Werkprogramma Privacy 2024-2025 gemeente Nieuwkoop

Rode draad uit het jaarverslag 2023 van de FG

"De gemeente Nieuwkoop is goed op weg naar een basis privacy volwassenheidsniveau."

1. Inleiding

De bescherming van persoonsgegevens binnen de gemeentelijke organisatie is een continu proces. Dit document bevat een overzicht van actiepunten die voortvloeien uit het FG-jaarverslag 2023 van de gemeente Nieuwkoop, uit de al verrichte werkzaamheden en in zijn algemeenheid uit de eisen van de Algemene Verordening Gegevensbescherming (AVG). De aanbevelingen van de FG uit zijn jaarverslag over 2023 zijn gebruikt als input om het 'Werkprogramma privacy 2024-2025' op te stellen.

Het werkprogramma heeft betrekking op een afgekaderde[1] periode waarin we aan de slag gaan met de actiepunten.

Voorgaande jaren:

- In 2018 lag het accent op 'opzet/inrichting'.
- In 2019 en 2020 lag de nadruk meer op 'opzet, bestaan en werking' van het privacy beleidskader en het privacy beleid. Al moest worden vastgesteld dat in 2020 door corona/covid-19 en het (verplicht) thuiswerken, de verdere implementatie en uitvoering van de AVG toch wat minder aandacht heeft gekregen.
- In 2021 is, ondanks het verplichte thuiswerken, de verdere implementatie en uitvoering van de AVG, voortvarender ter hand genomen.
- In 2022 hebben we de ingeslagen weg voortgezet, echter zijn enigszins beperkt door het vertrek van onze Privacy Officer, waardoor we enige tijd zonder hebben gezeten.
- In 2023 hebben we ons vooral gericht op de aanbevelingen van de FG in zijn jaarverslag 2022.

Bij het opstellen van dit werkprogramma is nagedacht over een logische volgorde van uitvoering. Onze FG heeft medio december 2020 een ***Baseline bescherming persoonsgegevens*** opgesteld. Dit normenkader betreft een toetsingskader van de FG op naleving van de AVG. In deze Baseline Bescherming Persoonsgegevens zijn de eisen van de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) vertaald naar concrete, hanteerbare normen die duidelijk maken wat o.a. Nieuwkoop moet doen om in overeenstemming met de wet de bescherming van persoonsgegevens van de betrokkenen te waarborgen. Door het toepassen van de Baseline kunnen we ook aantonen dat passende waarborgen voor de bescherming van persoonsgegevens worden getroffen. Als laatste doel heeft de Baseline het bewerkstelligen van meer uniformiteit in beleid en uitvoering.

2.1 Korte evaluatie van de aanbevelingen uit Jaarverslag FG 2022 en werkprogramma 2023

a. Stel de visie op gegevensbescherming en de doelen vast. Neem deze doelen op in gegevensbeschermingsbeleid voor de periode 2023-2027. (parameters 1, 2 en 3).

[1] Doordat het jaarverslag pas in maart 2024 is aangeboden en kan worden vastgesteld door het college heeft het werkprogramma een looptijd van april 2024 tot en met maart 2025.

De Missie, Visie en Doelen zijn door op 17 januari 2023 door het college vastgesteld. De uitwerking van de visie op gegevensbescherming is inmiddels vertaald in gegevensbeschermingsbeleid 2023-2027. Dit beleid wordt gelijktijdig met dit werkprogramma 2024-2025 ter vaststelling voorgelegd aan het college.

b. Zorg dat de nieuwe privacy governance ook betekenis krijgt (parameter 4).

De nieuwe Governance structuur is ook op 17 januari 2023 vastgesteld door het college. Door de implementatie van het ISMS-systeem moeten de rollen en verantwoordelijkheden nog duidelijker worden.

Vanuit dit systeem zullen de procesverantwoordelijken periodiek gevraagd worden om bepaalde taken uit te voeren. Zo zullen onder meer de verwerkingen gecontroleerd moeten worden, en wordt toegezien op of de maatregelen die voortvloeien uit een DPIA zijn nageleefd.

c. Maak van het Information Securtity Management System een dynamisch instrument voor de bescherming van persoonsgegevens. Richt het daarom zorgvuldig in (parameter 8).

In 2023 hebben de Privacy Officer en de CISO alle afdelingen en teams bezocht om hen te ondersteunen bij het invullen van het ISMS-systeem. Gestart is met het registreren/opnemen van alle verwerkingen (het zgn. verwerkingenregister). Ook heeft een presentatie voor het Managementteam plaatsgevonden.

d. Schroef het tempo van uitvoeren van DPIA's op. Zorg ervoor dat managers gaan inzien dat zij daarin een belang hebben (parameter 6).

Er is ook in 2023 gewerkt aan diverse DPIA's en zijn een aantal nieuwe gestart. De noodzaak wordt ook al meer onderkend in de organisatie. Het verbeteren van het eigenaarschap van de managers is een blijvend aandachtpunt. Het implementeren van het ISMS systeem (zie ook onder c.) moet hier een grote bijdrage in leveren. Dus ook het herkennen of een DPIA moet worden uitgevoerd.

e. Zet een cyclus van trainingen en bijeenkomsten op om het privacy-bewustzijn te bevorderen (parameters 4 en 17).

Hier is in 2023 actief invulling aan gegeven. Bij alle teams heeft de PO een presentatie verzorgd. Dit betrof een algemene (basis) privacy bewustwordingssessie. Een stukje historie werd verteld, enkele veel voorkomende begrippen uit de AVG werden toegelicht, met daarbij als afsluiting een datalekken quiz.

2.2 Overige werkzaamheden

Naast de 5 aanbevelingen in het jaarverslag 2022 is er natuurlijk meer gebeurd. Een paar voorbeelden: we hebben de medewerkers van de organisatie, in overleg met het team Communicatie, periodiek geïnformeerd via SharePoint over privacy -en informatiebeveiliging gerelateerde onderwerpen. Daarnaast zijn er voor de medewerkers van de organisatie verplichte e-learnings uitgezet. De e-learnings hadden betrekking op: de AVG, Phishing en Informatiebeveiliging. Eind van het jaar is er nog een datalekkencampagne geweest, waarbij de medewerkers bewust werden gemaakt over dit onderwerp. Echter veel tijd is gaan zitten in de reguliere werkzaamheden.

3. Aanbevelingen uit het jaarverslag 2023

De aanbevelingen zijn overgenomen uit het jaarverslag 2023 van de FG. Deze aanbevelingen corresponderen met de focuspunten van de FG voor 2024.

In de Baseline bescherming persoonsgegevens 2020 van de FG zijn zeventien parameters beschreven waarlangs elke gemeente de bescherming van persoonsgegevens kan vormgeven overeenkomstig

de eisen van de AVG. Hieronder staat per aanbeveling vermeldt om welke parameter(s) het gaat. En waar de FG in 2024 zijn focus op zal leggen in zijn jaarverslag over 2024.

1. *Stel het gegevensbeschermingsbeleid voor de komende periode vast en maak elk jaar op basis van dit beleid een jaarplan. Neem hierin uiteraard ook de aanbevelingen en adviezen van de FG mee. (parameters 1, 2 en 3).*

Wat gaan we doen?

Het gegevensbeschermingsbeleid 2023-2027, zoals eerder beschreven, wordt gelijktijdig met dit werkprogramma 2023-2024 aan het college ter vaststelling aangeboden. Dit werkprogramma zien wij tevens als het jaarplan, waarin de voor 2024 beschreven doelen worden opgenomen en uitgevoerd. Het gegevensbeschermingsbeleid zorgt ervoor dat de gemaakte doelen in de tijd worden weggezet, en aan de hand van het jaarplan worden uitgewerkt. Zodoende is voorspelbaar welke inspanningen er verwacht kunnen worden op het gebied van privacy.

2. *Zorg dat de privacy governance bij alle medewerkers betekenis krijgt (parameter 4).*

Wat gaan we doen?

Zorgen dat de taken en verantwoordelijkheden betekenis krijgen binnen de gemeente en niet alleen woorden op papier zijn. Het in 2024 verder te implementeren ISMS systeem kan hier een (grote) rol in spelen.

Dit werkt onder meer door periodiek controlemomenten in te bouwen voor onder andere de verwerkingen van persoonsgegevens en het nagaan van de uitgevoerde maatregelen rondom DPIA's. Door deze te controleren en actueel te houden, blijven de procesverantwoordelijken betrokken. Door de herhaling zal het belang van hun rol en verantwoordelijkheid ingezien worden.

3. *Rond het invullen van het register van verwerkingsactiviteiten in het ISMS af in 2024 (parameter 6).*

Wat gaan we doen?

Dit is prioriteit in 2024 en zal gerealiseerd worden. Procesverantwoordelijken zullen actief betrokken worden bij het invullen van dit register.

4. *Ga door met dit tempo van uitvoeren van DPIA's. Zorg ervoor dat managers gaan inzien dat zij daarin een belang hebben (parameter 8).*

Wat gaan we doen?

Er zal een overzicht worden gemaakt van uit te voeren DPIA's met een hoog risico. Het eigenaarschap wordt verhoogd bij procesverantwoordelijken zodat het vanzelfsprekend wordt dat bij nieuwe verwerkingen onderzocht wordt of een DPIA nodig is. Het ISMS systeem zal daarbij (ook) een (grote) rol spelen.

5. *Blijf het privacy-bewustzijn te bevorderen. Maak presentaties gericht op specifieke groepen. (parameters 4 en 17).*

Wat gaan we doen?

We gaan door op de in 2023 ingeslagen weg en zullen waar nodig, specifieke presentaties verzorgen. Qua kennis en bewustwording zal een privacy training worden ontwikkeld voor de nieuwe medewerkers, die 2 keer per jaar zal worden aangeboden. Dit wordt gecombineerd met informatiebeveiliging zodat een compleet beeld kan worden gegeven. Met betrekking tot de verschillende afdelingen zal opgehaald worden waar zij behoefte aan hebben dan wel zal een verdieping worden aangeboden op een aantal specifieke privacy thema's.

4. Overige aanbevelingen

In het jaarverslag 2023 zijn nog meer adviezen gegeven, die niet zijn vertaald in de aanbevelingen voor 2024, dus waarop niet specifiek door de FG in 2024 wordt getoetst. Zie de paragrafen 4.1 tot en met 4.13. Voor zover de tijd dit toelaat, nemen we deze mee. Soms ontkomen we daar niet aan. Denk bijvoorbeeld aan het opstellen van beleid voor ChatGPT. Dit is onderstaande planning opgenomen.

5. Planning (op basis van de aanbevelingen en andere opmerkingen FG in jaarverslag)

Actie	Onderwerpen	Q1 2024	Q2	Q3	Q4	Q1 2025
Ad 1	Vaststellen gegevensbeschermingsbeleid 2023-2027 en het opstellen en vaststellen van een jaarplan om de gestelde doelen te realiseren	X				
Ad 2	Zorgen dat de privacy governance bij alle medewerkers betekenis krijgt		X	X	X	X
Ad 3	Verwerkingenregister in ISMS systeem, inclusief het opnemen van bezwaartermijnen		X	X	X	X
	Actualiseren verwerkingen register verwerkingen (door procesverantwoordelijke)			X	X	
	Bezien of register van Datalekken kan worden opgenomen			X		
	Leg apart register aan met verwerkersovereenkomsten			X		
Ad 4	Uitvoeren DPIA's	X	X	X	X	X
	In ieder geval: • Analyse/verbeterplan Zaakgericht werken (Djuma) • Adreskwaliteit (loopt nog) • Welzijnsbezoeken • City Control (inclusief module vaartoezicht) • Bodycams door BOA's • Welzijn op recept • (toegang tot) Jeugdhulp • Jeugdhulp (SOZ) • Vroegsignalering • Ondermijning (plan van aanpak/uitwerking)					
	Nazien verbeterplannen en beheersmaatregelen op uitgevoerde DPIA's door PO voor procesverantwoordelijke	X	X	X	X	X
	Extra DPIA's bezien/uitvoeren (op hoog risico)	X	X	X	X	X
	Privacy by design bij nieuwe verwerkingen	X	X	X	X	X
Ad 5	Periodiek communiceren op SharePoint, conform Communicatiekalender IB & Privacy 2024	X	X	X	X	X
	E-learning voor de hele organisatie (team I&A)					

	Bewustwording bijeenkomsten/trainingen (uitvoeren)		X	X	X	X
	Acties buiten de aanbevelingen op basis van het jaarverslag 2023					
	Stel beleid op voor AI (ChatGPT)		X			
	Breid de functie van Privacy Officer uit naar 1 fte (onder 4.3)					
	Stel verbeterplan op n.a.v. de uitkomsten DPIA ondermijning (onder 4.4)	X	X			
	Doelbinding: Ontwikkel een visie op datagedreven werken vóórdat databronnen gecombineerd gaan worden en persoonsgegevens gekoppeld (onder 4.5)					
	Bezien welke verwerkersovereenkomsten nog moeten worden gesloten (onder 4.9)	X	X	X	X	X
	Stel verbeterplan WPG audit op en wijs een WPG-FG aan (onder 4.10)[2]		X			
	Testen uitoefenen rechten van betrokkenen (onder 4.11)		X			
	Neem het register van datalekken op in het ISMS (onder 4.12)				X	X

[2] Onze FG wordt ook WPG-FG voor 1 uur per week. De DVO is al gesloten. Besluitvorming in het college medio maart 2024.