Werkprogramma Privacy 2023 gemeente Nieuwkoop

Rode draad uit het jaarverslag 2022 van de FG

"De gemeente Nieuwkoop heeft in 2022 weer stappen gezet richting een basis privacy volwassenheidsniveau. Maar er valt nog genoeg te doen en te verbeteren"

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 2022 van 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 2022 zijn gebruikt als input om het 'Werkprogramma privacy 2023' op te stellen. Het PIT is hierin leidend geweest. Onze FG heeft meegelezen.

Het werkprogramma heeft betrekking op een afgekaderde periode waarin we aan de slag gaan met de actiepunten. 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. Per 1 november 2022 is de functie weer ingevuld. In 2023 gaan we nog actiever aan de slag met de aanbevelingen van de FG. Binnen het team BJZ is het aantal uren voor de Privacy Officer verhoogt van 16 uur naar 24 uur per week, zonder dat daar formatie uitbreiding aan ten grondslag ligt. De werkzaamheden zijn anders ingericht.

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 2021 en werkprogramma 2022

a. Ontwikkel een visie op gegevensbescherming voor de komende 5 jaar en stel doelen vast waarvan het bereiken de visie gaat verwezenlijken. Neem deze doelen op in het gegevensbeschermingsbeleid (parameters 1, 2 en 3).

Er is een Missie, Visie en Doelen document opgesteld. Deze is op 17 januari 2023 door het college vastgesteld. Verdere uitwerking vindt plaats in 2023. Zie ook de aanbeveling hierover in het jaarverslag 2022.

b. Zet een nieuwe governance-structuur op en laat deze ook betekenis krijgen (parameter 4).

Er is in 2022 een nieuwe Governance structuur opgesteld. Deze is ook op 17 januari 2023 vastgesteld door het college. Verdere uitwerking vindt plaats in 2023. Zie ook de aanbeveling hierover in het jaarverslag 2022.

c. Ga verder met het zelf uitvoeren van DPIA's. Zorg voor meer eigenaarschap bij managers zodat zij ook een belang hebben om hun medewerkers daarvoor vrij te maken (parameter 6).

Er is ook in 2022 gewerkt aan diverse DPIA's, maar niet zoals vooraf was voorzien en beoogd. Mede door het vertrek van de Privacy Officer (PO) medio juli. Per 1 november is de nieuwe Privacy Officer begonnen. Wel zijn er een aantal DPIA's in gang gezet die hun beslag zullen krijgen in 2023. Djuma verdient nog altijd aandacht, de DPIA ondermijning is opgeleverd en wacht op een reactie/advies van de FG en de verplichte WPG-audit is opgeleverd. Aan het verbeteren van het eigenaarschap van de managers wordt gewerkt. Enerzijds door de recent vastgestelde governance structuur en anderzijds door het (nu) in 2023 te implementeren ISMS systeem (zie ook onder d.). Er is nog geen complete probleemanalyse van (en oplossingen voor) de ongeoorloofde toegang tot Djuma om datalekken te voorkomen. Echter de ongeoorloofde toegang is wel al verbeterd. Dit zet zich voort in 2023.

d. Zorg voor een goed plan van aanpak om het nieuwe Information Security Management System (ISMS) te implementeren en om draagvlak te krijgen bij de toekomstige gebruikers (parameter 8).

In 2022 is hard gewerkt aan het vullen van het ISMS systeem te vullen. Eind augustus zou dit systeem worden gepresenteerd aan het MT met een schema van implementatie in de organisatie vanaf 1 januari 2023 tot en met 1 juli 2023. Echter door het vertrek van de PO en ziekte van de CISO is de implementatie vertraagd. De start van de implementatie staat nu gepland vanaf Q3 2023.

e. Bouw de activiteiten op het gebied van privacy-bewustzijn verder uit en laat deze cyclisch terugkomen. Focus op het betekenis krijgen van privacy! (parameters 4 en 17).

Hier is in 2022 te weinig aandacht voor geweest en deze aanbeveling is niet (goed) opgevolgd. Dit wordt een prioriteit in 2023!

2.2 Overige werkzaamheden

Naast de 5 aanbevelingen in het jaarverslag is er natuurlijk meer gebeurd. Een paar voorbeelden: DPIA ondermijning is uitgevoerd, interne procedure melding datalekken is aangepast (via TopDesk), de FG heeft een presentatie aan MT/teamleiders gegeven over rollen en verantwoordelijkheden.

3. Aanbevelingen uit het jaarverslag 2022

De aanbevelingen zijn overgenomen uit het jaarverslag 2022 van de FG. Deze aanbevelingen corresponderen met de focuspunten van de FG voor 2023.

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 2023 zijn focus op zal leggen in zijn jaarverslag over 2023.

1. Stel de visie op gegevensbescherming en de doelen vast. Neem deze doelen op in gegevensbeschermingsbeleid voor de periode 2023-2028 (parameters 1, 2 en 3).

<u>Wat gaan we doen?</u>

De visie is, zoals eerder beschreven, al vastgesteld. De doelen zullen in de tijd worden gezet en omgezet in een gegevensbeschermingsbeleid, waarna dit beleid wordt uitgevoerd. Hierbij zullen bij

voorkeur zo veel mogelijk stakeholders worden betrokken. Het huidige privacybeleid uit 2018 zal worden geëvalueerd.

2. Zorg dat de nieuwe privacy governance ook 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 Q3 te implementeren ISMS systeem kan hier een (grote) rol in spelen.

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

Wat gaan we doen?

Zorgen voor een goed plan van aanpak om het nieuwe ISMS te implementeren en om draagvlak te krijgen bij de toekomstige gebruikers/procesverantwoordelijke. Zie ook onder 3.

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

Wat gaan we doen?

Er zal een overzicht worden gemaakt van uit te voeren DPIA's met een hoog risico. Er worden alsnog DPIA's uitgevoerd naar (hoog risico) verwerkingsactiviteiten in Djuma. 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 een (grote) rol spelen.

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

Wat gaan we doen?

Er wordt in 2023 meer aandacht besteed aan het vergroten van het privacy-bewustzijn binnen de organisatie. Er zal een cyclus van voorlichtingsbijeenkomsten worden opgezet om het draagvlak voor en de kennis van de AVG te vergroten. Ook wordt bekeken of e-learning kan worden ingezet om het bewustzijn van medewerkers te vergroten.

4. Overige aanbevelingen

In het jaarverslag zijn nog meer aanbevelingen genoemd, waarop niet specifiek door de FG in 2023 wordt getoetst, maar die wel aanbevelenswaardig zijn om, voor zover de tijd dit toelaat, mee te nemen. Dit is onderstaande planning opgenomen.

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

Actie	Onderwerpen	Q1	Q2	Q3	Q4
Ad 1	Opstellen gegevensbeschermingsbeleid 2023-2028 en evaluatie Privacybeleid 2018. Hierin worden de doelen van de Missie, Visie en Doelen verwerkt		X	X	
Ad 2	(nieuwe) Governance-structuur betekenis geven		X	X	X
Ad 3	Inrichting ISMS systeem	X	X		
	Uitrol ISMS/PMS, inclusief voorlichting procesverantwoordelijken			X	X

	Actualiseren verwerkingen register verwerkingen (door procesverantwoordelijke)			X	X
	Opnemen bezwaartermijnen in register van verwerkingen.		X	X	X
	Bezien of register van Datalekken kan worden opgenomen		X		
	Leg apart register aan met verwerkersovereenkomsten		X	X	
Ad 4	Uitvoeren DPIA's	X	X	X	X
	In ieder geval: • Analyse/verbeterplan Zaakgericht werken (Djuma) • Datamask • Adreskwaliteit • Welzijnsbezoeken •	 X X X X	 X X X X	X	X
	Nazien verbeterplannen en beheersmaatregelen op uitgevoerde DPIA's door PO voor procesverantwoordelijke	X	X	X	X
	Extra DPIA's bezien/uitvoeren (op hoog risico)	X	X	X	X
	Privacy by design bij nieuwe verwerkingen	X	X	X	X
Ad 5	Wekelijks/maandelijks communiceren op SharePoint, conform Communicatiekalender IB & Privacy 2022	X	X	X	X
	E-learning voor de hele organisatie		X	X	
	Opstellen awareness plan (cyclus trainingen en bijeenkomsten)		X		
	Bewustwording bijeenkomsten/trainingen (uitvoeren)		X	X	X
	Acties buiten de aanbevelingen op basis van het jaarverslag 2022				
	Breid de functie van Privacy Officer uit naar 1 fte (onder 4.3)				
	Doelbinding: Voordat persoonsgegevens uitgewisseld gaan worden in samenwerkingsverbanden moeten de doeleinden van de verwerkingen van de persoonsgegevens concreet bepaald zijn en duidelijk omschreven (onder 4.5)				
	Beveiliging: Voer de nog niet uitgevoerde acties uit het uitvoeringsplan informatiebeveiligingsbeleid 2020-2022 alsnog uit om zo passende waarborgen voor de beveiliging van persoonsgegevens te kunnen treffen. Stel in 2023 een nieuw uitvoeringsplan voor de komende periode op (onder 4.7)	Ciso	Ciso	Ciso	Ciso
	Bezien welke verwerkersovereenkomsten nog moeten worden gesloten (onder 4.9)	X	X	X	X
	Stel verbeterplan WPG audit op en wijs een WPG-FG aan (onder 4.10)[1]		X		
	Gemeentelijke website toegankelijker maken voor rechten van betrokkenen (onder 4.11)		X		

[1] Dit wordt in maart 2023 besproken met de regio-gemeenten.