Bescherming Persoonsgegevens in Noordwijk

rapport
versie 1.0
datum 18 juni 2021

PBLQ

verbinders in de informatiesamenleving

Inhoudsopgave

Bestuurlijke samenvatting 1

1. Inleiding 4

1.1 Aanleiding en opdracht 4
1.2 Normenkader 5
1.3 Werkwijze 6
1.4 Indeling rapport 7

2. De privacykaders 8

3. Het gemeentelijk beleid 11

3.1 Beleidskaders 11
3.2 Uitvoering van het beleid 14
3.3 Leren en verbeteren 17
3.4 Inwoners 19
3.5 Risico's en nieuwe ontwikkelingen 21
3.6 De rol van de gemeenteraad 23

4. Conclusies 25

Bijlage A Geïnterviewde personen 27

Bijlage B Aanwezigen Mini-PIA Noodfonds 27

Bijlage C Bestudeerde documentatie 27

Bijlage D Definitielijst 29

Bijlage E Afkortingslijst 30

Bijlage F Organisatiestructuur gemeente Noordwijk 30

Bijlage G Bestuurlijk wederhoor 31

Bijlage H Nawoord Rekenkamer 32

PBLQ

verbinders in de informatiesamenleving

Bestuurlijke samenvatting

In dit onderzoek is gekeken hoe in het licht van de verdergaande digitalisering de privacy van inwoners juridisch en in de dagelijkse beleidspraktijk van de gemeente Noordwijk is geborgd. Eveneens is aan de orde gekomen op welke punten het beleid aanpassing en verbetering behoeft.

De gemeente Noordwijk borgt de privacy van inwoners in haar privacybeleid en informatiebeveiligingsbeleid. Er worden verschillende eisen gesteld aan gemeenten waarvan de belangrijkste staan in de Algemene Verordening Gegevensbescherming (AVG). De gemeente voldoet aan een aantal van die vereisten. Er is sprake van privacybeleid. Het privacybeleid is naar aanleiding van de inwerkingtreding van de AVG aangepast. In het beleid wordt op hoofdlijnen uitgelegd hoe de gemeente Noordwijk omgaat met persoonsgegevens. Ook is er een verwerkingsregister en worden datalekken gerapporteerd.
Er zijn ook tekortkomingen. Uit het beleid blijkt geen strategische visie op het onderwerp. Die is er wel voor informatiebeveiliging. Het privacybeleid is sinds 2018 weinig geactualiseerd. Weliswaar wordt er aan inwoners meegedeeld hoe de gemeente omgaat met hun persoonsgegevens, deze informatie is niet meer compleet en actueel. Het informatiebeveiligingsbeleid op de website is verouderd en moet worden geactualiseerd.

Weliswaar is aannemelijk dat medewerkers van de gemeente vooral dankzij de e-learningmodules bekend zijn met het thema privacy, dat betekent niet automatisch dat zij (voldoende) bekend zijn met het privacybeleid van de gemeente. De e-learningmodules worden ervaren als nuttig en leerzaam. Sommige medewerkers zijn bovengemiddeld goed bekend met de inhoud en vereisten van het privacybeleid, omdat zij hier zelf de nut en noodzaak van inzien. Dit kwam onder meer naar voren tijdens de mini-Privacy Impact Assesment (mini-PIA) over het Noodfonds.

In gangbare overleggen binnen de gemeentelijke organisatie is privacy geen thema dat met regelmaat wordt besproken, of waar de ambtelijke organisatie op wordt aangesproken. Als het ter sprake komt, gebeurt dat met name door medewerkers die vanuit hun kennis en ervaring affiniteit hebben met het onderwerp. Verschillende mensen in de ambtelijke organisatie geven aan dat zij het belangrijk vinden zorgvuldig om te gaan met persoonsgegevens en ze te behandelen zoals zij ook willen dat anderen met hun persoonsgegevens omgaan. Er zijn binnen de organisatie zeker de nodige kundige en proactieve medewerkers die op eigen initiatief met het onderwerp aan de slag gaan. Maar de organisatie leunt daarbij toch vooral op de toevallige affiniteit van individuele medewerkers. Er zijn binnen elk gemeentelijk team zogeheten teamcoaches, die onder andere aandacht zouden moeten geven aan privacy. Hun precieze rol en verantwoordelijkheid ervaren zij echter niet als duidelijk, waardoor zij geen proactieve houding op dit thema innemen.

Privacyrisico's en (juridische) ontwikkelingen worden niet actief, structureel en overzichtelijk in kaart gebracht of gemonitord. De AVG vereist dat hiervoor Data Protection Impact Assessments (DPIA's) worden uitgevoerd. Daarvan is nauwelijks sprake. Binnen de ambtelijke organisatie is sprake van onvoldoende bewustzijn over de inzet van dit middel. Binnen de huidige organisatiestructuur (waarin de functies van Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) zijn verenigd in één medewerker), is het lastig voor de CISO hierin een aanjagende rol te spelen. De organisatie mist op het moment van dit onderzoek de capaciteit en juridische kennis om het

privacybeleid te professionaliseren. Er wordt organisatiebreed (nog) weinig geanticipeerd op toekomstige opgaven en juridische ontwikkelingen.

De meeste activiteiten die horen te liggen bij een FG en een privacy officer zijn opgepakt door de CISO. De AVG vereist een onafhankelijke FG. De Autoriteit Persoonsgegevens heeft aangegeven dat deze rol niet door de CISO kan worden ingevuld, omdat dit verhindert dat de FG onafhankelijk het beleid kan controleren. De CISO is zich ervan bewust dat deze rollen niet kunnen worden gecombineerd en is bezig hier een oplossing voor te zoeken. Niet alleen is het, met het oog op de eisen die aan beide rollen worden gesteld, onhoudbaar om ze samen te nemen, het is ook te veel werk voor één persoon.

Het informatiebeveiligingsbeleid van Noordwijk is dusdanig uitgewerkt dat het medewerkers die er uitvoering aan moeten geven, duidelijke richtlijnen verschaft. In de uitvoering van het beleid is er ook voldoende aandacht voor risicomanagement, door middel van het inrichten van regelmatige controles en de Eenduidige Normatiek Single Information Audit (ENSIA) rapportage.

De gemeenteraad wordt op verschillende manieren geïnformeerd. De raads- en commissieleden antwoorden wisselend over of zij voldoende geïnformeerd worden. Zij vinden het vooral belangrijk om geïnformeerd te worden over de uitgangspunten van het privacybeleid. Een kleinere groep vraagt om specifieke aandacht voor die domeinen waar veel met persoonsgegevens wordt verwerkt. Een belangrijk deel van de raadsleden (circa één op de vijf) is van mening dat zij hun controlerende verantwoordelijkheid niet goed kunnen uitvoeren. In het coalitieakkoord zijn geen kaders op het gebied van ICT en privacy beschreven.

Aanbevelingen aan het College van B&W

De juridische en praktische borging van de privacy van inwoners schiet op verschillende vlakken te kort. Daarom doet de rekenkamercommissie op basis van het privacyonderzoek de volgende aanbevelingen aan het college met betrekking tot de omgang met persoonsgegevens:

- Wijs zo spoedig mogelijk een onafhankelijk FG en een privacy officer aan;
- Draag aan de onafhankelijke FG op om ieder jaar aan het college van B&W verslag uit te brengen over de stand van zaken in het privacybeleid;
- Werk het beleid uit, op een dusdanige wijze dat dit duidelijke en concrete richtlijnen verschaft aan alle medewerkers;
- Geef hier vervolg aan in concrete beleidsregels en procedures;
- Besteed in de uitwerking van het beleid ook aandacht aan de specifieke taken en verantwoordelijkheden van voor het privacybeleid cruciale functionarissen, zoals met name de FG, de CISO, de privacy officer en de teamcoaches;
- Draag er zorg voor dat regelmatig DPIA's worden uitgevoerd;
- Besteed eveneens aandacht aan de verantwoordelijkheden met betrekking tot privacy die tot het reguliere werk behoren van elke medewerker, en geef ook aan op welke wijze directie en teamleiders de naleving daarvan bewaken;
- Beïnvloed de organisatiecultuur op een dusdanige wijze dat het belang van de naleving van privacy integraal onderdeel uitmaakt van het denken en handelen van elke medewerker;
- Bespreek de uitgangspunten van het (nieuwe) privacybeleid met de raad voordat deze worden vastgesteld.

Aanbevelingen aan de gemeenteraad

De rekenkamercommissie heeft de volgende aanbeveling aan de gemeenteraad:

- Agendeer het privacybeleid zo spoedig mogelijk;
- Bespreek de uitgangspunten van het gewenste privacybeleid en stel deze vast;
- Leg vast hoe de raad door het college van B&W geïnformeerd wordt over de stand van zaken in het privacybeleid;

1. Inleiding

1.1 Aanleiding en opdracht

Privacy is een belangrijk grondrecht. Iedereen heeft het recht om niet continue te worden gevolgd, om te weten welke beslissingen er worden genomen op basis van zijn (persoons)gegevens en om na te gaan of dit op een goede manier is verlopen. Overheden beheren veel persoonsgegevens 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. Burgers moeten ervan uit kunnen gaan dat hun gegevens bij de gemeente in veilige handen zijn.

Gemeenten moeten dat vertrouwen verdienen, zowel in de directe contacten met de burger als in verantwoordingen achteraf. Veel gemeenten hebben daar de laatste jaren, mede vanwege de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) al ruim aandacht aan gegeven. Onder meer als gevolg van de AVG lopen gemeenten risico op boetes in het geval zij niet conform de geldende normen de beveiliging van persoonsgegevens op orde hebben.

Het maatschappelijk belang van een adequaat privacybeleid en een strikte uitvoering daarvan zijn al met al sterk toegenomen. In het verleden is de vertrouwelijkheid van persoonsgegevens in Noordwijk niet altijd gegarandeerd.[1] In dit licht heeft de rekenkamercommissie van de gemeente Noordwijk een onderzoek geïnitieerd naar de wijze waarop deze gemeente uitvoering geeft aan de bescherming van persoonsgegevens van inwoners van de gemeente Noordwijk, zowel in beleid als in de uitvoeringspraktijk. Aan de basis van het onderzoek staat de volgende onderzoeksvraag:

Centrale onderzoeksvraag

Hoe is in het licht van de verdergaande digitalisering de privacy van inwoners juridisch en in de praktijk geborgd en op welke punten behoeft dit eventueel aanpassingenverbetering?

Deze centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen.

Deelvragen

1. Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de (juridische) borging van privacy van inwoners?
2. Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Overheid (BIO)[2], BRP 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?
5. Hoe worden medewerkers betrokken bij en getraind in het borgen van de privacy van inwoners?
6. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop de privacy van inwoners is geborgd binnen de gemeente?

[1] https://www.rtlnieuws.nl/nederland/artikel/2576661/gevoelige-gegevens-1800-kwetsbare-kinderen-op-straat
[2] De BIG is per 1 januari 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO)

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?
8. Hoe communiceert de gemeente naar inwoners over de wijze waarop zij omgaat met persoonsgegevens?
9. Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?

1.2 Normenkader

Het normenkader is gebaseerd op relevante en actuele kaders voor privacy- en informatiebeveiligingsbeleid, zoals de AVG en de BIO, en de ervaring van de onderzoekers. Het volgende normenkader is vastgesteld door de rekenkamer en gebruikt bij het beantwoorden van de vragen.

Gehanteerde norm

Gemeentelijk beleid

- 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.
- In het gemeentelijk beleid wordt ingegaan op:
  - Juridische aspecten op basis van de AVG en de materie wetten.
  - 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 Overheid.
- In de procesbeschrijvingen en instructies 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.
- 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 haar privacy-rechten, zowel schriftelijk als mondeling.

Uitvoeringspraktijk

- 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.
- Afspraken in verwerkersovereenkomsten met derden worden door de gemeente gemonitord en geverifieerd.
- De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt. Hierin is aandacht voor mogelijke (ongewenste) knelpunten.
- 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.
- Indien er sprake is geweest van een datalek, heeft de gemeente conform de vastgelegde procedure gehandeld.
- 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.
- In de praktijk wordt de raad conform de overeengekomen systematiek geïnformeerd over de ontwikkelingen in het privacybeleid.
- De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om hun sturende en controlerende verantwoordelijkheden waar te maken.

Leren en verbeteren

- 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, wat 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.
- 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.

Kaderstellende en controlerende rol van de raad

- In de jaarstukken 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 beleid heeft aandacht voor het waarborgen van privacy op de agenda van de Raad gestaan.

1.3 Werkwijze

Het onderzoek is begonnen met een startbijeenkomst waaraan de rekenkamer, de onderzoekers van PBLQ en de Chief Information Security Officer (CISO) van de gemeentelijke organisatie[3] deel hebben genomen. Binnen een organisatie is de CISO verantwoordelijk voor het informatiebeveiligingsbeleid. Vervolgens is kennisgenomen van relevante documenten. Aansluitend is in gesprekken met ambtenaren en portefeuillehouders allereerst ingegaan op het gemeentelijk beleid. Daarnaast is aandacht besteed aan de uitvoering van dit beleid en de ervaringen die daarbij zijn opgedaan.

Om inzicht te krijgen in de cultuur en het bewustzijn rondom privacy is aan de hand van een praktijkcasus ´Noodfonds aanvraag´ vanuit meerdere perspectieven (zoals juridisch en informatiekundig) bekeken welke privacy dilemma's er spelen. Verschillende betrokken ambtenaren bij het proces ´Noodfonds aanvraag´ hebben aan deze casus meegewerkt in een zogenaamde mini-Privacy Impact Assesment (mini-PIA). Met de deelnemers is het vraagstuk in kaart gebracht, zijn vragen gesteld over de werkwijze en waarborgen met betrekking tot dit fonds en is doorgevraagd waar risico's met betrekking tot de privacy bestaan. Ook is van gedachten gewisseld over eventuele maatregelen die zowel recht doen aan de privacy van de burger als aan het werk van de gemeente. Zo is niet alleen achterhaald of betrokkenen de afspraken kennen en naleven, maar ook of zij zich bewust zijn van privacy en op welke wijze dit onderwerp deel uitmaakt van de leer- en verbetercyclus.

[3] Als in deze rapportage gesproken wordt over 'de gemeentelijke organisatie' worden hier zowel de ambtelijke organisatie als het college van B&W bedoeld.

Om een beeld te verkrijgen van de opvattingen van de raad is een enquête afgenomen onder raadsleden en commissieleden. In deze enquête zijn vragen geweid aan de ambities van raadsleden met betrekking tot privacy. Eveneens is aan de orde geweest of zij hun sturende en controlerende verantwoordelijkheden rond dit onderwerp kunnen invullen.

Het veldwerk voor dit rekenkameronderzoek is in april 2021 afgesloten. Van eventuele ontwikkelingen en aanpassingen in het geldende beleid die nadien hebben plaatsgevonden, kan in deze rapportage niet altijd melding worden gemaakt.

1.4 Indeling rapport

Dit rapport is als volgt ingedeeld. In het volgende hoofdstuk worden de belangrijkste privacykaders voor dit onderzoek toegelicht. Vervolgens worden de bevindingen uiteengezet, parallel aan de indeling van de deelvragen. Er wordt eerst ingegaan op het gemeentelijk beleid, vervolgens wordt aandacht besteed aan de uitvoering van het beleid en de ervaringen van de raad. Elke paragraaf sluit af met een beoordeling van de relevante normen en de beantwoording van de relevante deelvragen.

2. De privacykaders

Het gemeentelijk privacybeleid van Noordwijk is weliswaar specifiek opgesteld voor Noordwijk, maar dat is natuurlijk gebeurd in de context van algemene wet- en regelgeving waaraan elke gemeente moet voldoen. Hieronder worden kort de belangrijkste ´algemene´ kaders en begrippen toegelicht waarbinnen de rekenkamer het privacybeleid van de gemeente Noordwijk beoordeeld. De eisen uit deze kaders zijn vertaald naar een normenkader (zie paragraaf 2.2).

Privacy en gegevensbescherming
De begrippen privacy en gegevensbescherming worden vaak uitwisselbaar gebruikt. Ze liggen ook in elkaars verlengde. Privacy is een mensenrecht en is als zodanig vastgelegd in verschillende mensenrechtenverdragen[4] en in de Grondwet. Het is een recht dat beschermt dat mensen onbespied mogen leven en ruimte moeten krijgen om hun eigen identiteit te vormen.

Privacy is geen absoluut recht. Er spelen ook andere belangen, zoals veiligheid of het recht op goede gezondheidszorg of het recht op een veilige omgeving, die moeten worden afgewogen tegen het recht op privacy. Soms wegen andere belangen zwaarder dan het recht op privacy. Het is belangrijk dat de afweging, om privacy al dan niet zwaarder te laten wegen dan andere belangen en rechten, expliciet wordt gemaakt in de vorm van beleid.

Het recht op bescherming van persoonsgegevens bepaalt dat zorgvuldig wordt omgegaan met (digitale) persoonsgegevens. Persoonsgegevens mogen niet zomaar door organisaties worden verwerkt. Als organisaties persoonsgegevens mogen verwerken moeten ze dit op een zorgvuldige, correcte en transparante wijze doen.

Algemene Verordening Gegevensbescherming (AVG)
Op 25 mei in 2018 trad de Algemene Verordening Gegevensbescherming (AVG) in werking. In Nederland verving deze Europese wet de Wet bescherming persoonsgegevens (Wbp). Hoewel de Wbp ook al vereiste dat gemeenten op een behoorlijke manier met persoonsgegevens moesten omgaan, was de AVG voor veel organisaties aanleiding om de omgang met persoonsgegevens te actualiseren en intensiveren. Een belangrijke verandering die de AVG met zich mee bracht was dat de Autoriteit Persoonsgegevens (AP) als toezichthouder bij misstanden boetes kan uitdelen. Deze stok achter de deur heeft organisaties doen inzien dat zij de bescherming van persoonsgegevens hoog op de agenda dienen te zetten.

[4] Art. 8 Europese Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden (EVRM) en art. 7 en 8 van het Handvest Grondrechten van de EU

De AVG[5] is een Europese wet die eisen stelt aan wanneer en hoe er met persoonsgegevens moet worden omgegaan door organisaties. Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet met een gerechtvaardigd doel. Bij het verwerken van persoonsgegevens moeten een aantal uitgangspunten in acht worden gehouden. Gemeenten moeten aan een de volgende vereisten voldoen:

- Er moet een actueel privacybeleid zijn.
- Alle categorieën van verwerkingen moeten worden opgenomen in een overzicht. Dit heet het verwerkingsregister.
- Organisaties moeten zo min mogelijk gegevens verwerken. Dit wordt ook wel dataminimalisatie genoemd.
- Er moet op een behoorlijke, zorgvuldige en veilige manier met gegevens worden gewerkt. Hiervoor moeten technische en organisatorische maatregelen worden genomen.
- Overheidsorganen moeten een interne onafhankelijke toezichthouder hebben, namelijk een functionaris gegevensbescherming (FG). Deze eis komt voort uit de AVG.[6][7]
- Het handelen van de gemeente moet helder en transparant zijn.
- Gemeentelijke processen moeten uitlegbaar zijn.
- De omgang met persoonsgegevens moet worden gecommuniceerd naar inwoners op een manier die aansluit bij zijn of haar belevingswereld.
- In een aantal gevallen[8] is de gemeente verplicht privacyrisico's in kaart te brengen. Dit heet een gegevenseffectbeoordeling of een Privacy/Data Portection Impact Assessment.

In de praktijk is er vaak naast een FG ook een privacy officer werkzaam bij een organisatie. De privacy officer is geen onafhankelijke toezichthouder, maar een medewerker van de organisatie met een expertise op privacy. Deze medewerker helpt collega's op de werkvloer met vragen over privacy en ondersteunt de organisatie met het voldoen aan de wettelijke verplichtingen. Het is niet verplicht vanuit de AVG om een privacy officer in dienst te hebben. Het hebben van een FG is wel wettelijk verplicht. Een FG kan in dienst zijn van de organisatie waar hij toezicht op houdt, maar moet zijn functie zonder druk, onafhankelijk kunnen uitvoeren.

Wat is een DPIA?

DPIA staat voor *Data Protection Impact Assessment*. Dit wordt ook wel een Gegevenseffectbeoordeling of een Privacy Impact Assessment (PIA) genoemd. De AVG vereist dat er in verschillende situaties, bijvoorbeeld bij grootschalige verwerking van persoonsgegevens, vooraf aan die verwerking moet worden bepaald wat het effect van de geplande verwerkingsactiviteit is op de bescherming van de persoonsgegevens van een persoon. Een DPIA is een manier om dit te doen. Een DPIA geeft inzicht in de impact van de verwerking op de privacy van deze persoon. Op basis van een DPIA kunnen maatregelen worden genomen om de impact zo nodig te verminderen.

---

[5] De AVG is een Europese Verordening. Deze verordening heeft directe werking in Nederland en gaat boven Nederlandse wetgeving.
[6] In de 'Richtlijnen voor functionarissen voor gegevensbescherming van de Werkgroep gegevensbescherming artikel 29 staat hoe een FG zijn rol moet invullen.
[7] Er is ook een externe toezichthouder. In Nederland is dat de Autoriteit Persoonsgegevens(AP). De AP kan boetes opleggen wanneer een organisatie niet voldoet aan de eisen van de AVG.
[8] De AP heeft gespecificeerd in welke gevallen dit precies is. Deze lijst is te vinden op: Definitieve DPIA-lijst beschikbaar | Autoriteit Persoonsgegevens

Veel eisen aan gegevensbescherming zijn verder uitgewerkt in nationale wetten. Zo is er veel wetgeving die aanvullende eisen stelt aan hoe er met gezondheidsgegevens moet worden omgegaan, bijvoorbeeld de Wet op de Geneeskundige Behandel Overeenkomst (WGBO) en stelt de Participatiewet eisen aan wie wanneer gegevens mag uitwisselen bij het uitkeren van financiële hulp aan een bijstandsgerechtigde.

Baseline Informatiebeveiliging
Informatiebeveiliging is het proces van het nemen en beheren van passende technische en organisatorische maatregelen om dit te garanderen. Omdat de AVG stelt dat er technische en organisatorische maatregelen moeten worden ondernomen ten aanzien van de verwerking van persoonsgegevens, is er overlap tussen privacy en informatiebeveiliging. Voor Nederlandse overheden is de Baseline Informatiebeveiliging Overheid (BIO) als normenkader van toepassing. In de BIO zijn (verplichte) beheersmaatregelen opgenomen. Verder gaat de BIO uit van risicomanagement op basis van een Plan-Do-Check-Act cyclus om de beveiliging continue bij te stellen en te verbeteren. Voor de verantwoording over informatiebeveiliging gebruiken gemeenten de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). Via deze systematiek legt de gemeente verantwoording af over de informatieveiligheid van een aantal basisregistraties en informatiestelsels (waaronder de Basisregistratie Personen, DigiD en Suwinet).

Een Chief Information Security Officer (CISO) heeft een toezichthoudende en controlerende rol op het gebied van informatiebeveiliging. Meestal coördineert de CISO ook de rapportageverplichtingen over de ontwikkelingen rondom informatiebeveiliging. Organisaties zijn niet wettelijk verplicht een CISO te hebben. De AP heeft verduidelijkt dat de functie CISO niet verenigbaar is met het vervullen van de functie van de FG, omdat de FG dan niet onafhankelijk kan opereren.

Basisregistratie Personen
Gemeenten houden persoonsgegevens[9] van burgers bij in de Basisregistratie Personen (BRP). Hier worden voornamen, achternaam, geslacht en het burgerservicenummer (BSN), maar ook andere gegevens zoals of iemand is getrouwd, in opgeslagen. Niet iedereen in de gemeente mag deze gegevens zomaar inzien of gebruiken. In de Wet Basisregistratie personen (Wet BRP) zijn hiervoor regels opgesteld. Via de ENSIA rapportage leggen gemeenten verantwoording af over hun gebruik van de BRP.

In Bijlage D en E staat een overzicht met een definitie- en afkortingslijst.

[9] Voor een overzicht van de meeste gegevens zie Welke gegevens staan er in de Basisregistratie Personen (BRP)? | Rijksoverheid.nl

3. Het gemeentelijk beleid

3.1 Beleidskaders

Deelvragen

1.	Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de (juridische) borging van privacy van inwoners?
2.	Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Overheid (BIO), BRP en vanaf 25 mei 2018 aan de algemene verordening gegevensbescherming (AVG)?

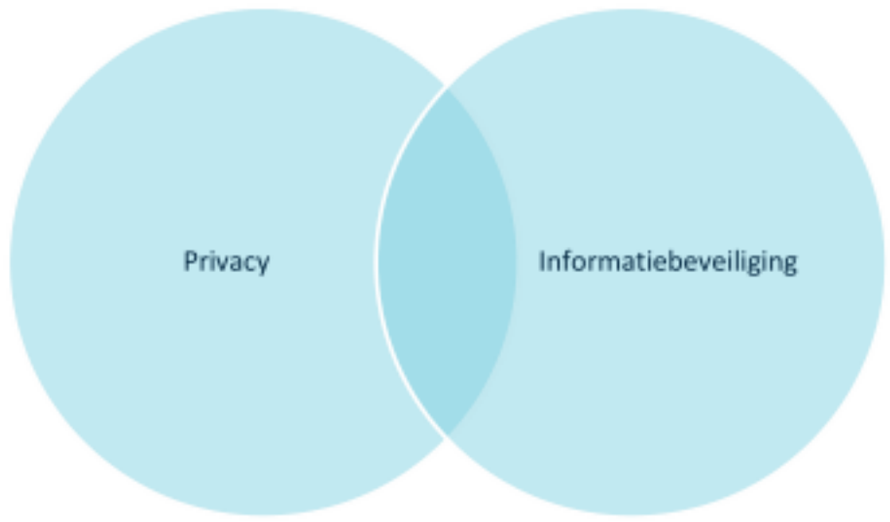
Het huidige privacybeleid van de gemeente Noordwijk vindt haar oorsprong in 2018. Zoals het geval bij de meeste organisaties was de inwerkingtreding van de AVG een belangrijke aanleiding om een nieuw privacybeleid op te stellen. De Vereniging van Nederlandse Gemeenten (VNG) heeft in 2018, om gemeentes te helpen bij de transitie naar de AVG, een model Privacybeleid en -reglement[10] voor gemeenten opgesteld. Ook heeft de VNG andere modellen opgesteld, zoals standaardverwerkersovereenkomsten[11] en een modelprivacyverklaring die gemeenten helpen de basis op orde te stellen.

Het Privacybeleid en het Reglement van Noordwijk zijn gebaseerd op het VNG model. Hierin worden de belangrijkste aspecten toegelicht: de van toepassing zijnde wettelijke kaders en de belangrijkste uitgangspunten voor het beleid. In het VNG model is er rekening mee gehouden dat het privacybeleid begrijpelijk moet zijn voor inwoners door juridische jargon zo veel mogelijk te vermijden. In het Privacyreglement wordt uitgebreider stilgestaan bij de belangrijkste begrippen uit de AVG, zoals ‘persoonsgegeven’ en wordt met meer diepgang dan in het Privacybeleid ingegaan op de samenhang van de AVG met andere wetgeving, zoals de Wet openbaarheid van bestuur (Wob). Ook is er aandacht voor geautomatiseerde verwerkingen, big data en tracking en de inzet van camera’s.

Het beleid is in 2018 opgesteld door de CISO. De CISO is in 2018 ook benoemd als FG. In 2019 is hij ook benoemd als FG voor de gemeenteraad en de rekenkamer.[12] Hij was de medewerker met de meeste kennis van privacy en informatiebeveiliging. De CISO heeft het beleid met het MT besproken. Het College van B&W is eindverantwoordelijk voor de bescherming van persoonsgegevens binnen de gemeente. Het meest recente beleid komt uit 2019.[13] Het privacybeleid stelt dat dit beleid jaarlijks wordt geëvalueerd. Een uitgebreide evaluatie heeft in 2019 niet plaatsgevonden. Het huidige Privacybeleid en -Reglement zijn vastgesteld in april 2019 en komen overeen met het eerdergenoemde beleid uit 2018. In 2019 is gemeente Noordwijk gefuseerd met gemeente Noordwijkerhout tot één nieuwe fusiegemeente. Hierbij is het privacybeleid van (voorheen) gemeente Noordwijk overgenomen.

[10] Vereniging van Nederlandse Gemeenten, Model Privacybeleid en – reglement, januari 2018
[11] De AVG stelt verplicht dat verwerkingsverantwoordelijke, de organisatie de eindverantwoordelijk is voor de verwerking van persoonsgegevens, overeenkomsten afsluit met organisaties die in opdracht verwerkingen uitvoeren. Deze overeenkomsten heten verwerkersovereenkomsten.
[12] Gemeente Noordwijk, Aanwijzen functionaris gegevensbescherming gemeenteraad, 18 juni 2019
[13] Gemeente Noordwijk, Privacybeleid, 1 april 2019

Het Privacybeleid is aangevuld met een strategisch Informatiebeveiligingsbeleid 2020 - 2023.[14] Dit beleid is gebaseerd op de Europese informatiebeveiligingsstandaarden NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). Dit meerjarenplan wordt jaarlijks verder uitgewerkt in overleg met de directie in het informatiebeveiligingsplan (IBP). In het beleid worden de beveiligingseisen uit wetgeving benoemd en meegenomen.[15]



Centrale principes van het informatiebeveiligingsbeleid

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

Het informatiebeveiligingsbeleid pleit er duidelijk voor om informatiebeveiliging ook bestuurlijk aandacht te geven. Het beleid stoelt op een aantal uitgangspunten:

- Het beleid is van toepassing op de gehele organisatie dat wil zeggen ‘alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen)’[16].
- Het college van BenW is eindverantwoordelijk voor de informatiebeveiliging.
- De directie en teamcoaches zijn verantwoordelijk voor de uitvoering. Tegelijkertijd heeft iedere medewerker de verantwoordelijkheid om gegevens en informatiesystemen te beschermen door zorgvuldig om te gaan met deze systemen en wanneer dit niet gebeurt hiervan melding te maken.
- Er wordt gekeken naar informatiebeveiliging als een continu verbeterproces waarvoor deze uitgangspunten het vertrekpunt zijn.

De gemeente neemt deel aan ENSIA controles en legt via deze weg verantwoording af over het informatiebeveiligingsbeleid. De CISO verzamelt alle benodigde informatie. De verantwoording wordt ook beschreven in het jaarverslag. Dit is ook het document waarin het bestuur en de raad worden geïnformeerd.

Het informatiebeveiligingsbeleid is nader uitgewerkt. Dit geldt zowel voor de uitgangspunten, de governance (de verdeling van de rollen van verantwoordelijkheden) en de uitwerking van het beleid op strategisch, tactisch en operationeel niveau. Het privacybeleid is op hoofdlijnen uitgewerkt.

---

[14] Gemeente Noordwijk, Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Noordwijk 2020-2023, december 2019

[15] Het gaat om eisen die voortkomen uit Basisregistratie Personen (BRP), Paspoorten en Nederlandse identieitskaarten (PNIK) en Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), Paspoortuitvoeringsregeling (PUN), Basisregistratie Adressen en Gebouwen (BAG) en Basisregistratie Grootschalige Topografie (BGT).

[16] Gemeente Noordwijk, Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Noordwijk 2020-2023, december 2019, p. 5

Het privacy- en informatiebeveiligingsbeleid zijn aangevuld door een Gedragscode[17], en verschillende procedures, bijvoorbeeld over datalekken[18] en over hoe moet worden omgegaan met rechten van burgers die voortkomen uit de AVG. Er is ook een wachtwoordbeleid. Dit zijn praktische documenten die medewerkers inzicht geven in hoe zij privacybewust behoren te handelen. Enkele domeinen hebben afzonderlijk nog aanvullend privacybeleid opgesteld.[19] Een deel van het privacybeleid is niet omschreven in een beleidsstuk, maar komt wel tot uiting in functionele eisen in het zaaksysteem waar in de gemeente mee wordt gewerkt. Alleen bepaalde personen zijn geautoriseerd bepaalde informatie in te zien en deze te verwerken. De wijze waarop deze verwerkingen moeten plaatsvinden is beschreven in het zaaksysteem.

Beoordeling normen t.a.v. Gemeentelijk beleid

• Het gemeentelijk beleid[20] voldoet tenminste aan de eisen die in wet- en regelgeving worden gesteld: generiek aan de AVG, en specifiek voor de genoemde materiewetten. • In het schriftelijk gemeentelijk beleid wordt ingegaan op: – Juridische aspecten op basis van de AVG en de materie wetten – 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.	Onvoldoende	De gemeente voldoet niet aan alle eisen die worden gesteld door de AVG, zo is er momenteel geen onafhankelijke FG.
	Voldoende	Het privacybeleid[21] uit 2019 samen met het Strategisch informatiebeveiligingsbeleid 2020 – 2023[22] beschrijft genoemde aspecten. Het privacybeleid is zeer beknopt en gaat weinig in op de betekenis van het beleid in de context van gemeente Noordwijk.
• De gemeente hanteert landelijke standaarden, zoals de Baseline Informatiebeveiliging Overheid.	Goed	De BIO is het uitgangspunt voor het Strategisch Gemeentelijk Informatiebeveiligingsbeleid 2020-2023.
• In de procesbeschrijvingen en instructies is duidelijk welke functionaris welke gegevens in welke processtap mag verwerken, en onder welke condities dat mag.	Voldoende	Of er voldoende procesbeschrijvingen en instructies zijn verschil per team.
• De gemeente heeft beleid voor incidenten waarbij sprake is van schending van de privacy van inwoners. Dit beleid voldoet aan de wettelijke vereisten.	Voldoende	Er is een procedure[23] om incidenten, waaronder datalekken te melden.
• 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	Voldoende	De gemeente heeft een privacyreglement[24] en een privacyverklaring[25] waarin inwoners kunnen lezen hoe de gemeente met persoonsgegevens omgaat.

[17] Gemeente Noordwijk, Gedragscode voor de publicatie van persoonsgegevens door de gemeente raad van de gemeente Noordwijk
[18] Gemeente Noordwijk, Datalek melden – procesbeschrijving, 2020 en Gemeente Noordwijk, Processen rechten burgers (art. 15,16,17 AVG)
[19] Bijvoorbeeld in de Handleiding Burgerzaken
[20] Hiermee wordt bedoeld het gemeentelijk beleid in brede zin waar het privacybeleidsstuk onderdeel van maakt, alsmede de benoeming van de juiste functionarissen en het hebben van verplichte procedures zoals in het geval van een datalek.
[21] Gemeente Noordwijk, Privacybeleid gemeente Noordwijk – openbaar, 2019
[22] Gemeente Noordwijk, Strategische Gemeentelijk Informatiebeveiligingsbeleid Gemeente Noordwijk 2020 – 2023, december 2019
[23] Gemeente Noordwijk, Proces datalek melden, 2020
[24] Gemeente Noordwijk, Privacyreglement gemeente Noordwijk, 2019
[25] www.noordwijk.nl/privacyverklaring

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.	Voldoende	De bovengenoemde documenten zijn toegankelijk geschreven. Daarnaast kunnen inwoners mailen of bellen met vragen, opmerkingen of klachten.

Beantwoording deelvragen

1.	*Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de (juridische) borging van privacy van inwoners?*
Antw.	De belangrijkste beleidskaders staan beschreven in het privacybeleid en het informatiebeveiligingsbeleid. Er is een privacybeleid en een privacyreglement. Het privacybeleid geeft een overzicht van de basis vereisten en beginselen uit de AVG aan de gemeente. Het informatiebeveiligingsbeleid staat beschreven in het 'Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Noordwijk 2020 – 2023'. Er is een jaarplanning, maar er is geen meerjarenplan.
2.	*Voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Overheid (BIO), BRP en vanaf 25 mei 2018 aan de algemene verordening gegevensbescherming (AVG)?*
Antw.	Het beleid voldoet aan de minimale vereisten. Het privacybeleid voldoet aan de minimale vereisten van de AVG, maar geeft medewerkers weinig handvatten voor het omgaan met privacy in hun dagelijkse werkzaamheden. De eisen vanuit de BRP zijn omgezet in verschillende processen. Het informatiebeveiligingsbeleid is nader uitgewerkt op strategisch, tactisch en operationeel niveau.

3.2 Uitvoering van het beleid

	Deelvraag
3.	Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?

Privacy is een gemeentebreed thema en het privacybeleid is van toepassing op heel de gemeente. Een belangrijke rol bij uitvoering van het privacybeleid is weggelegd voor de teamcoaches. De gemeente Noordwijk is na de herindeling in 2019 zelforganiserend gaan werken. De gemeente Noordwijk bestaat uit 31 zelforganiserende teams. Deze teams zijn opgedeeld in 13 secties. In Bijlage F is een overzicht opgenomen van de organisatiestructuur.

De ambtelijke organisatie is opgedeeld in teams met teamcoaches. De teams werken aan doelen, maar bepalen zelf hoe zij dit organiseren en bereiken. De teamcoaches zijn, naast coaches voor zelforganiserende teams, ook eindverantwoordelijk voor hun domein. Zij worden geacht een schakel te zijn tussen de teams en het college van B&W. De teamcoaches ondersteunen ambtenaren bij het bereiken van vastgestelde beleidsdoelen in integraliteit met andere teams. Teamcoaches zijn gemandateerd proceseigenaar en zijn verantwoordelijk voor privacy en informatiebeveiliging binnen hun teams. In de praktijk blijkt het lastig dat de teamcoaches door het zelforganiserende karakter van de teams verder van de inhoud staan, terwijl de directie dit op gebied van privacy wel van hen verlangt.

Het privacybeleid werd ten tijde van dit onderzoek gecoördineerd door de CISO. De CISO monitort ontwikkelingen op het gebied van privacy en houdt onder andere het verwerkingsregister bij. Dit gebeurt voor informatiebeveiliging structureel voor alle beveiligingsmaatregelen. De privacy ontwikkelingen worden op hoofdlijnen gemonitord. De CISO is onderdeel van het team Informatie- en gegevensmanagement (team IGM), het team dat gaat over het informatiebeleid van de gemeente. Gemeenten kiezen er steeds vaker voor om de CISO op te nemen in de directie danwel het MT. De gemeente Noordwijk heeft er bewust voor gekozen de CISO niet toe te voegen aan de directie, omdat de verwachting was dat zij dan ook andere bedrijfsvoering rollen zouden moeten toevoegen zoals control en juridische zaken wat zou leiden tot een te grote directie.

Vooralsnog vervult de CISO ook nog de rol van Functionaris Gegevensbescherming (FG). Tot voor kort vervulde de CISO ook de rol van privacy officer. Afgelopen jaar is een privacy officer aangenomen, maar het precieze werkpakket van deze persoon was ten tijde van het onderzoek nog niet helder. Hij was nog niet voldoende ingewerkt om deel te kunnen nemen aan dit onderzoek. De opdracht voor de Privacy Officer was om het eerste aanspreekpunt te zijn voor vragen uit de organisatie en het monitoren van de actielijnen uit het privacybeleid.

Gewoonlijk is de FG de onafhankelijke interne toezichthouder van de gemeente. De FG moet zijn werk naar eigen inzicht kunnen uitvoeren. Daarom is het ook gebruikelijk dat de FG zich niet te veel met uitvoerende taken bezig houdt. Als dat het geval is, is het namelijk moeilijk voor een FG diezelfde taken onafhankelijk te controleren. Dit is een belangrijke reden voor het gescheiden houden van de rol van FG en de rol van CISO. De CISO voert namelijk taken uit op het gebied van informatiebeveiliging. Informatiebeveiliging is een belangrijk onderdeel van de bescherming van persoonsgegevens en wordt ook in de AVG benoemd. Een FG moet een onafhankelijke positie kunnen innemen ten aanzien van het informatiebeveiligingsbeleid. Als de FG tevens CISO is, is dat volgens de AP niet mogelijk.

De gemeente Noordwijk is zich ervan bewust dat de rol van FG en CISO niet bij één persoon behoren te liggen. Gelijktijdig aan het onderzoek bekeek de gemeente Noordwijk of de rol van FG en PO anders konden worden belegd. De gemeente is van plan de FG rol interim te beleggen voor de komende twee jaar. Daarna zal worden gekeken of deze rol structureel kan worden belegd en of hierin kan worden samengewerkt met omliggende gemeenten. De PO zou zich bezig gaan houden met de dagelijkse uitvoering van het privacybeleid.

De CISO is onafhankelijk en rapporteert zelfstandig aan het college en de raad. Verschillende medewerkers geven aan de weg naar de CISO te kennen en hem ook om hulp te vragen indien zij dit nodig achten. Het is onduidelijk of dat geldt voor zowel het thema privacy als het thema informatiebeveiliging. Wanneer de FG danwel PO ruggenspraak wil houden, kan deze een advocatenkantoor inschakelen als hulplijn.

Als de gemeente een derde partij opdracht geeft om namens de gemeente persoonsgegevens te verwerken, is de gemeente verplicht een verwerkersovereenkomst af te sluiten. Een verwerkersovereenkomst is een overeenkomst waarin de gemeente afspreekt met een derde partij op welke manier deze in opdracht van de gemeente persoonsgegevens moet verwerken. De gemeente maakt voor het opstellen van verwerkersovereenkomsten gebruik van de standaard VNG verwerkersovereenkomst. Vooralsnog tekent de gemeentesecretaris alle verwerkersovereenkomsten, maar in de toekomst gaat dit naar de teamcoaches.

Het privacybeleid is uitgewerkt in een paar processen binnen het zaaksysteem. De gemeente is bezig de werkprocessen verder te beschrijven. Wanneer sprake is van een proces in de gemeente met gegevensverwerkingen die een hoog privacy risico opleveren voor de mensen van wie gegevens worden verwerkt, dan dient de gemeente een Privacy Impact Assesment (PIA) uit te voeren waarbij systematisch in kaart wordt gebracht wat de risico's zijn van de gegevensverwerking. De gemeente Noordwijk voert zeer weinig PIA´s uit. Tijdens het onderzoek waren er twee uitgevoerde PIA's bekend. De gemeente streeft ernaar inhoudelijke teams zelf de PIA te laten uitvoeren, waarbij de FG meekijkt om zijn akkoord te geven op de conclusies.

Voorbeeld Casus Noodfonds

Wanneer sprake is van een proces in de gemeente met gegevensverwerkingen die een hoog privacy risico opleveren voor de mensen van wie gegevens worden verwerkt, dan dient de gemeente een Privacy Impact Assesment (PIA) uit te voeren waarbij systematisch in kaart wordt gebracht wat de risico's zijn van de gegevensverwerking. In een workshop is samen, met een aantal medewerkers, de omgang met persoonsgegevens in het kader van 'Noodfonds aanvragen' op eenzelfde wijze onderzocht. De workshop had als doel inzicht te verkrijgen in de cultuur van de organisatie en hoe er in de dagelijkse praktijk met privacydilemma's wordt omgegaan.

Er is een noodfonds voor inwoners van de gemeente Noordwijk die financieel in de knel raken door onverwachte kosten. Inwoners kunnen een aanvraag doen als er geen andere voorzieningen zijn (zoals bijvoorbeeld bijzondere bijstand). Het noodfonds is niet bedoeld voor betalingsachterstanden, boetes of problemen die de inwoner zelf had kunnen voorkomen. Het noodfonds is voor een incidentele, eenmalige acute persoonlijke financiële situatie.

Een inwoner dient een aanvraag voor het noodfonds in via een ingevulde PDF. Alleen behandelaars mogen zaken inzien via het zaaksysteem. Eventueel vraagt de behandelaar extra informatie over schulden of schuldhulpverlening bij de aanvrager. Wanneer een besluit is genomen wordt de inwoner telefonisch op de hoogte gebracht van het besluit en volgt bij afwijzing nog een beschikking per brief. Het Digitale Informatievoorziening team handelt de afronding van het dossier af. Er is een bewaartermijn. Voor vernietiging van gegevens hanteert Noordwijk de vernietigingslijst van de VNG.

De betrokken ambtenaren zijn zich bewust van het vertrouwelijke karakter van de informatie en handelen hier ook naar. Betrokken ambtenaren bij het proces willen stigmatisering voorkomen en het vertrouwen van inwoners niet beschamen.

Het enkele privacy risico dat de betrokken ambtenaren onderkennen is wanneer een aanvraag ten onrechte in een "verzamelbak" in het zaaksysteem terecht komt en niet direct bij de geautoriseerde ambtenaar. Maatregelen die reeds zijn getroffen omvatten het afschermen van aanvragen voor de rest van de organisatie. Bij overleg tussen ambtenaren wordt nooit de identiteit van de aanvrager vrijgegeven. Alleen de behandelaar is hiervan op de hoogte. Noordwijk heeft het proces 'Noodfonds aanvragen' sinds kort in eigen beheer. De kennis over de privacymaatregelen t.a.v. het noodfonds liggen maar bij enkele personen. Personen die verder van de directe uitvoering staan, zijn ook een stuk minder op de hoogte welke privacymaatregelen in het proces zijn ingebouwd.

Beoordeling normen t.a.v. Uitvoeringspraktijk		Toelichting
• 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.	Voldoende	Medewerkers handelen conform de voor hun werk opgestelde werkprocessen wanneer de werkprocessen beschikbaar zijn.
• Afspraken in verwerkersovereenkomsten met derden worden door de gemeente gemonitord en geverifieerd.	Voldoende	De CISO heeft overzicht op de lopende verwerkingsovereenkomsten.
• Indien er sprake is geweest van een datalek, heeft de gemeente conform de vastgelegde procedure gehandeld.	Goed	Er wordt conform procedure gehandeld.
• In de praktijk wordt de raad conform de overeengekomen systematiek geïnformeerd over de ontwikkelingen in het privacybeleid.	Voldoende	In de jaarstukken en via raadsbrieven wordt de raad geïnformeerd.
• De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken.	Onvoldoende	De huidige informatievoorziening is niet voor alle raadsleden altijd voldoende en/of volledig

Deelvragen

3. Hoe is dit beleid uitgewerkt en geborgd in processen op de werkvloer?

Antw. Het beleid is uitgewerkt in verschillende processen. Nog niet alle processen zijn in kaart gebracht. Sommigen zijn beschreven in beleidsstukken of handreikingen. Anderen zijn omgezet in functionele eisen in het zaaksysteem.

Teamcoaches zijn verantwoordelijk voor de gegevensbescherming binnen hun domein. Feitelijk worden de processen op dit moment met name geborgd door individuele medewerkers met kennis van privacy en IT.

3.3 Leren en verbeteren

Deelvragen

4. Zijn er casussen waarin sprake is van schending van de privacy van inwoners en hoe is daarmee omgegaan?
5. Hoe worden medewerkers betrokken bij en getraind in het borgen van de privacy van inwoners?

De gemeente biedt haar medewerkers online workshops, zogeheten e-learnings, aan op het gebied van privacy en informatiebeveiliging. De e-learnings behandelen een variatie aan thema´s (van fysieke toegang tot het gemeentehuis tot phishing) en zijn verplicht om te volgen binnen een bepaald tijdsbestek. In ontwikkelgesprekken is aandacht voor het al dan niet voltooien van de e-learnings. Certificaten worden dan ook opgenomen in het personeelsdossier. Over het algemeen zijn ambtenaren positief over de e-learnings.

Nieuwe medewerkers ontvangen bij aanstelling het privacy reglement en leggen een ambtseed af. Ambtenaren die veel met persoonsgegevens werken tekenen tevens een document waarin zij beloven veilig om te gaan met middelen en gegevens. De bewustwording rond privacy stijgt. Er worden steeds vaker vragen gesteld over privacy. Die vragen geven blijk van een basisbegrip van de thematiek.

Er is een overzicht van de datalekken in de gemeente. Ten tijde van dit onderzoeken waren er in 2021 acht bekend waarvan er twee zijn gemeld bij de Autoriteit Persoonsgegevens. Wanneer sprake is van een datalek, wordt contact gezocht met enerzijds de persoon die de verkeerde informatie heeft ontvangen en anderzijds met de persoon wiens informatie onterecht verstuurd is naar de verkeerde. De bekende incidenten zijn gemeld bij de CISO. Het is niet verplicht alle datalekken te melden bij de AP. Een enkele keer was er reden voor de CISO om het datalek te melden bij de Autoriteit Persoonsgegevens.[26] In sommige gevallen wordt het incident geëvalueerd, om na te gaan of en hoe het voorkomen had kunnen worden. In andere gevallen krijgt de ambtelijke organisatie onvoldoende feedback van de CISO. Wat mogelijk te verklaren is door een gebrek aan capaciteit.

Privacy wordt als onderwerp niet structureel besproken in de huidige overlegstructuren (zoals teamoverleggen). Het onderwerp staat nergens structureel op de agenda. Op de werkvloer wordt zonder specifieke aanleiding weinig gepraat over privacy. Dit onderzoek is uitgevoerd in de periode dat het overgrote deel van de werknemers vanuit huis werkte. In deze situatie is het (extra) lastig met collega's het onderwerp te bespreken, laat staan elkaar erop aan te spreken. De directie vindt het belangrijk dat gemeentebrede informatie via intranet wordt verspreid. Het intranet wordt echter nog weinig gebruikt en gelezen.

De meeste medewerkers zij niet bekend met het privacybeleid. Enkele medewerkers zijn dit wel, omdat zij persoonlijke affiniteit hebben met het onderwerp. Vooral binnen het sociaal domein en burgerzaken hebben ambtenaren vanuit eigen initiatief oog voor het thema privacy. Hierop wordt weinig gestuurd vanuit de teamcoaches. Over het algemeen zijn dit domeinen waar veel met persoonsgegevens wordt gewerkt. Verschillende mensen in de ambtelijke organisatie geven zelf aan dat zij het belangrijk vinden zorgvuldig om te gaan met persoonsgegevens en ze te behandelen zoals zij ook willen dat anderen met hun persoonsgegevens omgaan. Er zijn kundige en proactieve medewerkers aanwezig die op eigen initiatief met het onderwerp aan de slag gaan.

Beoordeling normen t.a.v. Leren en verbeteren		
• De gemeente heeft vastgelegd hoe en wanneer medewerkers worden getraind in / er aandacht besteed wordt aan het onderwerp privacy.	Voldoende	Elke medewerker moet een e-learning module te volgen over het onderwerp. Voor teamcoaches zouden er aanvullende trainingsmogelijkheden moeten worden geboden.
• 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.	Goed	Functioneel beheerders en medewerkers van team IGM houden toezicht op genoemde aspecten.
• Het controleplan sluit aan op het gemeentelijk beveiligingsplan en op het Integriteitsbeleid.	Voldoende	Dit is het geval, als wordt dit niet door alle raadsleden als voldoende ervaren.

[26] De belangrijkste richtlijn voor het melden van datalekken is: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf

• De medewerkers zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens. • 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.	Onvoldoende Voldoende Voldoende	Niet alle medewerkers zijn bekend met het beleid. Dit betekent niet dat zij niet conform het privacybeleid handelen. In praktijk wordt er conform werkprocessen gehandeld. Er zijn trainingsmogelijkheden, deze zijn (nog) niet cyclisch, maar dit is wel het plan.

Deelvragen

	4. Zijn er casussen waarin sprake is van schending van de privacy van inwoners en hoe is daarmee omgegaan?
Antw.	Er zijn enkele casussen bekend waar sprake was van een datalek. Deze zijn volgens procedure voor datalekken afgehandeld en zo nodig zijn inwoners geïnformeerd over het datalek.
	5. Hoe worden medewerkers betrokken bij en getraind in het borgen van de privacy van inwoners?
Antw.	Alle medewerkers volgen een e-learning module over privacy en informatieveiligheid. Medewerkers worden ook in de gelegenheid gesteld aanvullende cursussen over privacy te volgen als zij daar zelf om vragen. Privacy maakt standaard geen onderdeel uit van het inwerkprogramma van alle medewerkers. Toch zijn niet alle medewerkers op de hoogte van het privacybeleid. Nieuwe medewerkers die zich in hun werk in het bijzonder richten op privacy worden wel ingewerkt op dit thema.

3.4 Inwoners

Deelvraag

6. Hoe communiceert de gemeente naar inwoners over de wijze waarop zij omgaat met persoonsgegevens?

Het beschermen van de persoonsgegevens van inwoners is het belangrijkste doel van privacybeleid. Inwoners hebben een aantal specifieke rechten[27] ten aanzien van hoe hun persoonsgegevens worden verwerkt. Inwoners hebben onder andere het recht op inzage; zij mogen de gemeente vragen welke gegevens die over hen verwerkt. Ook hebben ze recht op duidelijke informatie over het beleid van de gemeente en de wijze waarop de gemeente persoonsgegevens verwerkt. Dit maakt dat de gemeente niet alleen verplicht is een privacybeleid te hebben, maar ook om dit beleid in begrijpelijke taal te communiceren naar inwoners.

[27] Rechten van betrokkenen | Autoriteit Persoonsgegevens

De gemeente communiceert op haar website over de wijze waarop zij met persoonsgegevens omgaat. Op de website staat de privacyverklaring[28], twee versies van het privacyreglement[29] en het informatiebeveiligingsbeleid van Noordwijk uit 2016[30]. Het is onduidelijk voor inwoners welk privacyreglement de juiste is. Inhoudelijk verschillen ze echter vrijwel niet van elkaar.

In de privacyverklaring wordt bondig uitgelegd wat persoonsgegevens zijn, dat er bewaartermijnen worden gehanteerd, hoe wordt omgegaan met cookies, voor welke risico´s zij maatregelen nemen en wat rechten zijn van betrokkenen. Daarnaast wordt verwezen naar het emailadres van de functionaris gegevensbescherming en is een link opgenomen naar het privacyreglement van de gemeente.

Het is in de afgelopen drie jaar slechts een enkele keer voorgekomen dat iemand zijn gegevens heeft opgevraagd. Deze verzoeken zijn ingewilligd volgens de hiervoor opgestelde procedure. Er is duidelijk gemaakt welke verwerkingen hadden plaatsgevonden met welke persoonsgegevens. Het toesturen van deze informatie aan degene die hierom vroeg is zo veilig mogelijk gebeurd. De gemeente heeft de aanvrager gevraagd naar het gemeentekantoor te komen. Zo weet de gemeente zeker dat de aanvrager is wie die zegt dat hij is. Dit voorkomt dat gegevens worden gestuurd naar de verkeerde persoon. Indien een aanvrager niet in staat is naar het gemeentehuis te komen, wordt de identiteit van de indiener digitaal gecontroleerd en worden de gegevens via beveiligde mail verstuurd.

Inwoners hebben de mogelijkheid om via de balie vragen te stellen. Bij het directe contact tussen de gemeente en inwoners worden inwoners indien relevant ook geïnformeerd over hoe de gemeente persoonsgegevens verwerkt. In sommige gevallen, wanneer de wet dit vereist, wordt aan inwoners toestemming gevraagd om hun gegevens te verwerken.

Beoordeling normen t.a.v. Communicatie		Toelichting
• De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.	Goed	De gemeente heeft een privacyreglement[31] en een privacyverklaring[32] waarin inwoners kunnen lezen hoe de gemeente met persoonsgegevens omgaat.
• 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.	Goed	De bovengenoemde documenten zijn toegankelijk geschreven. Daarnaast kunnen inwoners mailen of bellen met vragen, opmerkingen of klachten. Inzageprocedures worden conform beleid afgehandeld.

[28] Privacyverklaring - Gemeente Noordwijk
[29] https://www.noordwijk.nl/dsresource?objectid=26e1d1b2-cda1-46ff-891f-f7c3470406f9&type=pdf en https://www.noordwijk.nl/dsresource?objectid=1ad772c5-aca5-4c9b-8686-986b9d925533&type=pdf
[30] https://www.noordwijk.nl/dsresource?objectid=36f562e2-89ee-42ec-bfd6-02f75ffe9c34&type=pdf
[31] Gemeente Noordwijk, Privacyreglement gemeente Noordwijk, 2019
[32] www.noordwijk.nl/privacyverklaring

Deelvraag

6.	*Hoe communiceert de gemeente naar inwoners over de wijze waarop zij omgaat met persoonsgegevens?*
Antw.	De gemeente communiceert op haar website over de wijze waarop zij met persoonsgegevens omgaat in het kader van de AVG en BRP. Ook kunnen inwoners via de balie vragen stellen. Bij het directe contact tussen de gemeente en inwoners worden inwoners indien relevant ook geïnformeerd over hoe de gemeente persoonsgegevens verwerkt.

3.5 Risico's en nieuwe ontwikkelingen

Deelvragen

7.	Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop de privacy van inwoners is geborgd binnen de gemeente?
8.	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?

Hieronder volgen risico's en ontwikkelingen die invloed hebben op het privacybeleid van de gemeente.

(Juridische) privacyrisico's worden niet stelselmatig in kaart gebracht. De AVG schrijft voor dat organisaties regelmatig DPIA's uitvoeren. Bij de gemeente Noordwijk is nog geen praktijk ontstaan waar dit ook gebeurt. Het uitvoeren van DPIA's is een organisatiebrede verantwoordelijkheid. Medewerkers zouden zelf moeten kunnen signaleren wanneer het nodig is om een DPIA uit te voeren en zo'n DPIA moeten kunnen uitvoeren, eventueel met ondersteuning van de privacy officer of een FG.

Privacy staat niet vast op de agenda bij de overleggen van het team Informatie- en gegevensmanagement. Er is op het moment van het onderzoek in het team Informatie- en gegevensmanagement weinig juridische kennis over privacy aanwezig. Dit maakt het lastig voor de teamleden om juridische ontwikkelingen, bijvoorbeeld nieuwe wetgeving die van invloed kan zijn op de wijze waarop de gemeente persoonsgegevens verwerkt, proactief op te merken. Daarnaast is er weinig capaciteit. De meeste taken liggen bij de CISO. Er wordt op dit moment voornamelijk reactief omgegaan met ontwikkelingen.

De gemeente houdt technische ontwikkelingen en risico's met betrekking tot de informatieveiligheid wel in de gaten. Dit is mogelijk omdat op het gebied van informatiebeveiliging een strategische visie is opgesteld die ook is geoperationaliseerd. Zowel in het team Informatie- en gegevensmanagement als het team functioneel beheer is aandacht voor risico's en risicomanagement. In deze teams zijn werknemers werkzaam met kennis en kunde over processen, beveiliging, optimalisering en functioneel beheer.

Regelmatig vinden controles plaats op hoe systemen worden gebruikt. Het team functioneel beheer draait maandelijks een overzicht uit waarin staat welke rollen en rechten medewerkers hebben in het systeem. De CISO controleert vervolgens dit overzicht. Dit voorkomt dat personen die geen reden hebben de gegevens in te zien toegang hebben tot die gegevens. Deze controles zijn ook nodig omdat sommige personen zichzelf meer rechten kunnen geven. Dit maakt het extra belangrijk dat de verdeling van rechten regelmatig wordt gecontroleerd. Ook de logging, inzicht in wanneer een

medewerker een bepaald systeem heeft geraadpleegd, wordt gecontroleerd. De overzichten worden opgeslagen op een tijdelijke schijf die dagelijks worden geleegd.

De CISO zorgt voor een deugdelijke ENSIA rapportage. Om te voldoen aan deze verplichting worden vragenlijsten gebruikt waarin alle relevante informatie voor de rapportage is aangegeven. De CISO vult deze in overleg met de relevante medewerkers in.

Bij aanschaf van nieuwe applicaties worden over het algemeen de eisen en wensen vanuit privacyperspectief meegenomen door de CISO. Wat deze eisen zijn is niet altijd duidelijk voor andere personen die moeten werken met deze applicaties.

De gemeente is gestart met het in kaart brengen van processen in het algemeen, omdat de controller hiernaar heeft gevraagd. Bij deze inventarisatie is in het bijzonder aandacht voor rechtmatigheid en privacy. Er wordt bij deze inventarisatie ook in kaart gebracht in welke processen precies persoonsgegevens worden verwerkt.

Beoordeling normen t.a.v. Uitvoeringspraktijk		**Toelichting**
• De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt. Hierin is aandacht voor mogelijke (ongewenste) knelpunten.	Voldoende	De CISO monitort ontwikkelingen rondom privacy. De worden besproken in team IGM. De uitkomsten worden aan de raad gecommuniceerd via raadbrieven. Waar nodig wordt beleid herzien. Door gebrek aan capaciteit kunnen niet alle knelpunten worden geconstateerd.
• 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.	Voldoende	Dit proces vindt plaats op het gebied van informatiebeveiliging.

Deelvragen

	7. Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop de privacy van inwoners is geborgd binnen de gemeente?
Antw.	Er is op dit moment nog geen organisatiebreed overzicht van alle processen en in hoeverre er in deze processen privacyrisico's voor inwoners zijn. Wel is de gemeente hiermee gestart. Ook is er (nog) geen praktijk waar er bij veranderingen of nieuwe wetgeving door medewerkers DPIA's worden uitgevoerd. Daarnaast is er ten tijde van het onderzoek geen onafhankelijke toezichthouder (FG). Dit kan nadelige gevolgen hebben voor inwoners. Hierdoor kunnen er onder andere datalekken plaatsvinden die door maatregelen hadden kunnen worden voorkomen en kunnen er onnodig te veel persoonsgegevens worden verzameld of worden bewaard dan nodig.
	8. 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?
Antw.	Er wordt organisatiebreed (nog) weinig geanticipeerd op toekomstige opgaven en juridische ontwikkelingen. Dit gebeurt wel voor informatiebeveiligingsrisico's. De gemeente is gestart met het in kaart brengen van processen waar persoonsgegevens worden verwerkt.

Momenteel wordt er met name ad hoc met nieuwe ontwikkelingen omgegaan. Individuele medewerkers met veel affiniteit met privacy pakken sporadisch op eigen initiatief vraagstukken op.

3.6 De rol van de gemeenteraad

Deelvragen

9. Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?

De gemeenteraad heeft een kaderstellende en controlerende taak. Om deze taak goed te kunnen vervullen moet zij goed en tijdig worden geïnformeerd. Voor dit onderzoek is gekeken naar de wijze waarop de raad wordt geïnformeerd. Ook is geïnventariseerd welke opvattingen raadsleden zelf hebben over de ontwikkelingen rondom het privacybeleid. Hiertoe is een enquête uitgestuurd waar alle fracties op één na aan hebben deelgenomen. De enquête stond open voor zowel raadsleden als commissieleden. In deze paragraaf wordt eerst de wijze waarop de raad wordt geïnformeerd besproken. Vervolgens worden de resultaten van de enquête beschreven.

Bij de gemeente Noordwijk wordt de gemeenteraad op verschillende manieren geïnformeerd. Allereerst wordt over privacy en informatiebeveiliging gerapporteerd via een aantal algemene stukken, namelijk: het jaarverslag en de programmabegroting. In deze stukken worden de activiteiten op het gebied van informatiebeveiliging uitgebreider beschreven dan het privacybeleid.

Daarnaast wordt de raad jaarlijks via een raadsbrief uitgebreid geïnformeerd over de voortgang op het gebied van informatieveiligheid en op hoofdlijnen over de ontwikkelingen op het gebied van privacy.

De informatie over de ontwikkelingen op het gebied van informatiebeveiliging worden systematisch beschreven. De jaarlijkse raadsbrieven hebben een eenduidige systematiek, waardoor het inzichtelijk is welke voortgang is geboekt. De te nemen maatregelen op het gebied van informatiebeveiliging zijn onderverdeeld in 11 categorieën. In totaal zijn er 303 maatregelen. Per categorie wordt inzichtelijk gemaakt wat er moet gebeuren en wat de voortgang is. Uit de verschillende Raadsinformatiebrieven blijkt een duidelijke vooruitgang bij de implementatie van de maatregelen. De voortang op het gebied van privacy is beknopt beschreven.

De raad kan actief vragen stellen over het privacybeleid. Dit gebeurt incidenteel. Zo was er bijvoorbeeld in 2020 een landelijk incident met Citrix, een digitale omgeving die door veel overheden wordt gebruikt. Naar aanleiding van dit incident zijn er door de raad vragen gesteld aan het college van B en W. De raad heeft geen kaders opgesteld ten aanzien van privacy. In het coalitieakkoord wordt geen aandacht besteed aan ICT. Ook wordt hier geen aandacht gegeven aan privacy en informatiebeveiliging. De hierboven beschreven stukken die jaarlijks aan de raad over privacy en informatiebeveiliging worden gestuurd worden doorgaans meegenomen als hamerstukken.

De ambtelijke organisatie heeft het voornemen de raad meer te gaan informeren over privacy d.m.v. een jaarverslag waarin iets uitgebreider wordt gerapporteerd over bijvoorbeeld de controles die de FG heeft uitgevoerd.

Uit de enquête blijkt dat raadsleden zeer verschillend kijken naar het privacybeleid van de gemeente Noordwijk. De helft van de respondenten geeft aan matig of onvoldoende bekend te zijn met het huidig privacybeleid. Er is een grote verscheidenheid van opvattingen over de huidige informatie die wordt aangeleverd. Deze wordt van 'uitstekend' tot 'onvoldoende' beoordeeld. Vier deelnemers aan de enquête vonden de informatie onvoldoende, vier matig, vier voldoende, twee goed en maar één uitstekend. Een kwart van de respondenten vindt de huidige wijze waarop het college van B en W de gemeenteraad informeert onvoldoende.

De meeste raads- en commissieleden vinden het belangrijk om bij de ontwikkeling van het privacy beleid te worden meegenomen. Hierbij willen de meeste respondenten, meer dan de helft, geïnformeerd worden over de uitgangspunten van het privacybeleid. Voor een derde van de respondenten is het ook belangrijk te worden geïnformeerd over specifieke ontwikkelingen uit domeinen waar veel met persoonsgegevens wordt gewerkt.

40% van de respondenten valt op dat het onderwerp privacy steeds meer aandacht heeft gekregen in de gemeente in de afgelopen drie jaar. 40% vindt dat er nu nog precies hetzelfde met privacy wordt omgegaan als in 2018. Slechts één vindt dat privacy steeds minder aandacht heeft gekregen in de gemeente.

Op de vraag of de respondenten hun controlerende verantwoordelijkheid op het privacy beleid van de gemeente kunnen uitvoeren werd zeer wisselend geantwoord. Een kwart van de respondenten antwoordt ja, een kwart antwoord soms. Eveneens een kwart antwoordt 'weet het niet'. Een vijfde van de raadsleden laat weten dat zij niet hun controlerende verantwoordelijkheid kunnen waarmaken. Over het algemeen is er weinig verschil in de resultaten te zien tussen de opvatting van raadsleden en commissieleden. Het enige dat opvalt is dat raadsleden negatiever zijn over of zij de controlerende rol als raadslid kunnen vervullen dan de commissieleden.

Beoordeling normen t.a.v. de kaderstellende en controlerende rol van de raad		
• In de jaarstukken 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.	Voldoende	De onderwerpen privacy en informatiebeveiliging worden benoemd in het jaarverslag en de begroting.
• Bij de ontwikkeling van beleid heeft aandacht voor het waarborgen van privacy op de agenda van de Raad gestaan.	Onvoldoende	Er is voornamelijk ad hoc aandacht voor privacy bij de raad. Het onderwerp is niet opgenomen in het coalitieakkoord opgenomen.

Deelvraag

9.	*Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?*
Antw.	Het college van BenW informeert de raad met name over vorderingen op het gebied van Informatiebeveiliging. De raad wordt op hoofdlijnen geïnformeerd over de ontwikkelingen op het gebied van privacy. Dit gebeurt in raadsbrieven en in het jaarverslag.

Een groot deel van de raadsleden ervaart de informatie als onvoldoende om te kunnen sturen en controleren.

4. Conclusies

Er is bij de gemeente Noordwijk in de afgelopen jaren op verschillende manieren gewerkt aan het borgen van de privacy van inwoners. Dit vond plaats terwijl er door de fusie van Noordwijk en Noordwijkerhout ook sprake was van een grote organisatieverandering. De inwerkingtreding van de AVG was een belangrijke aanleiding om het privacybeleid te actualiseren en te versterken. In dit hoofdstuk wordt de centrale onderzoeksvraag beantwoord en worden de conclusies gepresenteerd.

De centrale onderzoeksvraag luidt:

Hoe is in het licht van de verdergaande digitalisering de privacy van inwoners juridisch en in de praktijk geborgd en op welke punten behoeft dit eventueel aanpassing en verbetering?

De gemeente Noordwijk borgt de privacy van inwoners in haar privacybeleid en informatiebeveiligingsbeleid. Er worden wat dit beleid betreft verschillende eisen aan gemeenten gesteld. De belangrijkste eisen komen voort uit de AVG. De gemeente voldoet aan een aantal van deze vereisten. Er is sprake van privacybeleid. Het privacybeleid is naar aanleiding van de inwerkingtreding van de AVG aangepast. Het beleid legt op hoofdlijnen uit hoe de gemeente Noordwijk omgaat met persoonsgegevens. Uit het beleid blijkt echter geen strategische visie op het onderwerp. Daarvan is wel sprake als het gaat om informatiebeveiliging. Het privacybeleid is sinds 2018 weinig geactualiseerd. Wel is er sprake van een verwerkingsregister en worden datalekken gerapporteerd. Er wordt aan de inwoners bekend gemaakt hoe de gemeente omgaat met hun persoonsgegevens, maar deze informatie is niet compleet en actueel. Het informatiebeveiligingsbeleid is verouderd en zou moeten worden vervangen voor het nieuwe beleid.

Niet alle medewerkers zijn (voldoende) bekend met het privacybeleid van de gemeente. Wel zijn ze bekend met het thema privacy dankzij de e-learningsmodule. Deze module wordt ervaren als nuttig en leerzaam. Sommige medewerkers zijn bovengemiddeld goed op de hoogte op het gebied van privacy, omdat zij hier zelf de nut en noodzaak van inzien. Dit kwam ook naar voren tijdens de mini-PIA over het Noodfonds.

In gangbare overleggen binnen de gemeentelijke organisatie is privacy geen thema dat met regelmaat wordt besproken, of waar de ambtelijke organisatie op wordt aangesproken. Als het ter sprake komt, gebeurt dat met name door medewerkers die vanuit hun kennis en ervaring affiniteit hebben met het onderwerp. Verschillende mensen in de ambtelijke organisatie geven aan dat zij het belangrijk vinden zorgvuldig om te gaan met persoonsgegevens en ze te behandelen zoals zij ook willen dat anderen met hun persoonsgegevens omgaan. Er zijn binnen de organisatie zeker de nodige kundige en proactieve medewerkers die op eigen initiatief met het onderwerp aan de slag gaan. Maar de organisatie leunt daarbij toch vooral op de toevallige affiniteit van individuele medewerkers. Er zijn binnen elk gemeentelijk team zogeheten coaches aangesteld, die aandacht zouden moeten geven aan privacy. Hun precieze rol en verantwoordelijkheid ervaren zij echter niet als duidelijk, waardoor zij geen proactieve houding op dit thema innemen.

Privacyrisico's en (juridische) ontwikkelingen worden niet actief, structureel en overzichtelijk in kaart gebracht of gemonitord. De AVG vereist dat hiervoor DPIA's worden uitgevoerd. Daarvan is nauwelijks sprake. Binnen de ambtelijke organisatie is er sprake van onvoldoende bewustzijn over de inzet van dit middel. Binnen de huidige organisatiestructuur (waarin de functies van CISO en FG zijn verenigd in één medewerker), is het lastig voor de CISO hierin een aanjagende rol te spelen. De organisatie mist op het moment van dit onderzoek de capaciteit en juridische kennis om het privacybeleid te professionaliseren. Er wordt organisatiebreed (nog) weinig geanticipeerd op toekomstige opgaven en juridische ontwikkelingen.

De meeste activiteiten die horen te liggen bij een FG en een privacy officer zijn opgepakt door de CISO. De AVG vereist een onafhankelijke FG. De Autoriteit Persoonsgegevens heeft aangegeven dat deze rol niet door de CISO kan worden ingevuld, omdat dit verhindert dat de FG onafhankelijk het beleid kan controleren. De CISO is er zich van bewust dat deze rollen niet kunnen worden gecombineerd en is bezig hier een oplossing voor te zoeken. Niet alleen is met het oog op de eisen die aan beide rollen worden gesteld onhoudbaar om ze samen te nemen, het is ook te veel werk voor één persoon.

Het informatiebeveiligingsbeleid van Noordwijk is dusdanig uitgewerkt dat het medewerkers die er uitvoering aan moeten geven, duidelijke richtlijnen verschaft. In de uitvoering van de beleid is er ook voldoende aandacht voor risicomanagement, door middel van het inrichten van regelmatige controles en de ENSIA rapportage.

De gemeenteraad wordt op verschillende manieren geïnformeerd. De raads- en commissieleden antwoorden wisselend over of zij voldoende geïnformeerd worden. Zij vinden het vooral belangrijk om geïnformeerd te worden over de uitgangspunten van het privacybeleid. Een kleinere groep vraagt om specifieke aandacht voor die domeinen waar veel met persoonsgegevens wordt verwerkt. Een belangrijk deel van de raadsleden (circa één op de vijf) is van mening dat zij hun controlerende verantwoordelijkheid niet goed kunnen uitvoeren. In het coalitieakkoord zijn geen kaders op het gebied van ICT en privacy beschreven.

Bijlage A Geïnterviewde personen

Naam	Rol/organisatie
[redacted]	Adviseur KCC
	Adviseur informatie en gegevensmanagement
	Teamcoach BOG, BOC, PCI, IGM
	Teamcoach MAS, OSS, DIV
	Projectleider Sociaal Domein
	Procesregisseur zorg en veiligheid
	CISO
	Adviseur processen informatievoorziening en gegevensbeheer
	Burgemeester Noordwijk

Bijlage B Aanwezigen Mini-PIA Noodfonds

Naam	Rol/organisatie
[redacted]	Teamcoach MAS, OSS, DIV
	Projectleider Sociaal Domein
	Procesregisseur zorg en veiligheid
	CISO
	Adviseur Maatschappij
	Secretaris RKC

Bijlage C Bestudeerde documentatie

Documentnaam
140819 Schriftelijke vragen ex art. 46 inzake privacymaatregelen nav 3D D66
190821 - 9312 B&W Voortgang informatieveiligheid en privacy
190821 - 9312 B&W Voortgang informatieveiligheid en privacyVerantwoordingsrapportage-BAG-2018-Noordwijk raad
200514 - Bijlage - Hoe beschermen we maximaal de privacy
201221 - 83638 - B&W - Voortgang informatieveiligheid en privacy 2020
B&W - Privacybeleid- en Privacyreglement
C03 171219 Brief college Voortgang informatieveiligheid en privacy
C09 181120 Brief college over voortgang informatieveiligheid en privacy 2018
Formulier inspraakreactie privacy (002)
Gemeente Noordwijk - Voortgang informatieveiligheid en privacy 2018 Noordwijkerhout
Memo Wvg en privacy definitief

Antwoordbrief op schriftelijke vragen DOEN! ICT beveiliging Noordwijk
Antwoordbrief schriftelijke vragen Wifi tracking
B_W advies Besluit gegevensverstrekking Gemeentelijke Belastingen Bollenstreek (1)
Bijlage 1 bij besluit gegevensverstrekking Gemeentelijke Belastingen Bollenstreek
Bijlage 2 bij besluit gegevensverstrekking Gemeentelijke Belastingen Bollenstreek
Brief aan de raad voortgang informatieveiligheid en privacy 2019
Brief aan de raad voortgang informatieveiligheid en privacy 2020
Gedragscode raad Noordwijk
Handreiking processen optimaliseren v1.0
Privacybeleid gemeente Noordwijk (voor medewerkers)
Privacyreglement gemeente Noordwijk (voor inwoners)
Proces datalek melden
Proces rechten burgers art. 15,16,17 AVG
Raadsbesluit FG Raad
Strategisch Gemeentelijk Informatiebeveiligingbeleid Noordwijk 2020-2023
Trainingen sociaal domein
Uitnodiging E-learning informatieveiligheid en privacy SEP mei 2019
Uitnodiging E-learning privacy Nexttech mei 2018
Uitnodiging E-learning privacy SEP december 2020
Voorbeeld beslissing inzageverzoek
17022021 Concept Intentieverklaring privacy sociaal domein Duin- en Bollenstreek
Agenda projectgroep Beveiliging 18-03-2021
Change proces TopDesk CISO FG
DPIA Meld een Vermoeden
Overzicht datalekken en AVG verzoeken 20202
Verwerkersovereenkomst DataMask
Wachtwoordbeleid gemeente Noordwijk
Bijlage HR pptx intake start proces optimaliseren v0.2
Format proces beschrijven v1.1
Handreiking processen optimaliseren v1.0
Processen in beeld voortgang
Coalitieakkoord 2019-2022 gemeente Noordwijk
Jaarstukken gemeente Noordwijk 2019
organisatieplaatje tbv OF rapport deel 2

Bijlage D Definitielijst

Begrip	Definitie
Datalek	toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie
Informatiebeveiliging	net nemen van passende technische en organisatorische maatregelen nemen om informatie veilig te houden
Persoonsgegeven	alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare levende natuurlijke persoon
Privacy	eerbiediging van de persoonlijke levenssfeer
Verwerking	elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens
Verwerkingsverantwoordelijke	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt
Verwerker	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerk

Bijlage E Afkortingslijst

Afkorting	Betekenis
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging
BRP	Basisregistratie personen
BSN	Burgerservicenummer
CISO	Chief Information en Security Officer
DPIA	Data Protection Impact Assessment
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris Gegevensbescherming
PIA	Privacy Impact Assessment
Wbp	Wet bescherming persoonsgegevens
Wob	Wet openbaarheid van bestuur
VNG	Vereniging Nederlandse Gemeenten

Bijlage F Organisatiestructuur gemeente Noordwijk

Overzicht vaste teams

PBLQ

verbinders in de
informatiesamenleving

Bijlage G Bestuurlijk wederhoor

gemeente
Noordwijk

Aan de leden van de rekenkamer

Voorstraat 42
2201 HW Noordwijk

Postbus 298
2200 AG Noordwijk

T +31 (0)71 36 60 000

gemeente@noordwijk.nl
www.noordwijk.nl

KvK nummer 73538469
BTW NL8257.92.150.B01
IBAN NL34BNGH0285044621
BIC BNGHNL2G

Noordwijk, 28 september 2021

Uw kenmerk	:
Uw mail van	: 19 augustus 2021
Zaaknummer	: 168488
Behandeld door	: [redacted]
Verzenddatum	: 29 SEP. 2021
Onderwerp	: Hoor- en wederhoor conceptrapport 'Onderzoek bescherming persoonsgegevens'
Bijlagen	:

Geachte leden van de rekenkamer,

Inleiding

In augustus heeft u het conceptrapport 'Onderzoek bescherming persoonsgegevens' aangeboden voor hoor- en wederhoor.

In onze vergadering van 21 september 2021 hebben wij het volgende besluit hierin genomen.

Besluit:

I. Kennis te nemen van het conceptrapport onderzoek bescherming persoonsgegevens.
II. In te stemmen met de conclusie en aanbevelingen uit het rapport.

Dit betekent tevens dat het college geen op- of aanmerkingen heeft op het rapport. Wij danken u voor de gedane aanbevelingen.

Hoogachtend,

Namens Burgemeester en wethouders van Noordwijk

R. van Zijl
loco-secretaris

Mw. W.J.A. Verkleij
burgemeester

Gemeente Noordwijk, Noordwijk, Noordwijkerhout & De Zilk

Bijlage H Nawoord Rekenkamer

De Rekenkamer heeft met genoegen kennis genomen van de volledige instemming van het College van B&W met de resultaten en adviezen van haar onderzoek naar de borging – zowel juridisch als in de dagelijkse praktijk – van de privacy van de inwoners van de gemeente Noordwijk.
Te meer, daar de adviezen die de Rekenkamer aan de gemeenteraad doet een uiteenlopend karakter hebben. Een deel van onze adviezen zal immers naar verhouding relatief snel geïmplementeerd kunnen worden, terwijl andere adviezen toch wellicht een wat langere organisationele adem vergen. Het zal hierbij vooral gaan om het een gedurende langere termijn verlenen en uitdragen van prioriteit en werk maken van de culturele inbedding in de organisatie. Zaken die gesteund kunnen worden actieve overname van de meer beleidsmatige en structurele adviezen (quick wins).
De Rekenkamer is gezien het verkregen brede draagvlak hoopvol dat haar adviezen tot een betere borging van privacy zullen bijdragen en zal dan ook met veel interesse de verdere implementatie van haar adviezen volgen, voor zover deze vanzelfsprekend ook door de Gemeenteraad omarmd worden.

Mevr. Mr. Drs. V. Tsjebanova
Drs. W.G. Wever
Drs. A.W. Spitsbaard