Onderzoeksopzet
Privacy en informatieveiligheid
Sociaal Domein

Gemeente Heerhugowaard

Rekenkamerfunctie Heerhugowaard

Mevr. E. Witzke, MSc
Ambtelijk secretaris

T. 06-451 713 57
E. eva@necker.nl

Datum: 3 mei 2018

Inhoudsopgave

1 Wat gaan we onderzoeken?

1.1 / Aanleiding en doelstelling

Gemeenten zijn altijd al verantwoordelijk geweest voor een juiste en veilige verwerking van persoonsgegevens. Zij dienen zich daarbij te houden aan de Wet bescherming persoonsgegevens (Wbp) en de Wet basisregistratie personen (Wet BRP). Door de toenemende taken van de gemeente op het sociaal domein is de aandacht voor en het belang van privacy en informatieveiligheid echter enorm toegenomen.

Het inkleuren van het lokale beleid op basis van de hierboven beschreven context is complex. Deskundigen en betrokken instanties, zoals Kwaliteitsinstituut Nederlandse Gemeenten (KING) en het College Bescherming Persoonsgegevens (CBP), maakten zich grote zorgen over de vraag of plannen om privacy van burgers te beschermen na de decentralisaties op 1 januari 2015 gereed zouden zijn. Het was volgens hen de vraag of de gemeenteraden hun controlerende en kaderstellende rol op het gebied van privacybeleid (specifiek in het sociaal domein) voldoende zouden kunnen vervullen en of colleges van B&W in staat zouden zijn de uitvoering aan te laten sluiten op wet- en regelgeving. Ondertussen gaan de ontwikkelingen op dit gebied razendsnel. Vanaf 1 januari 2016 geldt de Meldplicht Datalekken, per 1 juli 2017 is de Eenduidige Normatiek Single Information Audit (ENSIA) in werking getreden, begin juli werd duidelijk dat het project Basisregistratie Personen zoals het oorspronkelijk bedoeld was geen doorgang zal vinden en vanaf 25 mei 2018 wordt de Europese Algemene Verordening Gegevensbescherming (AVG) van toepassing.[1]

De toegenomen aandacht voor privacy gaat hand in hand met de aandacht voor informatieveiligheid. Informatieveiligheid is van belang, maar kan op gespannen voet staan met een noodzaak van efficiënt en pragmatisch werken. In het sociaal domein doet zich dat voelen in het dilemma dat integraal werken is gebaat bij gegevensverwerking en met name -deling, terwijl privacy en informatieveiligheid juist zijn gebaat bij minimalisatie van gegevensverwerking. Dit leidt tot de vraag hoe verschillende (technologische) ontwikkelingen op het gebied van data in combinatie met nieuwe gedecentraliseerde taken in het sociaal domein zich verhouden tot de informatieveiligheid en privacy en wat eventueel verbetering behoeft.

Ook in de raadsworkshop, die de rekenkamer jaarlijks met de raad houdt in het kader van het prioriteren van mogelijke onderzoeksonderwerpen, kwam het onderwerp 'privacy in het sociaal domein' als zeer gewenst onderzoeksonderwerp naar voren.

[1] De AVG is op 4 mei 2016 gepubliceerd in het Publicatieblad van de Europese Unie. Gemeenten hebben tot 25 mei 2018 de tijd om zich zodanig voor te bereiden dat zij vanaf dat moment voldoen aan de verplichtingen die de AVG met zich meebrengt.

Doelstelling onderzoek

Met dit onderzoek wil de rekenkamer de raad inzicht bieden in de mate waarin privacy en informatieveiligheid in het sociaal domein voldoende gewaarborgd zijn en indien nodig mogelijkheden voor verbetering aandragen.

1.2 / Hoofd- en deelvragen

Op basis van deze doelstelling is de volgende centrale vraag geformuleerd:

In hoeverre is de privacy van inwoners en de beveiliging van persoonsgegevens in het sociaal domein van de gemeente Heerhugowaard gewaarborgd?

Deze hoofdvraag hebben we vertaald in de volgende deelvragen, gerangschikt naar thema:

Beleid

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

Governance en werkprocessen

2 Hoe is de governance van het privacybeleid en informatieveiligheid in het sociaal domein vormgegeven?
3 Hoe functioneert de governance in de praktijk?
4 Welke werkafspraken zijn er binnen de gemeente gemaakt rondom gegevensverwerking en –beveiliging en rondom beveiligingsincidenten in het sociaal domein?
5 Hoe verloopt de omgang met persoonsgegevens in de praktijk?
6 Op welke wijze geeft het college van B&W invulling aan de actieve en passieve informatieverstrekking aan de gemeenteraad met betrekking tot informatieveiligheid en privacy in het sociaal domein?

Beheer en opslag gegevens

7 Is er zicht op:
   a. welke informatiesystemen er binnen de gemeente persoonsgegevens registreren;
   b. hoe de toegang van medewerkers tot informatiesystemen is geregeld (autorisatieregisters);
   c. hoe de verwerking van persoonsgegevens door samenwerkende partijen is geregeld (bewerkersovereenkomsten).

Bewustzijn

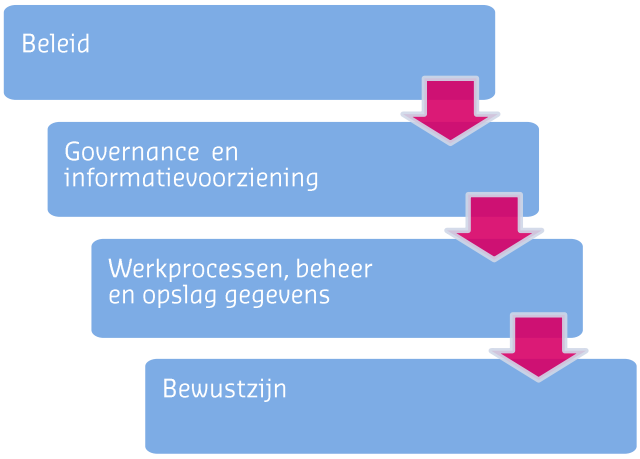
8 Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers in het sociaal domein op het gebied van privacy en informatieveiligheid?

1.3 / Kijk op het onderwerp en analyse-elementen

Vaak hechten gemeenten veel waarde aan afspraken op 'papier': denk aan werkafspraken, privacyprotocollen, samenwerkingsovereenkomsten of convenanten. Dit soort formele afspraken hebben echter alleen waarde als ze bij betrokkenen bekend zijn, als werkbaar worden beschouwd en er nagegaan wordt of de afspraken ook in de praktijk de verwachte uitwerking hebben. Zo kan beveiligd mailverkeer van persoonsgegevens het uitgangspunt zijn, maar kan er vanwege gemak toch onbeveiligde mail uit worden gestuurd. Of gegevens die toch al bekend zijn bij de ene afdeling van de gemeente (sociaal domein) worden intern doorgegeven aan een andere afdeling (toezicht en handhaving).

Een onderzoek naar informatiebeveiliging en privacy vraagt dus om een aanpak die verder gaat dan het analyseren van documenten. Daarom besteden wij in het onderzoek op een systematische wijze aandacht schenken aan de onderdelen die door de VNG en KING zijn onderscheiden: beleid (kaders, rollen en verantwoordelijkheden), governance, werkprocessen (organisatorische constellatie en uitvoeringspraktijk) & beheer en opslag van gegevens, en bewustzijn. Deze vier aspecten worden hieronder verder toegelicht.[2]

Figuur 1 Analyse-elementen



Beleid

Als het gaat om informatieveiligheid, is het college van B&W verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaatsvindt. Het opstellen van actueel informatieveiligheidsbeleid en decentralisatiebeleid waarin privacy een rol heeft, zorgt voor een basis voor een verantwoordelijke omgang met persoonsgegevens. Het startpunt voor een onderzoek naar informatiebeveiliging en privacy is dan ook het analyseren van de kaders die door raad en/of college zijn vastgesteld. Het beleid fungeert als een toetssteen voor de overige aspecten van het onderzoek, aangezien het beleid ook beschrijft wat de governance, werkprocessen en beheer van informatie inhouden. Tevens wordt vanuit het beleid vaak ook duidelijk welke rol landelijke kaders voor de gemeente spelen.

Governance en informatievoorziening

De rollen en verantwoordelijkheden op het gebied van privacy en informatieveiligheid dienen helder te zijn. De VNG geeft hierbij aan dat er duidelijk onderscheid moet zijn in bestuurlijke en ambtelijke eindverantwoordelijkheid. Hoe is de verantwoordelijkheid in het college belegd? En wie zijn in de ambtelijke organisatie aangewezen om de naleving van de privacywet- en regelgeving te waarborgen in de organisatie? Hoe communiceren deze personen met elkaar? Op basis van nieuwe wetgeving ontstaat het komende jaar een aantal verplichtingen op het gebied van de governance structuur. De gemeente moet bijvoorbeeld per 25 mei 2018 voldoen aan de verplichtingen die voortvloeien uit de AVG, maar moet voorafgaand daaraan stappen zetten om aan die verplichtingen te kunnen voldoen.

[2] Deze gefaseerde aanpak is gebaseerd op het 'privacyraamwerk' ontwikkeld door KING en VNG

Hier komt tevens de rol van de raad nadrukkelijk naar voren. Het onderwerp informatiebeveiliging raakt direct aan inwoners en is dus van groot belang voor de raad. Handelt de raad hier ook naar, en vraagt de raad actief om informatie?

Werkprocessen, beheer en opslag gegevens

Naast de afspraken op papier dienen gemeenten privacy en informatieveiligheid een plek te geven in werkprocessen of –afspraken. De interne werkprocessen moeten beschrijven wie wanneer toegang heeft tot informatie en hoe die informatie correct wordt verwerkt. Een belangrijke afspraak die met partnerorganisaties gemaakt kan worden is bijvoorbeeld op welke wijze bepaald wordt of gegevens verzameld en gedeeld worden. Maar het gaat ook over de afspraak of inwoners tijdens een 'keukentafelgesprek' standaard geïnformeerd worden over privacy en informatieveiligheid. Ook over verantwoording moeten zaken vastgelegd zijn, zowel van externe organisaties aan de gemeente als van het college aan de raad.
De werkprocessen worden gefaciliteerd door systemen. De systemen moeten een bepaalde beveiliging hebben, maar er moet ook helder zijn wie welke toegang heeft en of het gebruik van het systeem achteraf gecontroleerd wordt. Zonder goede systemen en correct gebruik daarvan kan de privacy van inwoners niet gewaarborgd worden.

Bewustzijn

De mate waarin medewerkers van de gemeente zich bewust zijn van hun verantwoordelijkheid ten opzichte van een zorgvuldige omgang met persoonsgegevens is een essentieel onderdeel van het waarborgen van privacy. Daarvoor is continue aandacht nodig, het bewustzijn rond informatiebeveiliging moet verweven worden met de organisatiecultuur. Hierbij kan worden gedacht aan training, opleiding, intervisie of andere methodieken om medewerkers te wijzen op het belang van privacy en de risico's als het gaat om de opslag en het delen van persoonsgegevens. Hier ligt een nadrukkelijke relatie met governance: wie is er in de organisatie aangewezen om het bewustzijn onder medewerkers (én samenwerkende partijen) te vergroten?

1.4 / Normenkader

In dit onderzoek werken we met een normenkader, dat gezien kan worden als een concrete uitwerking van de analyse-elementen die we hierboven hebben beschreven. We hebben niet de intentie om in dit onderzoek alle afzonderlijke normen 'af te vinken'. Wel geeft het normenkader een goede indruk van 'de bril' waarmee we naar de aangetroffen praktijk kijken.

Beleid
/ Er is een privacybeleid en een informatieveiligheidsbeleid. / De beleidsstukken beschrijven onder andere rollen en verantwoordelijkheden, werkprocessen, veiligheidsmaatregelen. / Het beleid wordt periodiek up to date gebracht.
/ In het privacybeleid van de gemeente wordt verwezen naar de relevante wettelijke kaders. / De gemeenteraad heeft in het privacybeleid bepalingen vastgelegd over de borging van privacy in het algemeen en de bescherming van persoonsgegevens in het bijzonder en hierbij ook de rolverdeling tussen college en raad vastgelegd. / Het privacybeleid is afgestemd op de AVG.
Governance en informatievoorziening
/ De rollen en verantwoordelijkheden zijn vastgelegd. / Er is tenminste een CISO en een verantwoordelijke op het gebied van privacy. Voor medewerkers binnen de gemeenten is er een duidelijk aanspreekpunt op het gebied van privacy.

/	Er is rekening gehouden met de gevolgen van de AVG voor de governance structuur.
/	Er zijn duidelijke afspraken over de communicatie/afstemming/sturing tussen organisatie en college, die in de praktijk worden nageleefd.
/	De gemeenteraad besteedt aandacht aan het onderwerp privacy.
/	De gemeenteraad wordt actief geïnformeerd over de borging van privacy binnen de gemeente en bij organisaties waar zij mee werkt.
/	Vragen vanuit de gemeenteraad over dit onderwerp worden adequaat beantwoord.
/	De organisatie weet wat er vanuit ENSIA nodig is om goed te rapporteren aan de gemeenteraad en handelt hier naar.
	Werkprocessen, beheer en opslag van gegevens
/	De gemeente heeft beveiligingsniveaus geïdentificeerd en haar systemen beveiligd.
/	Binnen de gemeentelijke organisatie is een controlemechanisme aanwezig dat er voor zorgt dat er op de juiste wijze wordt omgegaan met privacygevoelige gegevens.
/	Mogelijke risico's worden gesignaleerd. Hier wordt aantoonbaar actie op ondernomen.
/	De werkprocessen zijn - in ieder geval wat betreft het privacy en informatieveiligheid- voor ingebruikname getoetst met betrokken medewerkers op werkbaarheid en risico's.
/	Uit de werkprocessen is op te maken wanneer, door wie en om welke reden privacygevoelige informatie is geraadpleegd.
/	De wettelijke bewaartermijnen worden niet overschreden.
/	De gemeente heeft met partners convenanten afgesloten waarin de voorwaarden voor uitwisseling van persoonsgegevens staan.
/	De gemeente controleert of bovenstaande afspraken worden nageleefd.
/	De gemeente heeft bewerkersovereenkomsten afgesloten met organisaties die gegevens verwerken voor de gemeente.
	Bewustzijn
/	Gemeentebreed wordt aandacht aan informatieveiligheid besteed, bijvoorbeeld via intranet.
/	Informatie over privacy maakt deel uit van het inwerkprogramma van nieuwe medewerkers.
/	Medewerkers ontvangen (de voor hun afdeling relevante) trainingen en communicatie omtrent privacy.

2 Plan van aanpak in 4 fases

Dit onderzoek wordt uitgevoerd in vier fases. Elk van deze fases wordt hieronder kort toegelicht waarbij wordt benoemd wat de resultaten van de fase zijn en op welke manier deze worden behaald.

2.1 / **Fase 1:** Start van het onderzoek

Voor de startbijeenkomst nodigen we de gemeentesecretaris uit en bij voorkeur de Functionaris Gegevensbescherming en de CISO (Chief Information Security Officer). Eén van deze personen zal onze contactpersoon zijn voor dit onderzoek. Met hen maakt de projectleider heldere afspraken over het opvragen van documenten en het plannen van interviews. Bij de startbijeenkomst leggen we ook een informatieverzoek neer en stemmen we de planning af.

Fase 1: samenvatting

Resultaten

/ Onderlinge werkafspraken en verwachtingen zijn vastgesteld
/ Ambtelijke organisatie is op de hoogte en kent de informatievraag

Gehanteerde methode

/ Startbijeenkomst

2.2 / **Fase 2:** Beleid, governance en formele afspraken

In deze fase brengen we de beleidskaders van de gemeente in kaart als het gaat om de omgang met en beveiliging van persoonlijke gegevens. Ook analyseren we welke governance-structuur er op papier is neergezet en welke formele afspraken er zijn gemaakt met samenwerkingspartners in het sociaal domein. We kijken of de afspraken voldoen aan de wettelijke kaders en of de gemeente formele controle op derden heeft georganiseerd. Verder onderzoeken we of de gemeente bewerkersovereenkomsten heeft afgesloten met relevante partners. En is er een register aanwezig waaruit af te leiden is welke persoonsgegevens er verwerkt worden binnen de gemeente met bijbehorende risicoklassen?

Aanvullend houden we een interview met het collegelid dat het meest zicht heeft op privacy en informatieveiligheid. Dit interview geeft zicht op de wijze waarop de bestuurlijke verantwoordelijkheid is georganiseerd, welke ambities het college heeft op het gebied van privacy en informatieveiligheid, hoe dit doorwerkt in de governance structuur en welke vragen er op strategisch niveau leven met betrekking tot privacy. Daarnaast zal in een duo-interview met de privacy officer (of een andere functienaam met hetzelfde takenpakket) en de Chief Information Security Officer (CISO) een breed palet aan zaken aan bod komen, van de structuur van de privacy-organisatie en de stand van zaken op het gebied van informatiebeveiliging en privacy tot de veiligheid van de systemen/portalen en werkprocessen, onder andere rondom de Meldplicht Datalekken.

Fase 2: samenvatting

Resultaten

- Inzicht in gemeentelijk beleid, governance, formele werkprocessen
- Inzicht in formele werkafspraken met externe partijen
- Inzicht in het type initiatieven dat ondernomen wordt

Gehanteerde methode

- Documentanalyse
- Interview portefeuillehouder
- Duo-interview Privacy officer en CISO

2.3 / **Fase 3:** Governance en informatieveiligheid in de praktijk in het sociaal domein

In deze fase verdiepen we het beeld dat in fase 2 is ontstaan over de invulling van privacybescherming en informatieveiligheid in het sociaal domein. We gaan in gesprek met de teamleider van zorgconsulenten (soms ook wel coaches of sociaal teammedewerkers genoemd) en met drie of vier medewerker van de afdeling sociaal domein, zoals een regisseur of een consulent, in een groepsgesprek. We onderzoeken hoe de governance rondom privacy en informatieveiligheid in de praktijk functioneert en hoe gegevensverwerking binnen de systemen van het sociaal domein aan toe gaat. We vragen naar de beveiliging van het gebruik van relevante ICT-systemen. Hoe wordt het verwerken van persoonsgegevens door externe partijen gecontroleerd? Wat laten uitkomsten van interne controles zien? Verder bekijken we op welke wijze privacy en informatieveiligheid in het dagelijks handelen in het sociaal domein zijn plek krijgt. Op welke manier worden gegevens uit een keukentafelgesprek bewaard, hoe worden inwoners geïnformeerd over privacy en hoe verloopt gegevensuitwisseling met zorgpartners?

Fase 3: samenvatting

Resultaten

- Inzicht in de uitvoeringspraktijk en informatieveiligheidstructuur

Gehanteerde methode

- Aanvullende documentanalyse
- Interviews (totaal 2) met teamleider zorgconsulent (of vergelijkbare functie) en met medewerker sociaal domein (regisseur, consulent of vergelijkbare functie)

2.4 / Fase 4: Rapportage

In deze laatste fase van het onderzoek leggen we de laatste hand aan de Nota van Bevindingen. In de Nota van Bevindingen nemen we een overzicht op van relevante goede voorbeelden uit andere gemeenten. We leggen de Nota voor aan de organisatie voor het ambtelijk wederhoor. Na verwerking van de ambtelijke reactie maken wij de Nota van Bevindingen definitief en stellen wij de Bestuurlijke Nota op met daarin de conclusies en aanbevelingen. We nodigen het college uit om een bestuurlijke reactie te formuleren op de conclusies en aanbevelingen. De reactie van het college nemen wij integraal op in het definitieve rapport, dat aan de raad wordt aangeboden. De directeur van de rekenkamer presenteert de uitkomsten van het onderzoek aan de raad.

Fase 4: samenvatting

Resultaten

- Beantwoording van de deelvragen en hoofdvraag
- Overzicht van goede voorbeelden uit andere gemeenten

Gehanteerde methode:

- Feitenverificatie (ambtelijk wederhoor)
- Bestuurlijk wederhoor
- Rapportage inclusief conclusies en aanbevelingen

3 Onderzoeksteam en planning

3.1 / Onderzoeksteam

Eva Witzke vervult de rol van ambtelijk secretaris. De directeur van de rekenkamer, Hans Oostendorp, en het onderzoeksteam bestaande uit Emilie Stumphius en Gideon van der Hulst voeren het onderzoek uit.

3.2 / Planning

Wij starten het onderzoek op in mei 2018. We bieden het rapport in het najaar van 2018 aan.