FG-JAARVERSLAG 2025

Gemeente Nieuwkoop

Functionaris gegevensbescherming [redacted], 30 maart 2025

FG-Jaarverslag 2025 Gemeente Nieuwkoop

Inhoudsopgave

1. Managementsamenvatting

Op grond van de Algemene Verordening Gegevensbescherming brengt de functionaris gegevensbescherming (FG) jaarlijks verslag uit aan het College van Burgemeester en Wethouders over de maatregelen die de gemeente Nieuwkoop getroffen heeft om te kunnen waarborgen en aantonen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met de AVG.

Op basis van de parameters uit de Baseline bescherming Persoonsgegevens toetst de FG in hoeverre de gemeente aan de eisen van de AVG voldoet. Daarnaast geeft de FG per parameter aan binnen welke fase van het groeimodel de gegevensbescherming zich bevindt.

De gemeente Nieuwkoop heeft een basis privacy volwassenheidsniveau bereikt. In principe zijn hiervoor alle randvoorwaarden aanwezig. Wel blijft een aandachtspunt de privacy governance. De bescherming van persoonsgegevens is namelijk geen automatisme.

De conclusies uit dit jaarverslag hebben dan ook grotendeels betrekking op de sturing van het management op het waarborgen van de bescherming van persoonsgegevens. Het management zal meer gericht moeten sturen op het initiëren van DPIA's, het uitvoeren van de daaruit voortkomende beheersmaatregelen, het omarmen en onderhouden van het register van verwerkingsactiviteiten in het Privacy Information Management System en het trainen van hun medewerkers.

Het werkproces Ondermijning dient opnieuw ontworpen te worden. Het is nu onduidelijk of persoonsgegevens wel rechtmatig verwerkt worden en of de betrokkenen geïnformeerd worden over het verwerken van hun persoonsgegevens.

Het privacy-bewustzijn binnen de gemeentelijke organisatie moet minder vrijblijvend uitgevoerd worden. Zet een cyclus van wekelijkse trainingen op en geef deze een bij voorkeur verplichtend karakter.

2. Inleiding

2.1 Achtergrond

Per 1 mei 2020 heeft de gemeente Nieuwkoop een interne functionaris gegevensbescherming (FG) aangewezen. Deze aanwijzing is overeenkomstig artikel 37 van de Algemene Verordening Gegevensbescherming (AVG) verplicht voor overheidsorganisaties. De gemeente heeft hierbij gekozen voor een constructie waarbij de FG gedeeld wordt met de gemeenten Alphen aan den Rijn, Kaag en Braassem en Waddinxveen.
Naast het informeren en adviseren van de gemeente over haar verplichtingen uit hoofde van de AVG, ziet deze onafhankelijke functionaris toe op de juiste naleving van deze verordening.

2.2 Doelstelling

Jaarlijks brengt de FG een verslag uit aan het College van Burgemeester en Wethouders over de maatregelen die de gemeente getroffen heeft om te kunnen waarborgen en aantonen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met de AVG. In dit verslag wordt niet alleen de stand van zaken weergegeven met betrekking tot de belangrijkste aspecten van de bescherming van persoonsgegevens, maar worden ook adviezen gegeven en aanbevelingen gedaan ter verbetering van de gegevensbescherming.

2.3 Aanpak

Om te kunnen bepalen in welke mate de gemeente Nieuwkoop voldoet aan haar verplichtingen die voortvloeien uit de AVG, heeft de FG door middel van interviews, gesprekken, documentatiestudie en het bijwonen van overleggen een beeld kunnen vormen van de stand van zaken van de gegevensbescherming. Leidraad bij het beoordelen van de bevindingen is de door de FG opgestelde Baseline Bescherming Persoonsgegevens.

Om verrassingen te voorkomen brengt de FG elke drie maanden aan de gemeentesecretaris verslag uit van de stand van zaken. De aanpak van de FG is zoals de AVG voorschrijft altijd risicogestuurd, dat wil zeggen dat hij bij de uitvoering van zijn taken altijd prioriteiten stelt en zijn inspanningen richt op die zaken waarbij er sprake is van grotere risico's in termen van gegevensbescherming.

3. Leeswijzer

3.1 Parameters

De Functionaris voor Gegevensbescherming (FG) heeft een Baseline Bescherming Persoonsgegevens opgesteld op basis van de eisen van de AVG. Deze eisen zijn vertaald naar concrete en praktisch hanteerbare normen, hier parameters genoemd. Door inhoud te geven aan deze parameters kan de gemeente Nieuwkoop aantonen dat passende maatregelen zijn genomen om de bescherming van persoonsgegevens te waarborgen.

De FG beoordeelt aan de hand van de parameters in hoeverre de gemeente Nieuwkoop passende maatregelen neemt. Per parameter wordt eerst aangegeven binnen welke context de wettelijke eisen gezien moeten worden. Aansluitend worden de bevindingen van de FG aangegeven en afgesloten wordt met een kort advies.

3.2 Groeimodel

Het is niet realistisch om onmiddellijk een volledige naleving van de eisen van de AVG te verwachten van de gemeente Nieuwkoop. Mogelijk is volledige naleving zelfs onhaalbaar. Desondanks ontslaat dit de gemeente niet van de verplichting om voortdurend te streven naar verbetering. De ingevulde parameters moeten worden beschouwd als bouwstenen voor een groeimodel, waarbinnen de gemeente zelf haar ambitie en volwassenheidsniveau kan bepalen. In dit model zijn de volgende fasen te onderscheiden:

Initieel	• minimale vereisten van de AVG zijn aanwezig • situationeel op verwerkingsniveau geborgd • succes afhankelijk van inzet individuen • ad hoc herhaling van activiteiten privacy bewustzijn
Basis	• verwerkingen in het register zijn actueel • risicobesef aanwezig bij sleutelfiguren • succes door teaminzet • periodieke herhaling activiteiten privacy bewustzijn
Standaard	• verwerkingen worden cyclisch actueel gehouden • bescherming persoonsgegevens is organisatie breed • alle medewerkers worden standaard meegenomen • externe discipline organisatie
Integraal	• gegevensbescherming vanzelfsprekend onderdeel elk proces • interne discipline organisatie
Optimaal	• focus op systematische verbetering alle organisatieonderdelen • radicale aanpassing mogelijk na verandering externe factoren

Bij de conclusie wordt ten aanzien van de bescherming van persoonsgegevens per parameter aangegeven in welke fase de gemeente Nieuwkoop zich bevindt. Daarbij wordt ook vermeld welke prioriteit de FG geeft aan de invulling van de parameter. Het FG-Jaarverslag wordt afgesloten met de belangrijkste aanbevelingen.

4. Parameters

4.1 Visie, doelen en beleid

Context: Een heldere visie op privacy is van groot belang voor de inbedding, vooruitgang en ontwikkeling van de bescherming van persoonsgegevens. Een visie geeft richting en benoemt de ambities van de gemeente met betrekking tot de bescherming van persoonsgegevens. Uit deze visie worden specifieke, meetbare, aanvaardbare, realistische en tijdgebonden doelen afgeleid. Het behalen van deze doelen zorgt voor de verwezenlijking van de visie. Het gegevensbeschermingsbeleid beschrijft op welke manier wordt voldaan aan de geldende wet- en regelgeving. De doelen die de gemeente zichzelf heeft gesteld, vormen ook input voor dit beleid.

Bevindingen: De gemeente heeft in 2025 op onderdelen uitvoering gegeven aan het gegevensbeschermingsbeleid 2023-2027. Overeenkomstig de doelen voor 2025 is het register van verwerkingsactiviteiten in het Privacy Information Management System (hierna: PIMS) dat onderdeel uitmaakt van het Information Security Management System (hierna: ISMS), gevuld met alle verwerkingen van persoonsgegevens. Daarnaast is nu ook het datalekregister in het PIMS opgenomen. Nog niet is toegekomen aan het inzichtelijk maken van alle samenwerkingsverbanden en gemeenschappelijke regelingen waar de gemeente deel van uit maakt.

De gemeente heeft huisregels opgesteld voor het gebruik van bepaalde AI-toepassingen. Een beleidskader is nog in ontwikkeling. Er is echter nog geen visie ontwikkeld op het gebruik van deze toepassingen in de toekomst. Uit deze visie zou moeten blijken waarom de gemeente artificiële intelligentie wil inzetten en wat de toegevoegde waarde van AI is voor de gemeentelijke organisatie.

Volgens de AI-verordening is het vanaf 2 februari 2025 verplicht voor organisaties werk te maken van AI-geletterdheid. Een belangrijke voorwaarde voor de verantwoorde inzet van AI is een toereikend kennisniveau bij medewerkers die met AI te maken krijgen. Het doel is dat alle relevante personen binnen de gemeentelijke organisatie geïnformeerde keuzes met betrekking tot AI-systemen kunnen maken. De gemeente moet inventariseren welke AI-systemen er gebruikt worden binnen de organisatie en welke kennis er al is. Hiervoor is ook een module verkrijgbaar binnen het ISMS.

Advies: Voer het gegevensbeschermingsbeleid verder uit en actualiseer het eventueel als externe factoren hier invloed op hebben. Stel naast beleid ook een visie op voor het gebruik van AI en onderzoek of de uitvoering van AI toepassingen ook in het ISMS opgenomen kan worden.

4.2 Governance

Context: De verantwoordelijkheid voor het waarborgen van de bescherming van persoonsgegevens rust niet alleen op één persoon of de privacy-officer. Verschillende medewerkers binnen de gemeente spelen een rol, zij het in verschillende mate, om te voldoen aan de eisen van wet- en regelgeving. Een heldere toewijzing van taken en bevoegdheden, evenals duidelijke rapportagelijnen, zorgen ervoor dat het gegevensbeschermingsbeleid en de AVG op een juiste manier worden nageleefd.

Bevindingen: De taken, bevoegdheden en rapportagelijnen zijn schriftelijk vastgelegd in een Privacy Governance document. Onderdeel van de verantwoordelijkheden van het management is dat niet alleen de DPIA's worden uitgevoerd maar ook de daaruit volgende beheersmaatregelen, en wel vóórdat de verwerkingen van persoonsgegevens gaan plaatsvinden. Het aantal uitgevoerde DPIA's in 2025 was niet groot en de doorlooptijd vaak lang. Het initiëren van DPIA's en het bewaken van het tempo is echter niet de verantwoordelijkheid van de privacy officer maar van de procesverantwoordelijken binnen het management. Dit geldt ook voor het monitoren van de uitvoering van de beheersmaatregelen.

Advies: Blijf het eigenaarschap bij de procesverantwoordelijken voor gegevensbescherming stimuleren zodat de taken en verantwoordelijkheden steeds meer betekenis gaan krijgen bij het management en vervolgens ook bij de rest van de medewerkers.

4.3 Mensen en Middelen

Context: Het waarborgen van de bescherming van persoonsgegevens vergt inzet van medewerkers en middelen van de gemeente. Dit kan extra personeelsinzet betekenen, het inschakelen van externe experts of de aanschaf van specifieke applicaties of systemen. De governance-afspraken dienen als leidraad bij het maken van keuzes om de beperkte middelen effectief in te zetten voor het bereiken van de beoogde resultaten.

Bevindingen: De bemensing op privacy (i.e. de privacy-officer) was binnen de gemeente Nieuwkoop in 2025 op sterkte. Er is nog geen formatie voor de uren voor werkzaamheden met betrekking tot de Wet politiegegevens. Wellicht is hiervoor een kleine uitbreiding van uren gewenst.
De bescherming van persoonsgegevens vraagt ook om actieve betrokkenheid van het management: uit de ervaringen met het uitvoeren van DPIA's en het in kaart brengen van het werkproces rondom ondermijning blijkt dat het belang van persoonsgegevensbescherming bij sommigen nog verder benadrukt kan worden.

Advies: Zorg dat de privacy officer zich kan blijven ontwikkelen. Draag ook als management het belang van de bescherming van persoonsgegevens uit.

4.4 Risicomanagement

Context: Het beheren van risico's is een doorlopend proces waarbij de risico's met betrekking tot gegevensbescherming worden geïdentificeerd, beoordeeld en op passende wijze worden beheerd. Risicomanagement richt zich op het controleren van risico's die ontstaan tijdens het verwerken, inclusief het verzamelen, opslaan en doorgeven van persoonsgegevens. Door Privacy by Design toe te passen en Data Protection Impact Assessments (DPIA's) uit te voeren, worden de risico's bij de ontwikkeling, implementatie en uitvoering van de gegevensverwerking geanalyseerd en zo veel mogelijk beperkt of weggenomen.

Bevindingen: Op basis van de conclusies uit de in december 2022 opgeleverde DPIA Ondermijning en het FG-advies heeft de gemeente de intentie het proces Ondermijning zodanig in te richten dat de bescherming van persoonsgegevens op de juiste wijze gewaarborgd is. In 2025 was er echter nog steeds geen aangepast werkproces opgeleverd waarin de verwerkingen van persoonsgegevens in zijn weergegeven.

In 2025 zijn de DPIA's Platform Arbeidsmigranten, Peutermonitor en Personeel/YouForce uitgevoerd. Aangetoond zal nog wel moeten worden dat de in de DPIA voorgestelde mitigerende maatregelen alsmede de aanbevelingen van de FG uitgevoerd zijn.

Het is mogelijk dat de uitkomst van een FG-advies op een DPIA niet overeenkomt met de wensen of verwachtingen van procesverantwoordelijken. Indien afgeweken wordt van het FG-advies is het goed gebruik dit te laten vast leggen door de verwerkingsverantwoordelijke. Ook bestaat altijd de mogelijkheid de DPIA ter voorafgaande raadpleging voor te leggen aan de Autoriteit Persoonsgegevens.

De gemeente Nieuwkoop heeft voor de bescherming van haar personeel en eigendommen beveiligingscamera's geïnstalleerd of is voornemens dat te doen. Cameratoezicht staat op de lijst van de Autoriteit Persoonsgegevens voor verplicht uit te voeren DPIA's. Hier is nog steeds geen DPIA voor uitgevoerd.

Binnen de wettelijke taken die de gemeente uitvoert in het kader van de Wet Maatschappelijke Ondersteuning 2025 en de Jeugdwet worden gevoelige en bijzondere persoonsgegevens verwerkt. De inzet van nieuwe technologieën en veranderingen in deze werkprocessen maken de uitvoering van een DPIA op korte termijn noodzakelijk.

Advies: Hervorm het werkproces Ondermijning zodanig dat de bescherming van de te verwerken persoonsgegevens geborgd is. Voer het tempo van het uitvoeren van de DPIA's op en monitor ook de voortgang van de uitvoering van de beheersmaatregelen.

4.5 Doelbinding

Context: Een principe van de AVG is dat gegevens worden verwerkt en verzameld voor een

specifiek, duidelijk omschreven en gerechtvaardigd doel. Dit doel moet al zijn vastgesteld voordat de gemeente begint met verwerken. 'Welbepaald' betekent dat de beschrijving van het doel duidelijk moet zijn en niet vaag of breed, zodat het tijdens het verzamelproces als richtlijn kan dienen om te bepalen of de gegevens nodig zijn voor dat doel. Het doel mag ook niet later in het verzamelproces worden bepaald. 'Duidelijk omschreven' betekent dat de gemeente het doel van de verwerking helder en nauwkeurig moet beschrijven. 'Gerechtvaardigd' betekent dat de verwerking alleen mag plaatsvinden op basis van een wettelijke grondslag.

Bevindingen: In 2022 is de DPIA Ondermijning opgeleverd. Omdat onder het begrip Ondermijning persoonsgegevens worden verwerkt waarvan het vaak niet duidelijk is op basis van welke grondslag deze verwerkingen plaatsvinden, heeft de FG geadviseerd het proces Ondermijning te herontwerpen op basis van het beschikbaar wettelijk instrumentarium. Het nieuwe werkproces Ondermijning is echter nog steeds niet opgeleverd. Hierdoor is het voor de FG niet mogelijk te controleren of de persoonsgegevens worden verwerkt op basis van een gerechtvaardigd doel.

Advies: Herontwerp in 2026 het proces Ondermijning op basis van het beschikbaar wettelijk instrumentarium.

4.6 Register van verwerkingsactiviteiten

Context: Een van de eisen die gesteld worden om naleving van de AVG aan te kunnen tonen is het bijhouden van het register van verwerkingsactiviteiten. In dit register wordt vastgelegd welke verwerkingen van persoonsgegevens er in de organisatie plaatsvinden, hoe deze verantwoord worden en welke beveiligingsmaatregelen worden genomen voor de bescherming van deze persoonsgegevens. Het register maakt ook efficiënt toezicht op de rechtmatigheid van de verwerkingsactiviteiten mogelijk en zorgt ervoor dat kan worden voldaan aan de rechten van betrokkenen.

Bevindingen: Het register van verwerkingsactiviteiten is inmiddels ingericht in het PIMS van het ISMS. Nu dit register staat, is het wel de bedoeling dat de procesverantwoordelijken (of hun medewerkers) het register actueel en compleet houden. Dit is niet de verantwoordelijkheid van de privacy officer maar de taak van de procesverantwoordelijken waarbij de privacy officer kan ondersteunen. Het onder de aandacht brengen van het belang van het bijhouden van het register zal nog veel zendingswerk met zich mee brengen.

Het register van verwerkingsactiviteiten is nog vrij abstract. In het kader van transparantie naar de inwoners en het informeren over de verwerkingen van hun persoonsgegevens dient het register zodanig ingericht te worden dat het op termijn ook gepubliceerd kan worden. Dit betekent wel dat de verwerkingen in begrijpelijker taal verwoord zouden moeten worden.

Advies: Zorg voor zoveel mogelijk commitment en eigenaarschap bij het management om het register van verwerkingsactiviteiten goed bij te houden.

4.7 Beveiliging

Context: De gemeente moet passende technische en organisatorische maatregelen nemen om persoonsgegevens veilig te verwerken. Deze maatregelen dienen ter bescherming van persoonsgegevens tegen ongeautoriseerde toegang, onbedoelde openbaarmaking, vernietiging, verlies van toegang, wijziging, en tegen onrechtmatige of onnodige verzameling en verdere verwerking.

Bevindingen: Er was in 2025 nog geen volledige inventarisatie van de kritieke bedrijfsprocessen en kritieke bedrijfsapplicaties uitgevoerd. Ook was er nog geen business continuïteitsplan voor elke kritiek bedrijfsproces. Uit de in 2025 gehouden cyberveiligheidsoefening is gebleken dat in het geval van een cyberincident het van het grootste belang is dat er snel geschakeld kan worden tussen Informatieveiligheid/Ciso en de procesverantwoordelijken van de kritieke bedrijfsprocessen. Dit betekent wel dat deze kritieke bedrijfsprocessen bekend moeten zijn en dat voor elke kritiek bedrijfsproces er een actueel business continuïteitsplan aanwezig is. De coördinatie tussen de Ciso en de procesverantwoordelijken bij het uitvoeren van deze business continuïteitsplannen moet regelmatig en zorgvuldig geoefend worden omdat nog meer dan bij een ander incident, vooral in de eerste fase, snelheid geboden is.

Advies: Inventariseer zo snel mogelijk alle kritieke bedrijfsprocessen, ontwikkel daarop business continuïteitsplannen en ga daarmee cyberincidenten oefenen.

4.8 Bewaartermijnen

Context: Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld. De gemeente hanteert ten aanzien van de verwerkingen van persoonsgegevens bewaartermijnen en hoort de nodige maatregelen te treffen zodat deze niet worden overschreden.

Bevindingen: De AVG vergt dat in het register van verwerkingsactiviteiten de bewaartermijnen bij elke verwerking worden opgenomen. Nog niet alle bewaartermijnen staan nu in het register van verwerkingsactiviteiten. Daarnaast wordt in plaats van de termijn soms vermeld dat de persoonsgegevens bewaard worden conform de selectielijst. Omdat het register in de toekomst ook gepubliceerd zou moeten worden, verdient het de voorkeur ook de concrete termijn uit de selectielijst op te nemen.

Advies: Neem van alle verwerkingen in het register van verwerkingsactiviteiten de concrete bewaartermijnen op.

4.9 Doorgifte

Context: Persoonsgegevens kunnen op drie manieren doorgegeven worden door externe partijen. Ten eerste aan partijen die in opdracht van de gemeente werkzaamheden uitvoeren waarbij persoonsgegevens verwerkt worden. De gemeente is dan verwerkingsverantwoordelijke en de externe partij verwerker. In deze situatie dient een *verwerkersovereenkomst* gesloten te worden. Daarnaast geeft de gemeente ook persoonsgegevens door in situaties waarbij meerdere verwerkingsverantwoordelijken gezamenlijk de doelen en middelen voor de verwerking bepalen, zij zijn dan gezamenlijk verwerkingsverantwoordelijk. Dan dient een *onderlinge regeling* gesloten te worden. In het geval de gemeente persoonsgegevens doorgeeft aan een andere verwerkingsverantwoordelijke is een dataleveringsovereenkomst gewenst.

Bevinding: De gemeente besteedt taken uit aan andere gemeenten, organisaties en samenwerkingsverbanden. Indien deze partijen te kwalificeren zijn als verwerker, zal op grond van artikel 28 AVG de verwerking geregeld moeten worden in een verwerkersovereenkomst. Hiermee kan aangetoond worden dat er voldoende waarborgen getroffen zijn die maken dat de verwerker de persoonsgegevens volgens de regels van de AVG beschermt. De verwerkersovereenkomst blijft van kracht zolang de verwerking van persoonsgegevens plaatsvindt en eindigt wanneer de verwerking stopt of wanneer de overeenkomst wordt beëindigd. In de tussentijd kunnen echter wijzigingen in het werkproces c.q. de verwerking plaatsvinden die een aanpassing van de verwerkersovereenkomst noodzaken. Er vindt nu geen standaard monitoring van de verwerkersovereenkomsten plaats.

Advies: Integreer de monitoring van de verwerkersovereenkomsten in het contractmanagement zodat deze actueel zijn en tijdig aangepast kunnen worden.

4.10 Intern toezicht

Context: Elke overheidsorganisatie is verplicht een functionaris gegevensbescherming (FG) aan te wijzen. Deze onafhankelijke functionaris ziet toe op de naleving AVG, informeert en adviseert de gemeente over de verplichtingen die voorvloeien uit de AVG, adviseert over en ziet toe op de uitvoering van Data Protection Impact Assessments en fungeert als contactpunt voor de Autoriteit persoonsgegevens en werkt desnoods daarmee samen.

Bevindingen: De FG heeft vernomen dat er frustraties bestaan aangaande zijn advisering over DPIA's. Een functionaris gegevensbescherming is een toezichthouder en adviseur. In beginsel behartigt hij primair de belangen op het gebied van gegevensbescherming van de betrokkenen, i.e. de inwoners van de gemeente Nieuwkoop en van andere personen van wie de gemeente persoonsgegevens verwerkt.

Het belangrijkste doel van een DPIA is het in kaart brengen van de risico's voor de betrokkenen en vervolgens daarop maatregelen formuleren om deze risico te mitigeren. De restrisico's voor de betrokkenen worden hiermee duidelijk. Als deze risico's laag blijken, kan de voorgenomen verwerking plaatsvinden. Zijn de restrisico's hoog, dan zal de FG adviseren de verwerking niet uit te voeren of de verwerking ter voorafgaande raadpleging voor te leggen aan de Autoriteit Persoonsgegevens.

Als er geen grondslag is voor het verwerken van persoonsgegevens, zal het risico hoog zijn omdat de gemeente dan onrechtmatig persoonsgegevens verwerkt. Het is echter de keuze van de verwerkingsverantwoordelijke om hoge risico's wel of niet te accepteren dan wel de DPIA voor te leggen aan de Autoriteit Persoonsgegevens. Indien de adviezen van de FG niet opgevolgd worden, is het voor de verwerkingsverantwoordelijke goed gebruik dat te documenteren.

Advies: Volg in principe de adviezen van de FG op DPIA's op. Mocht dat niet zo zijn, documenteer dan het afwijken van de adviezen. Leg desnoods de DPIA ter voorafgaande raadpleging voor aan de Autoriteit Persoonsgegevens.

4.11 Rechten betrokkenen

Context: Iedere betrokkene wiens persoonsgegevens door de gemeente Nieuwkoop worden verwerkt heeft het recht te weten welke gegevens dat zijn en waarvoor en op welke wijze deze worden verwerkt. De gemeente moet hier transparant over zijn zodat de betrokkene zonder onevenredige kosten en/of moeite zijn gegevens kan laten corrigeren of de gemeente aanspreken op de onrechtmatige verwerking van persoonsgegevens. De gemeente moet binnen één maand richting de betrokkene reageren over het gevolg dat aan het verzoek is gegeven.

Bevindingen: Toegang tot uitoefening van rechten van betrokkenen is digitaal geregeld door middel van DigiD op de gemeentelijke website. Er zijn in 2025 drie inzageverzoeken binnengekomen. Deze verzoeken zijn binnen de termijn afgehandeld. Vier verwijderverzoeken werden ontvangen. Drie daarvan betroffen persoonsgegevens die reeds verwijderd waren en één is deels geweigerd in verband met de bepalingen uit de Archiefwet.

Advies: Test deze omgeving met enige regelmaat om te onderzoeken of de procedure efficiënt en effectief verloopt. Neem de inzageverzoeken ook op in het PIMS.

4.12 Datalekken

Context: Een snelle en effectieve respons op een datalek kan eventuele schadelijke gevolgen voor de betrokkenen voorkomen of beperken. Bovendien biedt het de mogelijkheid om te leren van het voorval, waardoor vergelijkbare datalekken in de toekomst kunnen worden voorkomen. Het is belangrijk om datalekken altijd te melden aan de privacy-officer zodat

deze de datalekken kan registeren. Bij een (hoog) risico dienen ze ook gemeld te worden aan de Autoriteit Persoonsgegevens en de betrokken personen.

Bevindingen: De gemeente Nieuwkoop beschikt over een register datalekken. Voor 2025 zijn elf datalekken geregistreerd. De datalekken worden inmiddels ook in het Privacy Information Management System (PIMS) opgenomen. De datalekken werden gerechtvaardigd niet gemeld aan de Autoriteit Persoonsgegevens. Wel werd bij twee van de datalekken contact opgenomen met de betrokkene.

Advies: Registreer de datalekken alleen nog maar in het PIMS. Blijf datalekken monitoren en evalueren om te voorkomen dat dezelfde fouten gemaakt worden, ook al is er geen of weinig risico aan verbonden.

4.13 Bewustzijn

Context: Het is niet altijd vanzelfsprekend dat medewerkers begrijpen hoe ze persoonsgegevens moeten beschermen. Daarom is het belangrijk dat ze niet alleen via voorlichting en educatie de basisprincipes van de AVG leren, maar ook dat ze begrijpen waarom het belangrijk is om persoonsgegevens te beschermen. Op het gebied van gegevensbescherming is privacy bewustzijn vaak de achilleshiel een organisatie. Zelfs als de processen en procedures van een organisatie goed beveiligd zijn, zullen de maatregelen niet effectief zijn als medewerkers zich niet bewust zijn van hun verantwoordelijkheden. Daarom is het essentieel om voortdurend aandacht te besteden aan privacy bewustzijn.

Bevindingen: Er is een cyclus van privacy-diners opgestart ter verhoging van het privacy bewustzijn. Team Bestuurlijk juridische zaken en team Personeel & organisatie hebben hier al aan deelgenomen. Daarnaast zijn bijeenkomsten gehouden voor nieuwe medewerkers. Om alle medewerkers én management op een adequaat niveau te krijgen op het gebied van privacy bewustzijn, is het sterk aan te raden om op wekelijkse basis trainingen te geven aan kleine groepen van vijf tot tien personen. Dit hoeven geen fysieke bijeenkomsten te zijn, maar kan ook digitaal. Dit is agenda-technisch beter te plannen en het is zo ook makkelijker om thuiswerkende collega's te bereiken.

Advies: Voer het aantal privacy trainingen flink op in 2026. Zorg ervoor dat er een cyclus van wekelijkse trainingen ontstaat om het draagvlak voor en de kennis van de AVG bij zowel medewerkers als management te vergroten. Maak deze bijeenkomsten niet facultatief maar geef ze een verplicht karakter.

5. Conclusies

De gemeente Nieuwkoop heeft een basis privacy volwassenheidsniveau bereikt. Het versterken van de privacy governance blijft echter belangrijk: de procesverantwoordelijken in het management moeten in de lead zijn bij het onderhouden van het register van verwerkingsactiviteiten, het initiëren van DPIA's en het controleren op de uitvoering van de uit de DPIA's voortkomende beheersmaatregelen.

Het wordt echt tijd dat het werkproces Ondermijning opnieuw ontworpen wordt. Dit was al een dringende aanbeveling uit het FG-advies op de DPIA Ondermijning uit 2022. Het is nu onduidelijk of persoonsgegevens wel rechtmatig verwerkt worden en of de betrokkenen geïnformeerd worden over het verwerken van hun persoonsgegevens.

Het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie moet op regelmatiger basis en minder vrijblijvend opgezet worden. Bij voorkeur met een verplicht karakter.

Hieronder wordt aangegeven in welke fase de gemeente zich bevindt met betrekking tot de invulling van de parameters en welke prioriteit de FG hier aan geeft. Dikgedrukte kapitale letters geven de verandering ten opzichte van het vorig jaar weer.

	Parameter	Fase groeimodel		Prioriteit	
		2024	2025	2025	2026
4.1	Visie, doelen en beleid	Basis	Basis	Midden	Midden
4.2	Governance	Basis	Basis	Hoog	Hoog
4.3	Mensen en Middelen	Basis	Basis	Laag	Laag
4.4	Risicomanagement	Basis	Basis	Hoog	Hoog
4.5	Doelbinding	Initieel	Initieel	Midden	**HOOG**
4.6	Register van verwerkingsactiviteiten	Basis	Basis	Hoog	Hoog
4.7	Beveiliging	Basis	Basis	Midden	Midden
4.8	Bewaartermijnen	Initieel	Initieel	Laag	Laag
4.9	Doorgifte	Initieel	Initieel	Laag	Laag
4.10	Intern Toezicht	Basis	Basis	Laag	Laag
4.11	Rechten betrokkenen	Basis	Basis	laag	Laag
4.12	Datalekken	Basis	Basis	Hoog	**MIDDEN**
4.13	Bewustzijn	Basis	Basis	Hoog	Hoog

6. Aanbevelingen

De belangrijkste aanbevelingen zijn afgestemd op de parameters waarbij de prioriteit *Hoog* is. Uiteraard is het raadzaam ook de andere adviezen in dit FG-Jaarverslag op te volgen.

1. Zorg dat de privacy governance zowel bij management als medewerkers betekenis krijgt;
2. Laat de procesverantwoordelijken het register van verwerkingsactiviteiten onderhouden;
3. Voer het tempo van uitvoeren van DPIA's op;
4. Controleer of de beheersmaatregelen uitgevoerd worden;
5. Herontwerp het werkproces Ondermijning;
6. Maak meer werk van privacy-bewustzijn. Maak trainingen bij voorkeur verplicht.