontale en verticale verantwoordingsproces voor informatieveiligheid. Het privacybeleid ten aanzien van specifieke domeinen wordt door medewerkers van dat domein

[2] Rekenkamercommissie Pijnacker-Nootdorp, *Privacybeleid – onderzoek naar privacybeleid in Pijnacker-Nootdorp*, oktober 2018, p. 5
[3] Overweging 98 AVG
[4] ENSIA staat voor Eenduidige Normatiek Single Information Audit. ENSIA is een gezamenlijk project van het ministerie van Binneblandse Zaken en Koninkrijksrelaties, de VNG, gemeenten en het ministerie van Sociale Zaken en Werkgelegenheid om de informatieveiligheid te verbeteren.

opgesteld waarbij de FG en de privacy offices ondersteunen. De FG en de CISO ontvangen voor juridische aspecten steun van daarin gespecialiseerde collega's.

De beleidskaders van de gemeente zijn opgesteld in een aantal beleidsdocumenten voor het privacy en informatieveiligheid beleid. De belangrijkste documenten zijn het Privacybeleid gemeente Pijnacker-Nootdorp[5] en het Strategisch Gemeentelijk Informatiebeveiligingsbeleid Pijnacker-Nootdorp '20-'23 [6], waarin de koers voor het beleid voor de komende jaren is uitgezet. Deze documenten zijn vastgesteld door het college van B&W. Wat de raad betreft wordt enkele keren per jaar met de griffier gesproken, mede om te informeren of er vragen leven bij de raad. In april 2019 is er een informatienota aan de raad gestuurd, waarin onder meer verslag is gedaan over de implementatie van de aanbevelingen uit het rekenkamerrapport.

Aan de landelijke standaarden op het gebied van informatiebeveiliging, waaronder de Baseline Informatiebeveiliging Overheid (BIO)[7] en de NEN-ISO/IEC27002:2017, wordt in het informatieveiligheidsbeleid van de gemeente aandacht besteed.[8]

Voor specifieke domeinen heeft de gemeente aanvullend privacybeleid. Binnen het sociale domein zijn er door medewerkers aanvullende documenten opgesteld te bevordering van de privacy. Zo is er bijvoorbeeld voor beeldbellen tussen medewerkers binnen het Sociaal Domein een werkinstructie opgesteld.

Het jaar 2019 was het eerste volle jaar met de AVG. De gemeente heeft in dat jaar verder ingezet op bewustwording met betrekking tot de AVG en de daaraan verwante rechten en plichten.[9] Medewerkers hebben een AVG-training kunnen volgen. Voor medewerkers van het sociaal domein is hierbij gebruik gemaakt van een specifieke methodiek (aangeduid als 'leertuinen-methodiek'). In deze aanpak is benadrukt dat het niet alleen belangrijk is om correct om te gaan met persoonsgegevens, maar dat een dergelijke consequente aanpak ook helpt om het werk efficiënter en beter te maken.

In het privacybeleid is het belang van dit onderwerp onderbouwd. Ook is aangegeven hoe in praktijk invulling wordt (c.q. moet worden) gegeven aan de rechtmatigheid van verwerkingen en welke governancestructuur wordt aangehouden. In het beleid worden met name de uitgangspunten weergegeven zoals die opgenomen zijn in de AVG en wat deze betekenen voor de context waarin de gemeente opereert. Daarnaast wordt duidelijk door middel van het RASCI-model hoe de verantwoordelijkheden zijn verdeeld binnen de organisatie. In zo'n model worden de verantwoordelijkheden onderverdeeld in verschillende rollen, namelijk Responsible, Accountable, Supporting, Consulted and Informed. Zo wordt duidelijk wie de (formele) verantwoordelijkheid draagt, maar bijvoorbeeld ook wie het werk uitvoert en wie over het werk moet worden geïnformeerd. In het privacybeleid wordt ook meermaals verwezen naar informatiebeveiliging en opgemerkt dat informatiebeveiliging en privacy aan elkaar zijn gelinkt, maar dat informatiebeveiliging gaat om het beveiligen van meer dan alleen persoonsgegevens.

Het college, de burgemeester en de gemeenteraad zijn eindverantwoordelijk. Het college van B&W heeft in april het privacybeleid vastgesteld. Vervolgens is de sturing de verantwoordelijkheid van het

[5] Gemeente Pijnacker-Nootdorp, *Privacybeleid gemeente Pijnacker-Nootdorp*, april 2020
[6] Gemeente Pijnacker-Nootdorp, *Strategisch Gemeentelijk Informatiebeveiligingsbeleid Pijnacker-Nootdorp '20-'23*, december 2020.
[7] Gemeente Pijnacker-Nootdorp, *Privacy Jaarrapportage 2019*, p. 3
[8] Gemeente Pijnacker-Nootdorp, Informatiebeveiligingsbeleid BIO Pijnacker Nootdorp 2020-2023, p. 3
[9] Privacy Jaarrapportage 2019, p. 3

directieteam. Afdelingshoofden zijn verantwoordelijk voor de implementatie van de maatregelen en het bevorderen van een bewustwording over privacy binnen hun afdeling[10].

Het beleid met betrekking tot informatiebeveiliging is vastgesteld in het Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2023. Dit document is 'richtinggevend en kaderstellend'. Het beleid wordt aangevuld met tactische beleidsregels. Jaarlijks wordt er een informatiebeveiligingsplan opgesteld op basis van input van de afdelingsmanagers, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van ENSIA.[11] De doelen van het informatiebeveiligingsbeleid gaan verder dan alleen privacyvraagstukken. Het richt zich niet alleen op het beschermen van persoonsgegevens, maar ook op het beschermen van andere gegevens die bijvoorbeeld samenhangen met het beschermen van kritieke bedrijfsprocessen.

Waar eerder de focus lag op de implementatie van de AVG, richt de aandacht zich inmiddels op het optimaliseren van bestaande processen. Ook is er gewerkt aan een verbetering van de samenhang tussen privacy en informatieveiligheid – iets dat ook in het Rapport 2018 werd aanbevolen.

In 2018 was de informatieplicht van de gemeente naar de burger nog niet helder uiteengezet. Op dit moment heeft de gemeente een privacyverklaring op haar website staan die op begrijpelijke wijze uitlegt aan inwoners hoe de gemeente met persoonsgegevens omgaat. In het privacybeleid worden de kaders met betrekking tot de informatieplicht ook adequaat toegelicht. Een en ander is ook opgenomen in een folder die beschikbaar is in de hal van het gemeentehuis.

2.3 Anticiperen op nieuwe wet- en regelgeving

Wet- en regelgeving is altijd aan verandering onderhevig. Dit kan ervoor zorgen dat er nieuwe of andere eisen worden gesteld aan de omgang met persoonsgegevens. Het is daarom belangrijk te anticiperen op veranderingen en die tijdig in te bedden in de organisatie.

Een voorbeeld van recente wetgeving met veel impact op het uitwisselen van (persoons)gegeven is de Wet verplichte geestelijke gezondheidszorg (Wvggz). De Wvggz is in 1 januari 2020 inwerking getreden en regelt de rechten van mensen die te maken hebben met verplichte zorg vanwege een psychische aandoening. Hiervoor moet vaak gevoelige informatie over mensen onder andere met de gemeente worden uitgewisseld. De gemeente heeft hier tijdig op geanticipeerd en een uitvoeringsplan Wvggz opgesteld. Hierin is beschreven wat de verantwoordelijkheid van de gemeente onder de wet is en hoe de gemeente de uit de wet voortkomende taken zal uitvoeren. De mini-PIA die voor de Wvggz is uitgevoerd heeft daarnaast laten zien dat, zelfs met de beperkte ervaring met de uitvoering van de wet (vanwege het lage aantal casussen in de gemeente), de bescherming van (persoons)gegevens een onderwerp is waar ambtenaren van de gemeente en het wijkteam bewust mee bezig zijn. Dit blijkt onder meer uit de zorgvuldige afwegingen die gemaakt worden met betrekking tot ontvangen meldingen en het al dan niet starten van een verkennend onderzoek. Wanneer de gemeente meer ervaring heeft met de uitvoering van de wet is een mogelijk aandachtspunt om te waken voor vermenging van persoonsgegevens die in het kader van de Wvggz verzameld zijn met persoonsgegevens voor andere taken (zoals Wmo of bemoeizorg).[12]

[10] In de uitgevoerde 'mini-PIA's' is gebleken dat zij in de praktijk invulling geven aan die verantwoordelijkheid.
[11] Gemeente Pijnacker-Nootdorp, *Strategisch Gemeentelijk Informatiebeveiligingsbeleid Pijnacker-Nootdorp '20-'23*, december 2019, p. 3
[12] Hier wordt gedoeld op een algemeen risico, zoals onder andere genoemd in de gemeentelijke DPIA Wvggz (VNG). In het onderzoek is niet geconstateerd dat hier sprake van was bij de gemeente.

De praktijkverkenningen die in het kader van deze quickscan zijn uitgevoerd (onder meer door middel van de ‘mini-PIA’s’) laten verder zien dat er binnen de gemeente veel pro-actieve aandacht is voor het belang van privacy- en informatiebeveiliging. Nieuwe wet- en regelgeving worden snel op hun consequenties op deze aspecten onderzocht, en de daaruit voortvloeiende maatregelen worden verwerkt in protocollen en werkinstructies. De aandacht daarvoor is sterk geborgd bij de FG en de CISO, die, mede naar mening van andere werknemers in de organisatie, op ‘activistische wijze’ invulling geven aan hun verantwoordelijkheden voor privacy- en informatiebeveiliging. Deze, positief bedoelde, typering is gebaseerd op de constatering dat deze functionarissen met grote regelmaat bij de overige collega’s aandacht vragen voor privacy- en informatiebeveiliging, geregeld deelnemen aan werkoverleggen binnen de diverse domeinen, om zo de verbinding te leggen tussen de inhoud van het beleid en hun verantwoordelijkheden. Hun inzet draagt er aan bij dat thema’s als integriteit, een zorgvuldige omgang met persoonsgegevens en informatiebeveiliging één of meer keer per jaar onderwerpen van gesprek zijn binnen het MT van de gemeente.

2.4 Tussenbalans

Ter afsluiting van de bevindingen met betrekking tot het actuele gemeentelijk beleid, kunnen de volgende bevindingen worden geresumeerd.

De gemeente is ook na implementatie van de AVG verder gegaan met beleidsontwikkeling met betrekking tot de bescherming van persoonsgegevens. Belangrijk is de vaststelling van het Privacybeleid in april 2020. Daarmee is direct ook gevolg gegeven aan de aanbeveling uit het rekenkamerrapport van 2018, waarin werd gepleit voor het realiseren van samenhang in het beleid. Ook zijn verantwoordelijkheden binnen de organisatie met betrekking tot de bescherming van persoonsgegevens uitgewerkt.

De privacyverklaring op de website is in lijn met een andere aanbeveling uit het Rapport 2018; daarmee is de informatieverstrekking aan de inwoners verbeterd.

In de praktijkverkenningen is gebleken dat de gemeente zich niet alleen bewust is van eisen die nieuwe wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens stelt, maar daar ook direct gevolg aan geeft in de vorm van de aanpassing van protocollen en werkinstructies.

Deze bevindingen schetsen het beeld dat de gemeente relevante beleidsvoornemens adequaat heeft opgenomen in het beleid van de gemeente. De beantwoording van de eerste deelvraag is daarmee:

Deelvraag 1 met betrekking tot het gemeentelijk beleid

Vraag 1	In hoeverre zijn de relevante beleidsvoornemens (voortkomend uit de aanbevelingen uit het onderzoek, de eigen voornemens van de gemeente of nieuwe wet- en regelgeving) opgenomen in het beleid van de gemeente?
Antwoord	De voor de bescherming van persoonsgegevens relevante voornemens, voortkomend uit zowel algemene en actuele wet- en regelgeving, en uit de aanbevelingen uit het rekenkameronderzoek van 2018 zijn in het beleid van de gemeente Pijnacker-Nootdorp opgenomen.

3. De uitvoering van het beleid

3.1 Inleiding

Een zorgvuldige omgang met persoonsgegevens is niet louter gediend met het vastleggen van beleid. In de dagelijkse praktijk moet daar ook uitvoering aan worden gegeven. Dat betreft onder meer de uitwerking van het beleid in procedures, werkinstructies e.d. Ook gaat het om een goed beheer van de wijze waarop functionarissen binnen de gemeente al dan niet toegang hebben tot persoonsgegevens (autorisaties).

Ook aan de beleidspraktijk is in dit onderzoek aandacht besteed. In dit hoofdstuk worden de relevante bevindingen gepresenteerd. Deze zijn vooral gebaseerd op de uitgevoerde interviews en op bevindingen die in de zogenaamde mini-PIA's naar voren zijn gekomen. Vanzelfsprekend is ook ingegaan op de wijze waarop opvolging is gegeven aan de relevante aanbevelingen uit het rekenkameronderzoek 2018.

3.2 Geregelde Privacy Impact Assessments (PIA's)

In de AVG is vastgelegd dat de gemeente verplicht is om zogenaamde Privacy Impact Assessments (PIA) te ondernemen als zij van plan is verwerkingen van persoonsgegevens uit te voeren die een hoog risico op kunnen leveren voor de privacy van personen wiens gegevens worden verwerkt. PIA's zijn relevant om vooraf privacyrisico's te signaleren en mitigeren. Het initiatief tot het doen van een PIA ligt op dit moment vooral bij de FG en daarmee minder bij medewerkers die direct betrokken zijn bij de specifieke verwerking van persoonsgegevens in kwestie.

Binnen de gemeente is er nog geen sprake van een staande praktijk in de uitvoering van een PIA. Eeb vaste opzet om PIA's uit te voeren bestaat nog niet. Als redenen waarom deze praktijk nog niet is uitgekristalliseerd wordt genoemd dat in de afgelopen periode de werkdruk in de relatief kleine organisatie van de gemeente Pijnacker-Nootdorp[13] dusdanig hoog is geweest, dat er geen tijd is geweest om dit uit te werken. Wel wordt er al jaarlijks een planning gemaakt waarin de uit te voeren PIA's worden meegenomen. Deze planning wordt besproken met de diverse betrokken managers. Enkele PIA's zijn daadwerkelijk uitgevoerd en ten tijde van de uitvoering van het onderzoek waren er drie conceptrapportages beschikbaar. Uit deze rapportages blijkt een gestructureerde en systematische uitvoering van de PIA's waarin alle relevante onderdelen terugkomen.

3.3 Meten en verbeteren

Het privacy en informatieveiligheid-beleid wordt gemonitord met behulp van een zogenoemde AVG-monitor. De AVG-monitor is een systeem dat actief en consequent informatie verschaft over informatiebeveiliging en privacy. Door die monitorinformatie te verbinden met normen uit de Baseline Informatiebeveiliging Overheid (BIO), het normenkader voor informatiebeveiliging binnen de gehele overheid en de AVG kunnen scores worden bepaald hoe de gemeente presteert op specifieke aspecten. Hierbij wordt gekeken naar: uitvoeren van (D)PIA's[14], gegevensbeheer, gegevensverkeer buiten de EU, Informatiebeveiliging, Informeren van betrokkenen, Meldplicht datalekken, Organisatie,

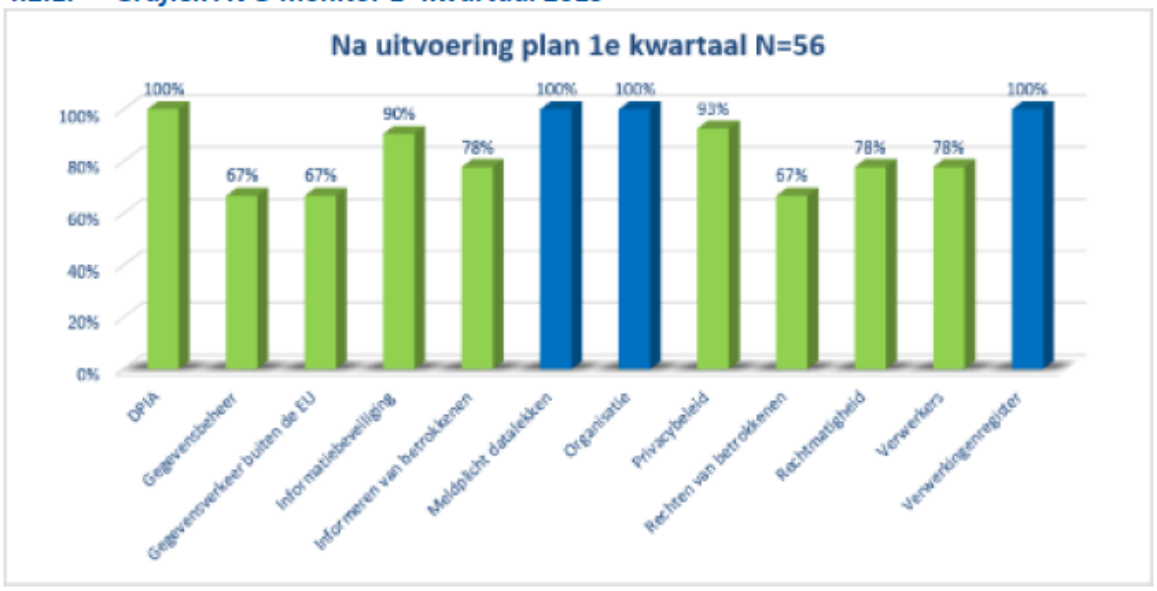
[13] In verhouding tot gemeenten met een min of meer vergelijkbaar inwoneraantal is de ambtelijke organisatie van Pijnacker-Nootdorp relatief klein.

[14] Binnen het vakgebied van privacy- en informatiebeveiliging wordt zowel gesproken over PIA's (Privacy Impact Assesment) als DPIA's. Die laatste afkorting staat voor Data Protection Impact Assessment; het betreft het geregeld doen van controles op de beveiliging van informatiesystemen.

Privacybeleid, Rechten van betrokkenen, Rechtmatigheid, Verwerkers en het Verwerkersregister. Deze categorieën worden op basis van audits en monitoren gescoord. Deze scores worden structureel elk kwartaal besproken met de afdelingshoofden en de stafgroep.

In onderstaande figuur is een voorbeeld van resultaten zoals die opgenomen zijn in de AVG-monitor weergegeven. De bevindingen zijn gebaseerd 56 beheersmaatregelen, die zich vervolgens weer laten aggregeren naar de 12 AVG-onderwerpen die op de horizontale as zijn vermeld. De vermelde procentuele score geeft aan hoe ver de implementatie van de beheersmaatregelen is gevorderd. Geregeld is er op onderdelen al sprake van een 100% score. Dat betekent dat bij dit specifieke onderwerp alle beheersmaatregelen zijn geïmplementeerd. Dat neemt niet weg dat er nog steeds aandacht nodig is om ervoor te zorgen dat die hoge score gehandhaafd blijft. Anders gezegd, bij een score van 100% is de gemeente niet 'klaar'. Dit besef is overigens bij de direct betrokkenen goed aanwezig, maar mensen die meer op afstand staan zouden wellicht wel de indruk kunnen krijgen dat een en ander geen aandacht meer behoeft. Hieraan zou nadrukkelijker in de controles en de jaarrapportages aandacht kunnen worden besteed.

4.2.1. Grafiek AVG-monitor 1e kwartaal 2019



Figuur 2 Voorbeeld van grafiek afkomstig uit de AVG-monitor

Gedurende de bespreking van de uitkomsten uit de AVG-monitor wordt eveneens ingegaan op de ontwikkelingen. Ook dat bevordert de aandacht voor dit thema.

3.4 Externe informatie en communicatie

Aan de inwoners wordt informatie over privacy verschaft via de website, waar onder andere het privacyreglement is vermeld. Hierin wordt uitgelegd hoe er met persoonsgegevens wordt omgegaan zonder het gebruik van jargon. Wanneer de gemeente persoonsgegevens verwerkt wordt de inwoner daarvan op de hoogte gesteld. Dit kan schriftelijk zijn of door middel van een gesprek. Indien dit mondeling gaat, wordt er in het dossier hiervan een aantekening gemaakt.

De gemeente ontvangt soms verzoeken van betrokkenen om inzicht in de verwerking van hun persoonsgegevens. Dit gebeurt niet vaak, en als het gebeurt is het vaak omdat er iets anders aan de hand is.

Er ligt een privacyfolder in de hal van het gemeentehuis. Voor medewerkers in het sociaal domein is een passage over privacy opgenomen in de gespreksinstructies. Het sociaal domein werkt aan een folder specifiek op dat domein gericht waar privacy ook wordt meegenomen. Op langere termijn heeft men de ambitie om ook meldingen te doen over privacy op de schermen in het stadskantoor en als mensen telefonisch contact opnemen met de gemeente. Hoewel inhoudelijk de melding gereed is, leent de huidige techniek van het telefonisch systeem zich er niet voor om deze eenvoudig in de welkomstboodschap op te nemen. Implementatie zal plaatsvinden na aanschaf van een nieuw systeem. Op de website van de gemeente wordt nog niet verteld over hoe de gemeente om gaat met nieuwe technologieën of grootschalige dataverwerkingen. In de toekomst is dit wel een ambitie.

3.5 Autorisatiebeleid

Voor een betrouwbare omgang met persoonsgegevens is het van belang dat medewerkers alleen toegang hebben tot gegevens die voor de uitvoering van hun taak van belang zijn. Dit wordt geregeld via het zogenaamde ‘autorisatiebeleid’. Daarin is vastgelegd welke medewerkers toegang hebben tot welke gegevens. Om allerlei redenen veranderen met grote regelmaat de autorisaties. Medewerkers kunnen van functie veranderen, of andere accenten leggen in hun bestaande functie. Dit vereist daarmee permanente aandacht. De verantwoordelijkheid daarvoor ligt bij afdelingshoofden en teamleiders, die immers overzicht hebben over de werkzaamheden die hun medewerkers verrichten, en welke persoonsgegevens daarvoor relevant zijn. Voorts zijn de datasystemen van de gemeente dusdanig ingericht, dat vooraf al is bepaald welke medewerkers toegang hebben tot welke informatie. De actualiteit van de toegangsrechten van de diverse medewerkers wordt geregeld getoetst. In het bijzonder in het sociaal domein bij het gebruik van Suwinet. Indien wordt geconstateerd dat medewerkers toegang hebben willen krijgen tot gegevens waarvoor zij niet geautoriseerd zijn, wordt actief bij deze medewerkers navraag gedaan om welke redenen zij dat hebben gedaan.

3.6 Actualisatie van beleid

Beleid is altijd in verandering, onder meer vanwege wijzigingen in landelijke wet- en regelgeving. Maar ook kan de dagelijkse uitvoering van beleid specifieke knelpunten aan het licht brengen, waarvoor aanpassingen nuttig en nodig zijn.

Binnen het MT van de gemeente bestaat de ambitie om systematisch te werken aan het aanpassen en verbeteren van het beleid. De systematiek is gebaseerd op de binnen managementtheorieën gebruikelijke PDCA-cyclus.[15] Door deze aanpak is geborgd dat er tijdig aandacht is voor eventuele aanpassingen in het beleid, zij het vanwege veranderde wet- en regelgeving of vanwege inzichten die tijdens de uitvoering van het beleid worden gedaan. De gemeente beoogt om deze cyclus integraal en gemeentebreed toe te passen, en daarbij alle verschillende risico’s en aandachtsgebieden in acht te nemen. Het spreekt voor betrokken managers daarom voor zich dat zij daarbij ook eventuele aanpassingen met betrekking tot de bescherming van persoonsgegevens en informatiebeveiliging meenemen; mochten zij dat niet uit eigen beweging doen, dan zijn zowel de CISO als de FG er alert op om hier alsnog aandacht voor te vragen. Tijdens de mini-PIA over fraudebeleid is daarbij

[15] De letters staan voor de woorden ‘Plan’, ‘Do’, “Check’ en ‘Act’. In dit onderzoek gaat het niet om de kwaliteitsborging binnen de gemeente Pijnacker-Nootdorp. Wel is voldoende aannemelijk geworden dat het MT probeert deze stappen systematisch te volgen en op basis daarvan geregeld reflecteert op het eigen functioneren. In dat verband komt ook de aandacht voor privacy- en informatiebeveiliging aan bod.

aangegeven dat de gemeente in het algemeen nog haar beleid nog beter kan evalueren (de ‘check’ en ‘act’ stap in de cyclus) en werkt aan de verbetering daarvan. Onder andere met het Rapport 2018 en dit opvolgingsonderzoek is dit voor de onderwerpen privacy en informatiebeveiliging in mindere mate van toepassing, omdat hiermee invulling wordt gegeven aan de ‘check’ fase.

3.7 Tussenbalans

In dit hoofdstuk is gebleken dat er tenminste goede en veelal ook concrete voornemens bestaan om uitvoering te geven aan het relevante privacybeleid. In veel gevallen is ook invulling gegeven aan die voornemens, zoals bij het gangbare beleid rond autorisaties en het beschrijven en analyseren van procedures, werkinstructies en afspraken.

Niet in alle gevallen is volledig gevolg gegeven aan wat in het beleid is vastgelegd. Zo is de praktijk rond het op eigen gemeentelijk initiatief uitvoeren van PIA’s nog onderontwikkeld. Binnen de gemeente zijn de betrokkenen zich overigens hiervan bewust. Ter verantwoording dat de praktijk nog niet volledig is uitgekristalliseerd wordt verwezen naar een als hoog ervaren werkdruk. Voor het eerste half jaar van 2020 wordt ook gewezen op de gevolgen van de COVID19-crisis.

Het spreekt voor zich dat in beleidsdomeinen waar veel privacygevoelige gegevens aan de orde zijn (zoals met name het sociaal domein) er ook meer aandacht is voor privacy en informatiebeveiliging. Waar nodig zijn er extra afspraken, zowel in protocollen als werkinstructies. Dat neemt niet weg dat er in andere domeinen voldoende aandacht is voor deze onderwerpen.

Aan de aanbevelingen uit het Rekenkameronderzoek 2018 met betrekking tot de uitvoering van het beleid is in algemene zin wel gevolg gegeven, maar ook daarvoor geldt dat zij niet volledig zijn opgevolgd. Dat betreft met name de aanbeveling om actief te investeren in het verkrijgen van een goed beeld van ervaringen, vragen en zorgen van burgers met betrekking tot privacy. Voor zover is gebleken worden dergelijke ervaringen niet systematisch door de gemeente geïnventariseerd. Zoals hierboven al opgemerkt is zeker wel een begin gemaakt met de aanbeveling dat de gemeente zelf geregeld PIA’s uitvoert. De aanbeveling met betrekking tot het autorisatiebeleid is opgevolgd.

De voor dit hoofdstuk relevante deelvragen kunnen nu als volgt worden beantwoord:

Deelvraag 2 en 3, met betrekking tot de uitvoering van het gemeentelijk beleid

Vraag 2	*In hoeverre wordt in de dagelijkse uitvoeringspraktijk van de gemeente gevolg gegeven aan de relevante beleidsvoornemens; in hoeverre is deze uitvoering geborgd in procedures, werkinstructies en overige afspraken;*
Antwoord	In het algemeen wordt in de dagelijkse uitvoeringspraktijk van de gemeente Pijnacker-Nootdorp goed gevolg gegeven aan relevante voornemens met betrekking tot de bescherming van persoonsgegevens. Op sommige onderdelen kan dit nog vollediger.
Vraag 3	*In hoeverre wordt het privacybeleid meegenomen bij het uitvoering geven aan nieuwe werkprocessen?*
Antwoord	Bij het aanpassen of actualiseren van nieuwe werkprocessen is er steeds aandacht voor privacyaspecten.

4. Cultuur

4.1 Inleiding

Het laatste thema in het onderzoek is hoe de bescherming van persoonsgegevens regulier onderdeel uitmaakt van het dagelijks functioneren van de medewerkers. Ook hiervoor geldt dat de relevante informatie daarover vooral verkregen is uit de interviews en de uitgevoerde mini-PIA's.

4.2 Bewustwording

Bewustwording rondom privacy was in 2019 een van de belangrijkste speerpunten van de FG. Hier wordt op verschillende manieren invulling aangegeven. In 2019 hebben werknemers een cursus over privacy kunnen volgen. Hierdoor hebben de meeste medewerkers informatie ontvangen over de basisaspecten van privacy.

Er is sprake van actieve scholing, en informatieverstrekking, in de vorm van presentaties in de teams en een E-learning module voor de hele organisatie. Het intranet wordt daarnaast volop gebruikt om medewerkers te attenderen op het belang privacy, zoals geïllustreerd in figuur 2 en 3.


Hoeveel 'digitale kopjes koffie' heb jij al gedronken?

[redacted]
FG Functionaris gegevensbescherming Privacy

Zoveel mogelijk collega's werken vanuit huis ten tijde van Corona. We zien een enorme toename aan digitale koffiemomentjes en zien dat we intensiever digitaal zijn gaan (samen)werken. Dat vraagt om zorgvuldigheid. Weet jij hoe je zo veilig mogelijk kunt werken vanuit huis? En hoe zorg je ervoor dat gevoelige data niet in de verkeerde handen valt?

Volg onderstaande tips op om zo veilig mogelijk vanuit huis te werken:

1. Ga bewust om met informatie en wat je bespreekt in berichtenapps of tijdens een videoconference.
2. Gebruik jouw Microsoft Surface als je deze hebt gekregen.
3. Gebruik Citrix alleen indien nodig.

Figuur 3 Screenshot intranet

Medewerkers ontvangen ook elke week een vraag via een applicatie genaamd 'Sir Ask A Lot'. Deze applicatie genereert vragen over privacy die door medewerkers kunnen worden beantwoord. Dit heeft een informatieve functie. Daarnaast geven de antwoorden van de medewerkers de FG en CISO inzicht in hoeverre medewerkers onderwerpen begrijpen en waar ze mogelijk nog meer ondersteuning nodig hebben.

Figuur 4 Voorbeeld vraag en antwoord 'Bewust in control – Sir Ask a lot'

De kennis van de medewerkers wordt op peil gehouden door een continue dialoog over privacy binnen de dagelijkse werkomgeving van de medewerkers, zoals tijdens teamoverleggen. Binnen verschillende afdelingen van gemeente wordt het gesprek over hoe om te gaan met persoonsgegevens structureel gevoerd. Dit wordt gedaan als integraal onderdeel van het werk. Bijvoorbeeld bij het bespreken van een lastige casus binnen het sociaal domein wordt naast problematiek ook besproken welke uitdagingen de casus geeft voor het waarborgen van de privacy. Aanvullend hierop geven medewerkers aan dat zij zich vrij voelen om als er een fout wordt gemaakt met de omgang van persoonsgegevens een collega hierop te wijzen en samen na te denken hoe ze het in de toekomst anders kunnen aanpakken.

Ter bevordering van de bewustwording hebben de FG en CISO een fictieve ‘phishing-actie’ georganiseerd. Medewerkers ontvingen een mail over een kerstpakket met een link naar een website waar hen gevraagd werd gegevens in te vullen. De bedoeling was medewerkers duidelijk te maken waar mogelijke kwetsbaarheden zitten op het gebied van informatiebeveiliging. Deze actie bleek een goede ‘geplande organisatie-opfrisser’ om het gesprek over privacy en informatiebeveiliging binnen de gemeente gaande te houden. Hiermee is ook deels opvolging gegeven aan een aanbeveling uit het Rapport 2018 om dit onderwerp bij de medewerkers structureel hoog op de agenda te houden.

Periodiek wordt bij nieuwe medewerkers aandacht gevraagd voor het belang van privacy en informatieveiligheid. Tevens wordt de hierboven reeds beschreven applicatie ‘Sir Ask A Lot’ voor nieuwe medewerkers geactiveerd zodra zij in dienst komen. Het inwerkprogramma voor nieuwe medewerkers ondervindt in 2020 vanwege de Corona-omstandigheden beperkingen. Dat heeft onder meer tot gevolg dat buiten de standaardonderdelen het belang van privacy tijdens het inwerkprogramma verder niet altijd aan de orde komt.

Naast pro-actieve communicatie naar medewerkers, zijn er in de gemeente ook sterke lijnen vanuit medewerkers met privacy-gerelateerde vragen naar MT-leden en de FG en CISO. Uit alle gesprekken is consequent naar voren gekomen dat collega’s de FG en de CISO goed weten te vinden en zich adequaat door hen voelen ondersteund. De FG en de CISO worden wat dit betreft omschreven als toegankelijk, kundig en behulpzaam. Daarbij merken wij ook op dat het gegeven dat medewerkers vragen over privacy en informatiebeveiliging hebben én deze ook actief via de aanwezige kanalen stellen betekent dat ze zich bewust zijn van het belang van het onderwerp.

4.3 Communicatie naar en het betrekken van inwoners

Contacten tussen de gemeente en de inwoners vindt op vele wijzen plaats. Alleen bij contacten waar de inwoners persoonlijke informatie delen met de gemeente, is er aanleiding om ook te spreken over privacy. Maar ook dan gebeurt dat niet altijd, of niet meteen in het eerste contact. Als een inwoner

urgente (hulp)vragen heeft, is de situatie er niet altijd naar om uitgebreid de wijze van bescherming van de vertrouwelijke informatie van deze inwoner aan de orde te stellen. Op een later moment in het proces, als de urgentie in de situatie wat is afgenomen, wordt er veelal alsnog teruggekomen op het onderwerp privacy. Als er toestemming wordt gevraagd voor verwerking van persoonsgegevens, wordt dit in het dossier opgenomen.

4.4 Tussenbalans

Ook in het dagelijks werk van de medewerkers wordt geregeld aandacht gevraagd voor het beschermen van persoonsgegevens. Dit gebeurt met enige regelmaat via het Intranet van de gemeente en via specifieke acties. Er is sprake van een cultuur waarin uitdagingen met betrekking tot enerzijds het beschermen van persoonsgegevens en anderzijds efficiënt en effectief invulling geven aan beleidsinhoudelijke opdrachten zowel onderling als in wisselwerking met de FG en CISO kunnen worden besproken.

Deelvraag 4, 5 en 6, met betrekking tot de cultuur in de gemeentelijke organisatie

Vraag 4	Op welke manier is privacy als kernwaarde in de cultuur van de organisatie verankerd?
Antwoord	De aandacht voor privacy wordt, vooral dankzij de inspanningen van de FG en de CISO, ook na de implementatie van de AVG, levendig gehouden binnen de organisatie. Dit komt door het consequent actualiseren van het beleid en de consequente aandacht voor bewustwording. Medewerkers zijn geïnformeerd over de basis principes van privacy en worden door wekelijkse vragen en de incidentele ludieke acties blijvend geïnformeerd. Privacy maakt nog niet altijd automatisch deel uit van het inwerktraject van nieuwe medewerkers.
Vraag 5	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?
Antwoord	Aandacht voor privacy is op verschillende wijzen geborgd. De FG en CISO zien er op toe dat privacy en informatiebeveiliging in de protocollen en werkprocessen voldoende worden geadresseerd. Ook MT-leden besteden aandacht aan privacy en informatiebeveiliging in overleggen, gesprekken en procedures. De onderwerpen privacy en informatiebeveiliging komen met regelmaat in werkoverleggen en functioneringsgesprekken aan de orde.
Vraag 6	Hoe wordt er intern en naar inwoners gecommuniceerd over privacy?
	Intern wordt er geregeld aandacht besteed aan het belang van privacy. Ook voor het versterken van de communicatie over privacy met de inwoners is er aandacht en zijn er sinds het onderzoek in 2018 verbeteringen gerealiseerd.

Aan de aanbevelingen uit het onderzoek van 2018 die gericht waren op de versterking van de cultuur binnen de organisatie met betrekking de bescherming van persoonsgegevens is grotendeels opvolging gegeven. Met name de CISO en de FG zijn actief en permanent bezig om te benadrukken dat privacy een belangrijke kernwaarde van de gemeentelijke organisatie is. Zij staan hierin niet geïsoleerd; zij staan midden in de organisatie, worden herkend door de medewerkers en worden ook makkelijk benaderd door medewerkers die uitdagingen ervaren met betrekking tot privacy. Binnen werkoverleggen van de verschillende sectoren binnen de organisatie komt het onderwerp geregeld ter sprake.

De raad is over het vaststellen van de betreffende nota's niet actief geïnformeerd met een informatienota. Wel heeft de raad het op 7 mei 2020 vastgestelde verslag van de collegevergadering ontvangen. Daarmee was de raad in de gelegenheid om naar aanleiding van dit verslag nader te informeren naar het beleid.

5. Beoordeling, conclusies en aanbevelingen

5.1 Beoordeling

In dit hoofdstuk toetsen wij 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 betrekking op de periode vanaf juni 2018 tot en met heden.

Beleid	Beoordeling
De gemeente heeft verschillende beleidskaders, regels en richtlijnen met betrekking tot de (juridische) borging van de privacy van inwoners aantoonbaar aangepast conform de AVG. Voor specifieke (meer risicovolle) domeinen heeft de gemeente aanvullende regels opgesteld.	Positief
In de verschillende beleidskaders 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.	Positief
De gemeente hanteert landelijke standaarden, zoals de Baseline Informatiebeveiliging Gemeenten.	Positief
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 en hoe en wanneer vastgestelde processen worden geëvalueerd en aangepast.	Positief

De gemeente heeft beleidskaders opgesteld waarover jaarlijks wordt gerapporteerd. In deze beleidskaders worden alle in het normenkader genoemd aspecten behandeld. De landelijke standaarden waaronder de BIG en de BIO worden in de beleidskaders nadrukkelijk meegenomen. Het toezicht vindt plaats door monitoring en audits. Er vinden periodieke controles plaats waaronder de jaarlijkse ENSIA-controles. Hiervoor wordt gebruikt gemaakt van een applicatie waardoor deze centraal worden aangestuurd. Daarnaast zijn er ook domein specifieke controles. Zo is er een kwaliteitsmonitor gericht op de BRP. In het algemeen verloopt de verantwoording over privacy via de reguliere kanalen. De monitoring wordt ondersteund door de AVG-monitor. Door het gebruik van het RASCI-model zijn de verantwoordelijkheden duidelijk en inzichtelijk.

Uitvoering

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 gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt.	Neutraal / deels 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
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.	Overwegend positief
De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.	Deels positief
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.	Deels positief

De gemeente heeft door middel van een cursus en het gebruik van intranet en de applicatie Sir Ask A lot verschillende middelen ingezet die medewerkers kennis tot zich te nemen over privacy en informatieveiligheid. Bij de inwerkingtreding van de AVG is de cursus breed in de organisatie uitgezet en door veel medewerkers gevolgd. In de huidige situatie krijgen nieuwe medewerkers in hun inwerktraject niet structureel informatie over privacy en informatieveiligheid.

De voortgang op het gebeid van meten en verbeteren wordt in kaart gebracht met de AVG-monitor en besproken per kwartaal. Daarmee heeft de gemeente een routine voor het meten en verbeteren van de bescherming van persoonsgegevens. Deze routine bestaat pas relatief kort en is ook nog in ontwikkeling. Hierdoor is het te vroeg om vast te stellen of er al sprake is van een structurele leer- en verbetercyclus. Dit geldt bijvoorbeeld ook de structurele inzet van PIA's; daartoe bestaan goede voornemens, die zich onder meer uit in een concrete planning. Maar een hele cyclus was ten tijde van dit rekenkameronderzoek nog niet doorlopen.

De burger wordt op de website op een begrijpelijke wijze geïnformeerd over de omgang van persoonsgegevens in de privacyverklaring. Er ontbreekt specifiek informatie over hoe de gemeente bijvoorbeeld bij datagedreven werken omgaat met (persoons)gegevens. Er zijn verschillende plannen om de communicatie naar de burger over privacy te verbeteren. Het sociaal domein werkt aan het verbeteren van de communicatie naar inwoners door het maken van een flyer. Ook wordt er gedacht in de hal van de gemeente op een scherm informatie te laten zien. Door de coronacrisis zijn deze ideeën nog niet uitgewerkt. Mondeling wordt de burger geïnformeerd als dat relevant is in de context van de situatie. Hier is geen 'standaardaanpak' voor. Het is daarom belangrijk dat alle medewerkers, zeker die contact hebben met inwoners, goed geïnformeerd blijven over privacy zodat zij kunnen herkennen in welke situaties zij dit onderwerp kunnen opbrengen.

Cultuur

De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens en worden van aanpassingen op de hoogte gehouden.	Positief
In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk privacybeleid na te leven.	Positief

5.2 Conclusies en aanbevelingen

In de hoofdstukken 2, 3 en 4 zijn de bevindingen gepresenteerd, successievelijk op basis van de thema's beleid, uitvoering en cultuur. In dat verband is tevens ingegaan op de opvolging die de gemeente heeft gegeven aan de aanbevelingen die opgenomen waren in het eerdere rekenkameronderzoek van 2018.

Elk van die hoofdstukken is afgerond met de beantwoording van de relevante deelvragen. Na een nadere verdieping en analyse van de bevindingen, door de beoordeling van de bevindingen op basis van het normenkader in paragraaf 5.1, kan nu eerst de centrale onderzoeksvraag worden beantwoord.

	Centrale probleemstelling
Vraag	Hoe is in het licht van de adviezen van 2018 de privacy van inwoners geborgd zowel in juridische, beleidstechnische en culturele zin en op welke punten behoeft dit eventueel aanpassingen?
Antwoord	Binnen de gemeente Pijnacker-Nootdorp is de aandacht voor de privacy van de inwoners goed geborgd, zowel in juridische, beleidstechnische als culturele zin. Omdat beleid altijd in verandering is, blijft er ruimte voor aanpassingen en verbeteringen.

Op basis van het onderzoek en deze conclusie onderscheidt de rekenkamer de volgende aanbevelingen:

- **Inwerktraject**
  Over het algemeen is de aandacht voor privacy goed geborgd in de organisatie. Het laatste half jaar is echter, vanwege de bijzondere 'Corona-omstandigheden', het inwerktraject onder druk komen te staan terwijl de manier van werken in de gemeente sterk is veranderd en meer op afstand is. Het strekt daarom tot aanbeveling om het toelichten en benadrukken van privacy- en informatieveiligheid meer nadrukkelijk onderdeel van het inwerkprogramma van nieuwe medewerkers te maken.

- **Communicatie naar inwoners**
  In het rekenkameronderzoek van 2018 is er op gewezen dat de communicatie naar de inwoners de nodige aandacht vereiste. Met name zou meer werk kunnen worden gemaakt van een proactieve informatieverstrekking over de wijze waarop de gemeente omgaat met de (al dan niet vertrouwelijke) gegevens van de burgers. De gemeente heeft op dit aspect vooruitgang geboekt, zoals onder meer door het vermelden van deze informatie op de website. Toch is nog ruimte voor verbetering. De gemeente heeft zelf ambities op dit punt met een privacyfolder voor het sociaal domein en het vertonen van privacy-gerelateerde meldingen op de schermen in het stadskantoor. Ook bij telefonische contacten zullen burgers in de nabije toekomst actief worden geïnformeerd over de bescherming van hun privacy door de gemeente.

De rekenkamer ondersteunt deze ambities en doet de aanbeveling om de communicatie naar inwoners via de website, folders, op het stadskantoor en in contacten met inwoners continue te blijven verbeteren. Daarbij kan de gemeente ook in gesprek gaan met (vertegenwoordigers van) inwoners om er achter te komen welke vragen er bij hen leven, om de communicatie uitingen daar op aan te passen.

- **Uitvoeren van (D)PIA's[16]**
  De gemeente heeft een plan en aanpak voor het uitvoeren van PIA's, maar deze uitvoering dient nog routine te worden. De aanbeveling is om deze routine spoedig te verkrijgen door meer PIA's uit te voeren, te beginnen met de processen waar veel en/of gevoelige persoonsgegevens verwerkt worden. De uitvoering van PIA's is mede een verantwoordelijkheid van de eigenaren van de betreffende processen; zij dienen nadrukkelijk een rol te krijgen bij de planning en totstandkoming van de PIA's. Daarnaast kan de gemeente routine opdoen door het uitvoeren van een PIA standaard praktijk te laten zijn bij nieuwe of veranderende wet- en regelgeving en/of uitvoeringsprocessen. Met de uitvoering van PIA's komen ook de belangrijkste privacyrisico's in de gemeente in beeld, die weer van belang zijn voor de leer- en verbetercyclus van de gemeente (zie de volgende aanbeveling).

- **Versterken leer- en verbetercyclus**
  De gemeente werkt volgens een (gemeente-brede) PDCA-cyclus waar ook de bescherming van persoonsgegevens en informatiebeveiliging in zijn opgenomen. De 'check' en 'act' fase, gericht op het evalueren en bijstellen van beleid kunnen nog gestructureerder en explicieter worden uitgevoerd. De aanbeveling is om dit voor privacy en informatiebeveiliging handen en voeten te geven door de privacy-risico's die in uitgevoerde PIA's zijn geïnventariseerd centraal te stellen. Met andere woorden, de gemeente kan de 'check' fase invullen door periodiek (bijvoorbeeld jaarlijks) voor de belangrijkste onderkende privacy-uitdagingen te toetsen of de benodigde maatregelen zijn genomen en of er noemenswaardige incidenten zijn voorgevallen.

[16] Zoals eerder in het rapport al genoemd wordt binnen het vakgebied van privacy- en informatiebeveiliging zowel gesproken over PIA's (Privacy Impact Assesment) als DPIA's. Die laatste afkorting staat voor Data Protection Impact Assessment; het betreft het geregeld doen van controles op de beveiliging van informatiesystemen.

Bijlage A Geïnterviewde personen

Datum	Naam	Functie
10-6-2020	Carlo Vreugde	Chief Information Security Officer
10-6-2020	Gosse Bouter	Functionaris Gegevensbescherming
12-6-2020	Dorothee Peters	Teamleider Gegevensbeheer en Belastingen
17-6-2020	Jeffrey Mangal	Programmamanager Datagedreven werken
10-6-2020	Frank van Manen	Juridisch beleidsmedewerker/privacy officer
17-6-2020	Monique van Waardenberg	Afdelingshoofd Sociaal Domein
17-6-2020	Odette Langeveld	Teamleider maatschappelijke ondersteuning

Bijlage B Bestudeerde documentatie

#	Documentnaam	Versie	Datum
1	Concept DPIA Cameratoezicht intern	-	-
2	Concept DPIA Participatie	-	-
3	Concept DPIA WMO	-	-
4	ENSIA collegeverklaring 2018	-	26 februari 2019
5	ENSIA collegeverklaring 2019	-	28 april 2020
6	Informatiebeveiliging Jaarrapportage 2019	-	-
7	Informatiebeveiligingbeleid BIO Pijnacker Nootdorp 2020-2023	0.2	10 december 2019
8	Informatiebeveiligingbeleid Pijnacker-Nootdorp (oud)	1.0	Juli 2018
9	Jaarplan Privacy en Informatieveiligheid 2020 Factsheet	-	-
10	Privacy Folder	-	-
11	Privacy Jaarrapportage 2018	-	-
12	Privacy Jaarrapportage 2019	-	-
13	Privacybeleid Pijnacker-Nootdorp (oud)	-	April 2018
14	Privacybeleid Pijnacker-Nootdorp	-	April 2020
15	Privacyverklaring website	-	20 september 2019
16	Sociaal Domein Informatie- en inzagerecht	-	Februari 2020
17	Sociaal Domein Werkinstructie beeldbellen	-	27 maart 2020
18	Sociaal Domein Werkprocessen Kernteam (concept) 2020	-	April 2020

Bijlage C Deelnemers Mini-DPIA's

Mini-DPIA Wvggz - 7 september 2020

Naam	Functie
Maria Dernee	Medewerker kernteam
Erik Visser	Beleidsadviseur sociaal domein
Frank van Manen	Juridisch beleidsmedewerker / privacy officer

Mini-DPIA Fraude - 16 september 2020

Naam	Functie
Judith van der Graaf	Afdelingshoofd interne dienstverlening
Monique van Waardenberg	Afdelingshoofd sociaal domein
Sander Hazebroek	Afdelingshoofd bedrijfsvoering
Wanda Bouwmeester	Concerncontroller

gemeente Pijnacker-Nootdorp

adres 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

Voorzitter Rekenkamercommissie Pijnacker-Nootdorp
mevr. S.E. Bueving

Cc: dhr. J. van der Haas, ambtelijk secretaris van de Rekenkamercommissie

onderwerp Bestuurlijke reactie op de Quickscan Privacy en Informatieveiligheid

nadere informatie G. Bouter

verzenddatum

zaaknummer 1203643

briefnummer 1083278

uw brief van 12 oktober 2020

uw kenmerk

Geachte mevrouw Bueving,

Allereerst danken wij u hartelijk voor uw verrichte onderzoek. Graag maken wij gebruik van de geboden mogelijkheid om op de Quickscan Privacy en Informatieveiligheid te reageren.

Het onderzoek heeft als doel om inzicht te krijgen in de wijze waarop invulling is gegeven aan de aanbevelingen uit de rapportage van de rekenkamercommissie uit 2018 betreffende de beveiliging en bescherming van persoonsgegevens. In de rapportage uit 2018 concludeerde u dat wij goed op weg waren om de privacy van inwoners juridisch en in de praktijk te borgen, maar dat dit op enkele punten nog verder geïmplementeerd kon worden.

De afgelopen twee jaar hebben wij op het gebied van privacy en informatieveiligheid verschillende maatregelen getroffen om een zorgvuldige omgang met persoonsgegevens te blijven waarborgen. Uw beoordeling en conclusie in deze Quickscan sterken ons in de gedachte dat wij in 2018 op de juiste weg waren en dit twee jaar later nog steeds zijn.

Wij zijn ons er terdege van bewust dat privacy en informatieveiligheid onverminderd van belang blijft en continue aandacht vereist binnen een steeds verder digitaliserende overheid. Wij zijn dan ook blij met uw aanbevelingen om de borging van de privacy te verbeteren en nemen deze van harte over. Hieronder gaan wij in op uw aanbevelingen.

Inwerktraject
U doet de aanbeveling om het toelichten en benadrukken van privacy en informatieveiligheid nadrukkelijker onderdeel te laten zijn van het inwerkprogramma van nieuwe medewerkers.
Aandacht voor privacy en informatieveiligheid is altijd van belang. Dat is een van de redenen dat tijdens introductiebijeenkomsten voor nieuwe medewerkers ook aandacht wordt besteed aan dit onderwerp.

Daarnaast worden nieuwe medewerkers vanaf hun eerste werkdag meegenomen in de reguliere activiteiten, zoals de vragen van 'Sir Ask A Lot', om de bewustwording onder medewerkers te vergroten. Uiteraard is gedurende de abrupte overgang van werken op kantoor naar een thuiswerkplek aandacht gevraagd voor en advies gegeven over 'veilig' thuiswerken en zullen wij dit blijven doen.
Ondanks de reeds bestaande communicatie over privacy en informatieveiligheid is deze periode waarin wij digitale middelen veelvuldiger zijn gaan gebruiken en meer op afstand zijn gaan werken een goed moment om te onderzoeken of, en zo ja, hoe privacy- en informatieveiligheid beter geborgd kan worden in het inwerkprogramma.

Communicatie naar inwoners
U concludeert dat vooruitgang is geboekt op het gebied van onze communicatie richting inwoners en dat er tegelijkertijd nog ruimte is voor verbetering. Door onze ambities op dit vlak te verwezenlijken, die u ook onderschrijft, hopen wij onze inwoners nog beter te bereiken en een excellente dienstverlening te bieden. Hoe wij hierbij onze communicatie nog beter af kunnen stemmen op de wensen en behoeften van onze inwoners zullen wij onderzoeken. In gesprek gaan met vertegenwoordigers van inwoners is daarin een goede suggestie.

Uitvoeren van DPIA's en ***Versterken leer- en verbetercyclus***
De aanbevelingen met betrekking tot de PIA's en de PDCA-cyclus worden herkend en wij zijn voornemens deze op te volgen. Wij zien de meerwaarde van het centraal stellen van mogelijke privacyrisico's in de PDCA-cyclus en gaan hiermee aan de slag. Hierbij zullen wij oog houden voor de samenhang tussen de verschillende onderdelen waarop in wordt gezet om privacy en informatieveiligheid te borgen.

Tot Slot
Wij vertrouwen erop dat met bovenstaande reactie aan uw verzoek is voldaan.

Hoogachtend,
het college van Pijnacker-Nootdorp,

J.P.R. Woudstra
secretaris (plv.)

mw. F. Ravestein
burgemeester

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