Werkprogramma Privacy 2025-2026 gemeente Nieuwkoop

Rode draad uit het jaarverslag 2024 van de FG

"De gemeente Nieuwkoop nadert het 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 2024 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 2024 zijn gebruikt als input om het 'Werkprogramma privacy 2025-2026' 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.
- In 2024 hebben we ons opnieuw, vooral, gericht op de aanbevelingen van de FG in zijn jaarverslag 2023.

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.

[1] Doordat het jaarverslag pas in april 2025 is aangeboden en pas in mei 2025 kan worden vastgesteld door het college heeft het werkprogramma een looptijd van mei 2025 tot en met april 2026 2025.

2.1 Korte evaluatie van de aanbevelingen uit Jaarverslag FG 2023 en werkprogramma 2024-2025

a. 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).

De Missie, Visie en Doelen zijn op 17 januari 2023 door het college vastgesteld. De uitwerking van de visie op gegevensbescherming is vertaald in gegevensbeschermingsbeleid 2023-2027. Dit gegevensbeschermingsbeleid is op 2 april 2024 door het college vastgesteld en is het privacy beleidskader gemeente Nieuwkoop van 19 juni 2018 ingetrokken. De in een jaar op te nemen werkzaamheden/acties worden meegenomen en beschreven in het werkplan van het desbetreffende jaar.

b. Zorg dat de privacy governance bij alle medewerkers 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.

In 2024 is, in overleg met de gemeentesecretaris afgesproken, om de kwartaalmemo's van de FG te agenderen en te bespreken in het MT. In de kwartaalmemo's beschrijft de FG de stand van zaken ten aanzien van de belangrijkste onderwerpen die spelen op het gebied van gegevensbescherming in de gemeente Nieuwkoop.

Volgens de hierboven genoemde Governance structuur zijn alle medewerkers (inclusief inhuur en externen) van de gemeente verantwoordelijk voor de bescherming van alle verwerkingen van persoonsgegevens binnen de gemeente. Dat betekent dat iedereen actief een bijdrage levert aan een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

Teamleiders en medewerkers worden via hun eigen afdelingsmanager op de hoogte gesteld van de ontwikkelingen zodat de bewustzijn gecreëerd wordt en duidelijk is wat ieders rol en taak is.

c. Rond het invullen van het register van verwerkingsactiviteiten in het ISMS af in 2024 (parameter 8).

Deze doelstelling is helaas niet gehaald. Het bleek, achteraf, lastiger om alle verwerkingen op een juiste manier in het systeem te krijgen. Ook omdat dit veel meer werk met zich meebracht voor de organisatie dan vooraf was voorzien. Echter, los hiervan, hebben we in het onder a. genoemde gegevensbeschermingsbeleid 2023-2027 voor 2024 beschreven dat dit jaar in het teken zal staan van het verder invullen van en werken met het ISMS-systeem. Daaraan is dus voldaan. Deze aanbeveling van de FG is nog van voor de datum van vaststelling van het gegevensbeschermingsbeleid 2023-2027. De FG is hierin meegenomen.

d. Ga door met dit tempo van uitvoeren van DPIA's. Zorg ervoor dat managers gaan inzien dat zij daarin een belang hebben (parameter 6).

Er is ook in 2024 gewerkt aan meerdere 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, maar ook medewerkers, 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. Blijf het privacy-bewustzijn te bevorderen. Maak presentaties gericht op specifieke groepen (parameters 4 en 17).

Hier is in 2024 minder actief invulling aan gegeven. Hoofdzakelijk omdat veel teams moesten worden bezocht voor het invullen van het verwerkingenregister in het ISMS systeem. Daar is heel veel tijd in gaan zitten. Dat is echter ook een vorm van bewustwording, maar dan meer specifiek gericht op de verwerkingen per team.

2.2 Overige werkzaamheden

Naast de 5 aanbevelingen in het jaarverslag 2023 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 is er voor de medewerkers van de organisatie een verplichte e-learning uitgezet over randsomware. Dat jaar is er nog een datalekkencampagne in relatie tot het vergrendelen van laptop (en scherm) geweest, waarbij de medewerkers bewust werden gemaakt over dit onderwerp. Echter veel tijd is gaan zitten in de reguliere werkzaamheden.

2.3. Overlegstructuren (nieuw toegevoegd)

Elke twee weken is er een overleg van het Privacy Informatiebeveiligingsteam (PIT). Het geeft advies op het gebied van privacy en informatieveiligheid. De leden van het PIT bespreken het jaarlijkse werkprogramma en vragen/incidenten/ontwikkelingen op het gebied van privacy en informatieveiligheid. Waar nodig neemt het PIT een signalerende rol richting de organisatie. In het PIT hebben zitting: de privacy coördinator, de privacy officer, de CISO, de functionaris voor gegevensbescherming (FG) en een medewerkster van team communicatie.

Daarnaast bespreken de privacy coördinator, de privacy officer en de FG maandelijkse (actuele thema's en onderwerpen, maar ook de voortgang van de uitvoering van het gegevensbeschermingsbeleid en het werkprogramma Privacy.

Elk kwartaal spreken de FG, de CISO, de privacy coördinator en de privacy officer (PO) met de gemeentesecretaris, waarbij de memo's van de FG alswel van de CISO worden besproken. Deze memo's worden daarna geagendeerd voor en besproken in de volgende MT-vergadering.

De PO en de CISO hebben periodiek overleg met de portefeuillehouder. Voor 2025 is een nieuwe structuur opgezet.

3. Aanbevelingen uit het jaarverslag 2024

De aanbevelingen zijn overgenomen uit het jaarverslag 2024 van de FG. Deze aanbevelingen corresponderen met de focuspunten van de FG voor 2025.

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 2025 zijn focus op zal leggen in zijn jaarverslag over 2025.

1. Zorg dat de privacy governance bij alle medewerkers betekenis krijgt (parameters 4).

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

Taken en verantwoordelijkheden moeten betekenis krijgen binnen de gemeente en niet alleen woorden op papier zijn. Het in 2025 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 en ook medewerkers betrokken. Door de herhaling zal het belang van hun rol en verantwoordelijkheid ingezien worden.

2. Rond het invullen van het register van verwerkingsactiviteiten in het ISMS af (parameter 8).

Wat gaan we doen?

Hierin is al voorzien in het vastgestelde gegevensbeschermingsbeleid 2023-2027 waarin staat: in jaar 3 (lees: 2025) worden de laatste zaken op orde maken binnen het ISMS-systeem en worden de procesverantwoordelijken hier meer en meer vertrouwd mee gemaakt. In gesprek met de procesverantwoordelijke zal zijn of haar rol, zoals aangegeven in Governance structuur, besproken worden en waar nodig handvatten gegeven worden om die rol te verbeteren.

3. Ga door met dit tempo van uitvoeren van DPIA's (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.

4. Registreer de datalekken in het ISMS (parameter 16).

Wat gaan we doen?

Dit wordt verzorgd. De meldingen worden gedaan in Top Desk. Waarna datalekken in een Excel bestand worden geregistreerd. Dat wordt overgebracht naar het ISMS systeem.

5. Maak meer werk van privacy-bewustzijn. Maak presentaties gericht op specifieke groepen (parameters 4 en 17).

Wat gaan we doen?

We gaan door op de ingeslagen weg en zullen waar nodig, specifieke presentaties verzorgen. Qua kennis en bewustwording is een privacy training ontwikkeld voor de nieuwe medewerkers, die 4 keer per jaar zal worden aangeboden. Dit wordt gecombineerd met informatiebeveiliging zodat een compleet beeld kan worden gegeven. De eerste bijeenkomst heeft inmiddels op 7 april plaats gevonden.

Met betrekking tot de bewustwording zal naast de standaard periodieke invulling hiervan, (een e-learning, bewustwordingssessies, informatie op SharePoint) ook een ludieke grote actie (gemeente breed) worden gepland. Tevens zal invulling worden gegeven aan het langsgaan van de verschillende teams om zo de actuele vragen die bij hen spelen over privacy en informatieveiligheid te bespreken.

4. Overige aanbevelingen

In het jaarverslag 2024 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, soms zijn ze voor een ander team of functionaris (lees: CISO).

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

Actie	Onderwerpen	Q1 2025	Q2	Q3	Q4	Q1 2026
Algemeen	Uitvoeren gegevensbeschermingsbeleid 2023-2027	X	X	X	X	X

Ad 1	Zorg dat de privacy governance bij alle medewerkers betekenis krijgt		X	X	X	X
Ad 2	Rond het invullen van het register van verwerkingsactiviteiten in het ISMS af		X	X	X	X
	Inclusief opnemen bezwaartermijnen		X	X	X	X
	Leg apart register aan met verwerkersovereenkomsten				X	
Ad 3	Ga door met dit tempo van uitvoeren van DPIA's	X	X	X	X	X
	De voortgang van DPIA's bespreken we elke 2 weken in het Privacy Informatiebeveiliging Team (PIT)	X	X	X	X	X
	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 4	Registreer de datalekken in het ISMS				X	
Ad 5	Maak meer werk van privacy-bewustzijn. Maak presentaties gericht op specifieke groepen	X	X	X	X	X
	Periodiek communiceren op SharePoint, conform Communicatiekalender IB & Privacy 2024	X	X	X	X	X
	E-learning voor de hele organisatie					
	Bewustwording bijeenkomsten/trainingen (uitvoeren)		X	X	X	X
Onder:	**Acties buiten de aanbevelingen op basis van het jaarverslag 2024**					
4.1	Stel beleid op voor AI (team I&A)					
4.4	Hervorm het werkproces Ondermijning zodanig dat de bescherming van de te verwerken persoonsgegevens geborgd is					
4.5	Ontwikkel een visie op datagedreven werken vóórdat databronnen gecombineerd gaan worden en persoonsgegevens gekoppeld					
4.5	Herontwerp in 2025 het proces Ondermijning op basis van het beschikbaar wettelijk instrumentarium					
4.7	Neem de nog niet gestarte projecten op in het nieuwe Informatieveiligheidsbeleid en voer deze projecten ook daadwerkelijk uit					
4.7	Ga cyberincidenten oefenen					
4.9	Integreer de monitoring van de verwerkersovereenkomsten in het					

	contractmanagement zodat deze actueel zijn en tijdig aangepast kunnen worden					
4.10	Zorg dat het externe auditrapport Wpg zo snel mogelijk ontvangen wordt. Pas het verbeterplan aan op basis van de bevindingen en voer dit uit vóórdat de tweede externe audit weer op de rol staat					
4.11	Test de rechten van betrokkenen met enige regelmaat om te onderzoeken of de procedure efficiënt en effectief verloopt					