

Gegevensbeschermingsbeleid 2023-2027

Gegevensbeschermingsbeleid

Dit document beschrijft het gegevensbeschermingsbeleid van de gemeente Nieuwkoop voor de komende 5 jaar (2023-2027).

Begin 2023 heeft het college van burgemeester en wethouders met betrekking tot de bescherming van persoonsgegevens voor de komende 5 jaar een Missie, Visie en Doelen vastgesteld voor de gemeente Nieuwkoop. Dit geeft de gemeente een richting en ambitie op het gebied van bescherming van persoonsgegevens, en worden er doelen gesteld om die visie en missie te realiseren.

De wijze waarop door het college wordt voldaan aan de van toepassing zijnde wet- en regelgeving op het gebied van privacy wordt opgenomen in het Gegevensbeschermingsbeleid. De doelen die het college zichzelf heeft gesteld, vormen onder meer de input van dit beleid.

Het college heeft zichzelf 4 doelen voor de komende periode (2023-2027) gesteld. Deze zijn:

- I. - Sturen op privacy
- II. - Kennis en bewustzijn van privacy
- III. - Actuele en complete privacy registraties
- IV. - Borging privacy risicomanagement

In dit beleidsdocument zal worden aangegeven hoe het college zal acteren op het verwezenlijken van deze doelen in de komende periode.

2023 – jaar 1

Om de sturing op privacy vorm te geven zal in jaar 1 de periodieke afspraken met de portefeuillehouder en de gemeentesecretaris in de agenda's een plek krijgen en vinden de gesprekken plaats. Eveneens zal de Governancecode worden vastgesteld¹ waarbij de verantwoordelijkheden binnen de organisatie op het gebied van privacy duidelijk zijn voor de procesverantwoordelijken.

Op het gebied van bewustwording zullen de medewerkers uit de organisatie allemaal in teamverband een basis bewustwordingstraining Privacy krijgen, waarbij iedereen weer dezelfde gelijke basis aan informatie heeft. Daarnaast zullen er nog online AVG-trainingen worden aangeboden. Tevens zal een datalekken campagne worden gelanceerd om ook op die wijze de bewustwording te vergroten. Met betrekking tot het hebben van actuele en complete privacy registraties weten de medewerkers bij datalekken een melding te maken in TOPdesk. Via de bewustwordingstrainingen worden ze daarop gewezen, en de applicatie is voor eenieder makkelijk te vinden. Verder zal dit jaar gestart worden met de voorbereiding en invulling van het ISMS-systeem. Daartoe zullen de bestaande verwerkingen geregistreerd worden in het systeem. De procesverantwoordelijken zullen kennis nemen van het ISMS-systeem alsook hun verantwoordelijkheid hierin. Verwerkingen dienen gecontroleerd te worden zodat in jaar 2 uitgegaan kan worden van een actueel, up-to-date verwerkingenregister.

Ten aanzien van de borging privacy risicomanagement zullen in dit jaar bij nieuw aan te schaffen applicaties via RFC de controle en advies plaatsvinden op het gebied van privacy en informatieveiligheid. En daarnaast zal ook bij iedere nieuwe verwerking/ applicatie maar ook bij bestaande verwerkingen gekeken worden of het al dan niet nodig is om een DPIA uit te voeren. Een pre-DPIA scan zal hieraan voorafgaan.

Dit Gegevensbeschermingsbeleid 2023-2027 wordt vanwege enige vertraging begin 2024 vastgesteld. Zodoende kan al worden aangegeven dat voor 2023 het beleid is nageleefd en de daarbij behorende doelen zijn behaald.

2024 - jaar 2

Dit jaar zal in het teken staan van het verder invullen van en werken met het ISMS-systeem. Het meer compleet krijgen van het systeem. Van de procesverantwoordelijken wordt verwacht dat zij hun rol kennen en nemen zoals is vormgegeven in de Governancecode. Ten aanzien van het ISMS-systeem

1) Op 17 januari 2023 is deze Governancecode door uw college vastgesteld.

zullen zij ook periodiek worden gevraagd om de verwerkingen te controleren en te actualiseren. Een overzicht/ kalender zal hiertoe gemaakt worden om dergelijke periodieke afspraken in de agenda's van de procesverantwoordelijken te krijgen.

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.

Vanwege het compleet maken van het ISMS- systeem zullen de privacy risico's meer duidelijk worden. Er kan beoordeeld worden of er een DPIA benodigd is ten aanzien van die bestaande hoog risicoverwerkingen. Een prioritering wordt gegeven aan de volgorde van de uitvoering van de DPIA. Tevens zal hierop aansluitend in het ISMS-systeem een proces voor het maken van DPIA's door de procesverantwoordelijken worden vormgegeven. Ook zal het ISMS-systeem meer duidelijk maken aan welke partijen verwerkingen zijn uitbesteed (verwerkingsovereenkomsten) en hoe lang de gegevens bewaard dienen te worden.

De informatievoorziening richting de burger (onder meer de website) zal worden herzien en waar nodig aangepast worden op actualiteiten, juistheid en ontbrekende onderdelen. Voor de betrokkene is duidelijk wat zijn rechten zijn en welke persoonsgegevens over hem worden geregistreerd.

2025 – jaar 3

In jaar 3 volgt de laatste zaken op orde maken binnen het ISMS-systeem en dat de procesverantwoordelijken hier meer en meer vertrouwd mee worden. In gesprek met de procesverantwoordelijke zal zijn of haar rol, zoals aangegeven in Governancecode, besproken worden en waar nodig handvatten gegeven worden om die rol te verbeteren.

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. Daartoe zal voorafgaande aan dit jaar een budget worden gevraagd en gereserveerd. Tevens zal invulling worden gegeven aan het inloopspreekuur zodat de organisatie op periodieke momenten vragen kan stellen over privacy en informatieveiligheid.

De gemeente Nieuwkoop werkt veel samen met andere gemeenten. Voorbeelden hiervan zijn samenwerkingsverbanden en gemeenschappelijke regelingen. In het kader van het hebben van een complete registratie zal dit jaar meer inzichtelijk worden gemaakt wat ieders rol en verantwoordelijkheid is als het gaat om verwerkingen van persoonsgegevens binnen deze samenwerkingsverbanden. Deze inzichten worden verwerkt in het ISMS-systeem.

Ook het oppakken van hoog risicoverwerkingen en het daarop te realiseren DPIA's raken steeds meer vertrouwd in de organisatie. De procesverantwoordelijke of de verantwoordelijke medewerker weet wie de stakeholders zijn die zij hierbij moeten betrekken en ook wat er van hen verwacht wordt. Het aantal op te pakken en te realiseren DPIA's zal hierdoor toenemen. De lijst met nieuwe applicaties zullen gecontroleerd worden op privacy en informatieveiligheid, en dit zal organisatorisch jaarlijks worden ingebed.

2026 - jaar 4

In jaar 4 zal meer aandacht worden gevraagd voor het meer integreren van privacy binnen de organisatie. Binnen teams zal hier aandacht voor gevraagd worden en met elkaar besproken worden hoe binnen de werkprocessen de privacy wordt gewaarborgd. Dit verhoogt het samenhangende bewustzijn met betrekking tot privacy.

Ten aanzien van de bewustwording zal verder dit jaar gekeken worden of dit dekkend is, of dat sommige organisatieonderdelen extra aandacht behoeven op dit gebied. Een passend aanbod volgt dan.

De registraties van het ISMS-systeem zijn op orde en de wijzigingen worden periodiek door de procesverantwoordelijke doorgevoerd. Invulling wordt gegeven aan het periodiek opleiden van het Servicepunt ICT om datalekken en andere beveiligingsincidenten te herkennen en de melding als zodanig classificeren. Omdat in de voorgaande jaren met name wordt ingezet op het verhogen van de frequentie van het opstellen van DPIA's op hoog risicoverwerkingen zal er in dit jaar specifiek aandacht zijn voor de genomen maatregelen in de DPIA's en de mate van opvolging hiervan. Dit is een onderdeel van de cyclus van plan-do-check-act. Welke maatregelen zijn er genomen, en zijn deze juist opgepakt. Periodieke invulling en controle hierop zal worden vormgegeven.

2027 – jaar 5

In jaar 5 werkt de gemeente enige tijd met het ISMS-systeem en de procesverantwoordelijken weten hun rol. Die rol wordt ook dusdanig genoten dat de medewerkers behorende tot de afdeling van de procesverantwoordelijke actief en bewust zijn van hun signaleringstaak en hun sturingstaak.

Het bewustzijn en de bewustwording van de organisatie op het gebied van privacy en informatieveiligheid is periodiek geregeld en voor de organisatie duidelijk wanneer dit plaatsvindt. De diverse programma's zullen geëvalueerd worden en waar nodig aangepast.

Het ISMS-systeem is een modulair systeem. Bij aanvang in jaar 1 is voor een bepaald aantal modules gekozen. Dit jaar zal met de procesverantwoordelijken bezien worden of er behoefte is aan aanvullende

modules (o.a. een dashboard) die bijdragen aan het vergroten van inzicht en overzicht over privacy en informatieveiligheid in het systeem.

In het 3^e kwartaal van dit jaar zal gestart worden met de evaluatie van dit gegevensbeschermingsbeleid. Aan de hand hiervan zal een nieuw gegevensbeschermingsbeleid voor de volgende periode van 5 jaar worden vastgesteld.

Aldus vastgesteld door het college van burgemeester en wethouders van de gemeente Nieuwkoop op 2 april 2024,

*Burgemeester
Robbert-Jan van Duijn*

*Gemeentesecretaris
Nicolette Caspers*