

JAARRAPPORTAGE 2023 FUNCTIONARIS GEGEVENSBESCHERMING

ARJO BUURMA

6 FEBRUARI 2024

Samenvatting

Voor u ligt het jaarverslag 2023 van de Functionaris Gegevensbescherming van de gemeente Noordwijk. In dit verslag worden de acties beschreven die de gemeente in 2023 heeft gezet om aan de eisen van de Algemene verordening gegevensbescherming (AVG) te kunnen blijven voldoen. Kort samengevat komt dat op het volgende neer.

In het jaar 2023 heeft de gemeente Noordwijk verdere stappen gezet in de professionalisering van het privacybeleid waardoor het volwassenheidsniveau van de organisatie is verbeterd. Dat is mede bereikt door de verschillende rollen van de Privacy-Officer (PO), Functionaris Gegevensbescherming (FG) en de Chief

Information Security Officer (CISO) en de daarbij behorende verantwoordelijkheden te scheiden. Er is een geactualiseerd privacybeleid opgesteld. De geactualiseerde procedure waarlangs betrokkenen hun rechten als bedoeld in hoofdstuk III AVG kunnen uitoefenen, is definitief opgesteld en geïmplementeerd. De procedure waarlangs datalekken moeten worden afgehandeld, is herzien en aangepast.

De verantwoordelijkheden voor de gemeente Noordwijk voor het verwerken van persoonsgegevens van burgers liggen in hoofdlijnen bij drie bestuursorganen: de burgemeester, het college van B&W en de gemeenteraad. Het college is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens binnen de gemeente. Dit brengt verplichtingen met zich mee. In deze jaarrapportage staat beschreven welke acties en maatregelen de gemeente in 2023 heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2024. Adequaats omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers.

Inleiding

De gemeente Noordwijk is zich sterk bewust van het belang van het beschermen van persoonsgegevens van haar burgers. De gemeente verwerkt immers bij de uitoefening van haar taken veel (gevoelige) gegevens van veel (kwetsbare) burgers in veel verschillende domeinen. Daarnaast staan persoonsgegevens van andere burgers, medewerkers, externen en zakenrelaties op de radar.

In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente transparant te zijn over welke persoonsgegevens zij verwerkt, voor welk doel en op welke grondslag. Tijdens de levensduur van persoonsgegevens moeten ze goed worden beveiligd, mogen ze niet zomaar voor een ander doel worden verwerkt en moeten ze na afloop worden vernietigd of geanonimiseerd. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de gemeente.

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt externe en interne toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dienen de gemeente te beschikken over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). Op 8 november 2021 hebben de bestuursorganen van de gemeente Noordwijk Arjo Buurma aangesteld als FG.

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van zijn deskundigheid. De uitvoerende taken liggen bij de Privacy Officer (PO) en coördinatie voor de informatieveiligheid is belegd bij de Chief Information Security Officer (CISO).

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijken van zijn werkzaamheden, bevindingen en aanbevelingen. Dit jaarverslag is bedoeld voor de burgemeester, de gemeenteraad en het college van B&W.

Leeswijzer

Deze jaarrapportage bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar het jaar 2023. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG? In het tweede deel worden aanbevelingen gedaan om gegevensbescherming en privacy in het jaar 2024 naar een hoger niveau te tillen.

De thema's die in dit rapport worden genoemd zijn afkomstig uit het AVG-borgingsproduct van de Informatiebeveiligingsdienst (IBD).¹ Er worden zeven thema's onderscheiden:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording
8. Wet politiegegevens

Deel 1. Terugblik op 2023

1. Beleid

Het privacybeleid is een kader waarin de gemeente Noordwijk aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving. Het nieuwe privacybeleid is door het college formeel vastgesteld.

¹ Zie het document 'Criteria borging AVG/ Borgingsproduct gegevensbescherming in de gemeentelijke organisatie', [link](#).

Het in 2022 ontwikkelde privacy statement voor werknemers, leveranciers en voor sollicitanten dat door de gemeente Noordwijk is opgesteld, is op de website gepubliceerd. Tevens is in 2023 een privacyverklaring in het kader van de Wpg opgesteld en gepubliceerd

2. Processen

De verwerkingen van persoonsgegevens van de gemeente Noordwijk dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten, getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast kan de gemeente in gevallen verplicht zijn om een gegevensbeschermingseffectbeoordeling (DPIA²) uit te voeren.

Binnen de gemeente voeren de PO, FG en CISO tweemaandelijks overleg waarbij de stand van zaken met betrekking tot privacy en informatieveiligheid wordt besproken en wordt onderzocht of de geformuleerde afspraken en doelstellingen zijn nagekomen en behaald.

Binnen de gemeente is een procedure opgesteld waarlangs een Data Protection Impact Assessment (DPIA) moet worden uitgevoerd. Een DPIA is een instrument waarmee de verwachte risico's van een verwerking van persoonsgegevens in beeld gebracht kunnen worden. De betreffende afdeling waar de persoonsgegevens worden verwerkt, voert eerst een pre-DPIA uit conform het pre-DPIA template dat is opgesteld om te beoordelen of er sprake is van een verhoogd risico en een DPIA inderdaad noodzakelijk is. De FG wordt bij de DPIA betrokken, daarin is ruimte gereserveerd voor het commentaar en de eventuele aanwijzingen van de FG.

In 2023 is één DPIA uitgevoerd. Deze had betrekking op de Koppeling Gegevensmakelaar (BRP) ten behoeve van het Elektronisch Cliënten Dossier (ECD). Daarbij is vastgesteld dat aan de beginselen van dataminimalisatie en doelbinding wordt voldaan. De bewaartermijnen en de uitoefening van rechten door betrokkenen is geborgd.

Het proces om een DPIA uit te voeren op het gebruik van bodycams is gestart. De pre-DPIA vragenlijst wordt ingevuld. De grondslag is een bespreekpunt.

3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

In 2023 was voor alle interne en externe medewerkers een E-learning module privacy & Informatiebeveiliging beschikbaar. Voor nieuwe medewerkers wordt in het inwerkprogramma voorlichting gegeven over de juiste wijze van omgaan met persoonsgegevens en de begeleiding daarvan.

Binnen de gemeente Noordwijk is een autorisatiematrix afgesproken, aan de hand waarvan kan worden vastgesteld welke functionarissen toegang hebben tot systemen waarin persoonsgegevens zijn opgeslagen. De gemeente Noordwijk heeft een rollen- en rechtenprotocol opgesteld waarin de taken van de FG, PO, CISO en de Clustermanagers zijn vastgelegd en waaruit blijkt wie verantwoordelijk is voor welke verwerkingen van persoonsgegevens en in wel kader dat het geval is.

Op de website van gemeente Noordwijk is een nieuw meldformulier gepubliceerd: Melden kwetsbaarheid gemeentelijke systemen | Gemeente Noordwijk. Dit om te voorkomen dat men meer gegevens kan delen dan nodig is en in feite de gehele melding anoniem kan geschieden. Hiermee tracht de gemeente duidelijkheid te verschaffen over dit soort meldingen en daarmee wordt verantwoordelijkheid genomen ten aanzien van de gegevensverwerking die in dit kader plaatsvindt.

² De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

4. Rechten van betrokkenen

De gemeente dient degenen van wie zij de persoonsgegevens verwerkt (de betrokkenen) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen. Daarnaast stelt de AVG de betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

Een procedure waarlangs betrokkenen hun rechten als bedoeld in hoofdstuk III AVG kunnen uitoefenen is op 21 februari 2022 definitief opgesteld en geïmplementeerd. Het E-formulier voor uitoefenen rechten betrokkenen is gepubliceerd op de website. Eenzelfde procedure is opgesteld voor de Wpg, evenals een webformulier.

Op de website is de privacyverklaring gepubliceerd. Er is een nieuwe privacyverklaring opgesteld, evenals een nieuw cookiebeleid, deze is in 2023 gepubliceerd op de website. Daarin wordt beschreven welke persoonsgegevens de gemeente verwerkt en waarom en hoelang die persoonsgegevens worden bewaard en beveiligd en hoe betrokkenen hun rechten kunnen uitoefenen. De website bevat een link waarlangs een bericht kan worden gezonden aan de FG. Tevens wordt uitleg gegeven over het cookiebeleid.

Er is een register met een overzicht van de verzoeken van betrokkenen die in 2023 zijn ingediend.

5. Samenwerking

De gemeente Noordwijk werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeente Noordwijk dient dan ook afspraken te maken met deze andere partijen.

Er is een overzicht beschikbaar van alle verwerkers en de verwerkersovereenkomsten die daartoe zijn gesloten. Er is tevens een overzicht beschikbaar van alle partijen (niet zijnde verwerkers) waarmee persoonsgegevens worden uitgewisseld en de gegevensuitwisselingsovereenkomsten die daartoe zijn gesloten (data transfer agreements).

Er is een register met een overzicht van alle partijen aan wie persoonsgegevens worden doorgegeven.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Noordwijk passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).

Zowel de website als de systemen zijn beveiligd volgens de actuele normen. (Ipv6, laatste antivirussoftware etc.). De procedure waarlangs datalekken moeten worden afgehandeld, wordt toegepast. Datalekmeldingen verlopen via een applicatie. De datalekken worden geregistreerd in het interne datalekregister en indien nodig gemeld bij de Autoriteit persoonsgegevens. Er hebben zich in 2023 acht datalekken voorgedaan, als gevolg van een onbedoelde of ongeoorloofde verstrekking. Er heeft één beveiligingsincident plaatsgevonden bij verwerker Visma Raet zonder dat daarbij persoonsgegevens van gemeente Noordwijk zijn ingezien, noch ontvreemd.

Een datalek bij Nebu (een softwareontwikkelingsbedrijf) zou een vergrootte kans op phishing e-mails kunnen inhouden. Daarom is de bewustwording ten aanzien van phishing e-mails in 2023 opnieuw onder de aandacht gebracht binnen de gemeente.

De gedragscode over het anonimiseren en publiceren van stukken is geactualiseerd maar nog niet vastgesteld.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat het college van B&W aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante wet- en regelgeving.

In november en december 2021 zijn de privacyverklaring en privacybeleid getoetst en geactualiseerd. Het verwerkingsregister is beoordeeld en geactualiseerd. Tevens is het strategisch gemeentelijk informatiebeveiligingsbeleid 2020 – 2023 vastgesteld.

Voor de gemeente Noordwijk is een Audit Trail ingericht. Een Audit Trail is een systeem dat automatisch stapsgewijs alle uitgevoerde activiteiten voor een onderzoek gedetailleerd vastlegt en opslaat. Met een Audit Trail kunnen getrokken conclusies tot in de bron worden herleid.

De gemeente Noordwijk heeft richtlijnen opgesteld voor de borging van privacy by design. Privacy by design houdt in dat al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) rekening wordt gehouden met privacyaspecten. Bijvoorbeeld door gedurende het proces extra (technische) maatregelen te nemen en in te bouwen om de persoonsgegevens te beschermen.

De gemeente heeft de rol van 'bijhoudingsgemeente' ten aanzien van SuWinet. Dit houdt in dat als andere instanties, bijvoorbeeld een andere gemeente, de SVB, de IND of een deurwaarder vaststellen dat een adres in het BRP mogelijk niet meer klopt, bijvoorbeeld omdat iemand niet reageert op brieven, dat kunnen melden bij de gemeente Noordwijk. De gemeente Noordwijk dient dan te controleren of de adresgegevens in BRP nog correct zijn. Ook intern bij de gemeente Noordwijk kan blijken dat de adresgegevens niet meer kloppen.

Tot de functie van de Medewerker Adreskwaliteit behoort het om deze controle uit te voeren en om een brief te sturen naar de betrokken persoon als de adresgegevens niet meer juist zijn. Deze persoon wordt dan gewezen op de plicht een adreswijziging door te geven en de gevolgen als dat niet gebeurt. Daarvoor is het noodzakelijk dat de betreffende Medewerker persoonsgegevens kan raadplegen van personen waarvan een melding is ontvangen dat die niet meer op een bepaald adres bereikbaar zijn. Daarmee is het verwerken van persoonsgegevens door deze Medewerker Burgerzaken rechtmatig en er is voldaan aan het beginsel van doelbinding.

Als Functionaris voor de Gegevensbescherming heb ik (net als in 2022) in 2023 middels een interview met een Medewerker Burgerzaken vastgesteld dat de toegang tot SuWinet voor deze functie niet in strijd is met de spelregels van de Algemene verordening gegevensbescherming (AVG) en de overige privacyregels.

8. Wet politiegegevens

Binnen de Gemeente Noordwijk zijn buitengewone opsporingsambtenaren (boa's) werkzaam op domein 1, de openbare ruimte. Voor zover zij in de uitoefening van hun functie persoonsgegevens verwerken ter uitvoering van de opsporingstaak, is er sprake van de verwerking van politiegegevens in de zin van de Wet politiegegevens (Wpg). In 2022 is er een overzicht opgesteld van alle maatregelen die in het kader van de Wpg zijn en moeten worden uitgevoerd. Naar aanleiding hiervan is een concept verbeterplan gemaakt conform het werkdocument van de VNG. In 2023 is een interne audit uitgevoerd inzake de politiegegevens die door de Boa's worden uitgevoerd aan de hand van de richtlijn 3000D van NOREA door de PO en de CISO. Op basis daarvan zijn de beheersmaatregelen die de gemeente Noordwijk hanteert, beschreven. Tevens heeft er Q4 2023 een Wpg hercontrole plaatsgevonden van de externe audit 2019-2021. In 2022 heeft de vereiste externe audit ter naleving van de Wpg plaatsgevonden, en de resultaten zijn overgedragen aan de

Autoriteit Persoonsgegevens. De conclusie van de externe audit luidt dat de gemeente Noordwijk 'niet (volledig) voldoet aan het bij of krachtens de wet bepaalde'. In reactie hierop is in de afgelopen jaren een traject ingezet om verbetermaatregelen te identificeren en te implementeren.

De afhandeling van de geconstateerde tekortkomingen en de verbetermaatregelen is onderworpen aan een hercontrole door de externe auditor. De beoordeling van de opvolging van de tekortkomingen luidt dat de beheersingsmaatregelen per 23 januari 2024 voor het overgrote deel in afdoende mate zijn opgezet en bestaan. Daarmee heeft er een aanzienlijke verbetering plaatsgevonden ten opzichte van de voorgaande externe audit.

De FG heeft voor de Buitengewoon Opsporingsambtenaren (Boa's) een presentatie verzorgd over de spelregels van de Wet politiegegevens (Wpg).

9. Conclusie

In 2023 heeft de gemeente Noordwijk de AVG verder geïmplementeerd in de organisatie door de systemen en de processen te blijven actualiseren. De doorgevoerde scheiding tussen de rollen van FG, PO en CISO en een geactualiseerd privacybeleid hebben het volwassenheidsniveau ten aanzien van privacy vergroot. De procedure waarlangs een DPIA moet worden uitgevoerd, wordt gehanteerd, evenals de procedure waarlangs datalekken moeten worden afgehandeld.

Deel 2. Vooruitkijken naar 2024

Gegevensbescherming structureel onderdeel laten zijn van de processen en systemen van het college, en daarmee aantoonbaar voldoen aan privacywetgeving, is een continu proces. Het vraagt om structurele borging van dit onderwerp. Waar het jaar 2023 in het teken stond van de het professionaliseren van het beleid en de procedures, zal daar in 2024 mee worden voortgegaan.

Tot april 2024 zal maandelijks overleg plaatsvinden tussen FG, CISO en PO. Vanaf 1 april zal de huidige CISO worden aangesteld als FG. De FG is dan afkomstig uit de interne organisatie. De huidige externe FG zal als juridisch adviseur worden ingezet ter ondersteuning van de FG en de PO. De gemeente Noordwijk zal de CISOfunctie as-a-service inrichten. Intern komt er een Information Security Officer.

In 2024 zal een DPIA worden uitgevoerd op de inzet van bodycams als uit de pre-DPIA naar voren komt dat daar een verhoogd risico bij aanwezig is ten aanzien van de rechten en vrijheden van natuurlijke personen.

Voor wat betreft de informatieveiligheid is de gemeente Noordwijk voornemens om ISO-27001 certificering te behalen. Dit zal een meerjarenproject worden.