FG-JAARVERSLAG 2024

Gemeente Nieuwkoop

Functionaris gegevensbescherming mr. R.R. de Vries, 14 maart 2025

FG-Jaarverslag 2024 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 nadert het basis privacy volwassenheidsniveau. Naar aanleiding van de in 2023 vastgestelde visie op gegevensbescherming is gegevensbeschermingsbeleid opgesteld. Op basis van dit beleid wordt een werkprogramma uitgevoerd.

Het inrichten en compleet maken van het register van verwerkingsactiviteiten in het ISMS vordert langzaam maar gestaag en zal in 2025 verder doorgang vinden. Het bijhouden van het ISMS en het reageren op de acties die het systeem vraagt, zullen wel meer commitment en inzet van het management vergen.

De governance op het gebied van gegevensbescherming moet daarom voor ieder duidelijk zijn: dit betekent dat alle medewerkers moeten weten wat hun taken en verantwoordelijkheden zijn en hoe de rapportagelijnen lopen. Het management heeft hierin een voorbeeldfunctie.

Hiervoor moet het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie weer opgepakt worden. Zet een cyclus van trainingen op en pas training en voorlichting aan naar de wensen en behoeften van de verschillende afdelingen en medewerkers.

2. Inleiding

2.1 Achtergrond

Per 1 mei 2020 heeft de gemeente Nieuwkoop een nieuwe (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: Het gegevensbeschermingsbeleid voor de periode 2023-2027 alsmede het werkprogramma privacy 2024-2025 zijn vastgesteld door het College van Burgemeester en Wethouders. Hiermee is weer een stap in privacy-volwassenheid gezet: de gemeente komt dan vanuit een afwachtende positie waarin zij de aanbevelingen van de FG overneemt, naar een situatie waarin zij proactief werkt aan het verbeteren van de bescherming van persoonsgegevens.

De gemeente heeft huisregels opgesteld voor het gebruik van bepaalde AI-toepassingen (Large Language Models). Deze huisregels geven mogelijkheden, richtlijnen en risico's aan van het gebruik van AI. Er is echter nog geen beleid ontwikkeld voor het gebruik van AI in de zin dat de gemeente een visie heeft op het gebruik van deze toepassingen in de toekomst.

Vanaf 2 februari 2025 verplicht de AI-verordening 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.

Advies: Voer het gegevensbeschermingsbeleid verder uit en actualiseer het eventueel als externe factoren hier invloed op hebben. Stel ook beleid op voor het gebruik van AI.

4.2 Governance

Context: De verantwoordelijkheid voor het waarborgen van de bescherming van persoonsgegevens rust niet alleen op één persoon of de privacy-officers. 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: Het in 2022 opgestelde governance document geeft de taken, verantwoordelijkheden en rapportagelijnen met betrekking tot gegevensbescherming weer. Nog niet iedereen in de organisatie is echter volledig doordrongen van de verantwoordelijkheden op dit gebied. Dit blijkt bijvoorbeeld uit de moeite die de privacy-officer zich moet getroosten om medewerkers te betrekken bij het vullen van het register van verwerkingsactiviteiten in het ISMS. Ook is nog niet bij iedereen in het management duidelijk dat de verantwoordelijkheid voor het actueel houden van dit register voortaan bij hen ligt.

Advies: Zorg dat de taken en verantwoordelijkheden betekenis krijgen binnen de gemeente en niet alleen woorden op papier zijn. Het hogere management vervult hierbij een voorbeeldfunctie.

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: In het PIT (privacy- en informatiebeveiligingsteam) bespreken de CISO (chief information security officer), de teamleider Bestuurlijk Juridische Zaken, de communicatieadviseur en de privacy officer elke twee weken de ontwikkelingen op het gebied van gegevensbescherming door en de te ondernemen activiteiten. Ook de FG sluit daarbij aan.

De functie van privacy-officer is op sterkte. De privacy-officer krijgt ook voldoende ruimte om zich bij te scholen door middel van opleidingen. Na het vertrek van de CISO begin 2024 is deze functie tijdelijk opgevuld met een externe medewerker. Eind 2024 is deze functie weer fulltime ingevuld en niet langer meer gepositioneerd binnen I&A. Deze positionering zorgt ervoor dat de CISO zijn taken onafhankelijker kan uitvoeren en het toezicht op de informatieveiligheid beter kan waarborgen.

Advies: Blijf op de ingeslagen weg doorgaan.

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 2024 is er echter nog steeds geen aangepast werkproces opgeleverd waarin de verwerkingen van persoonsgegevens in zijn weergegeven.

In 2024 zijn de DPIA Bodycam, DPIA Lokale jeugdhulp, DPIA Welzijn op recept en de DPIA Welzijnsbezoeken correct uitgevoerd. Aangetoond zal nog wel moeten worden dat de in de DPIA voorgestelde mitigerende maatregelen alsmede de aanbevelingen van de FG uitgevoerd zijn.

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.

Advies: Hervorm het werkproces Ondermijning zodanig dat de bescherming van de te verwerken persoonsgegevens geborgd is. Ga verder met het uitvoeren van de DPIA's.

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: De gemeente wil een visie ontwikkelen op Datagedreven werken. Er worden eerste stappen gezet op het gebied van informatie gestuurd werken door databronnen met elkaar te combineren. Er moet dan altijd bekend zijn welke gegevens opgeslagen worden en wie verantwoordelijk is voor de kwaliteit van deze gegevens. Ook moet voldaan zijn aan de hier bovengenoemde beginselen van de AVG. Concreet betekent dit dat wanneer persoonsgegevens aan elkaar gekoppeld gaan worden, altijd vooraf een welbepaald, duidelijk omschreven en gerechtvaardigd doel aanwezig moet zijn.

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 dit plaatsvindt, heeft de FG geadviseerd het proces Ondermijning te herontwerpen op basis van het beschikbaar wettelijk instrumentarium. Aan het opstarten van dit herontwerp wordt erg weinig aandacht geschonken terwijl er wel regelmatig "ondermijningszaken" lopen.

Advies: Ontwikkel een visie op datagedreven werken vóórdat databronnen gecombineerd gaan worden en persoonsgegevens gekoppeld. Herontwerp in 2025 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: De gemeente Nieuwkoop was in 2024 nog steeds bezig met het inrichten van het Information Security Management Systeem (ISMS) waar het register van verwerkingsactiviteiten een onderdeel van is. Duidelijk is inmiddels wel dat het actueel houden van het systeem niet de verantwoordelijkheid van de privacy officer is: deze heeft hierin een faciliterende rol. Het management is echter *in the lead* om de verwerkingen van persoonsgegevens actueel en compleet te houden. Dit besef is wellicht nog niet bij alle leden van het management aanwezig. Het belang van het ISMS zal daarom goed duidelijk gemaakt moeten worden.

Advies: Zorg voor zoveel mogelijk commitment en eigenaarschap bij het management om het ISMS te completeren en vervolgens 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: Het is in 2024 niet gelukt zowel het informatieveiligheidsdeel als het privacydeel van het ISMS volledig in te richten. Een van de onderdelen van het

Informatiebeveiligingsbeleid 2020-2024 was het onderzoek naar de omvang en diepgang van het business continuïteitsplan. Dit onderzoek is in 2024 afgerond maar er was in 2024 nog geen concreet plan opgeleverd. Net als in 2023 is er in 2024 geen back-up en herstelbeleid en encryptiebeleid opgesteld. Dit beleid zal meegenomen worden in het nieuwe Informatieveiligheidbeleid dat in 2025 opgesteld zal worden. Verder is het belangrijk dat het bestuur en management weten hoe opgetreden moet worden tijden een cybercrisis. Oefening baart dan ook kunst.

Advies: Neem de nog niet gestarte projecten op in het nieuwe Informatieveiligheidsbeleid en voer deze projecten ook daadwerkelijk uit. Zorg dat zowel het register van verwerkingsactiviteiten als de rest van het ISMS in 2025 volledig gevuld wordt. Ga 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. Bij het vullen van het register van verwerkingsactiviteiten in het ISMS zullen de bewaartermijnen automatisch aan bod komen.

Advies: Neem van alle verwerkingen in het register van verwerkingsactiviteiten ook de bewaartermijnen op en geef daarbij aan op welke wettelijke bepaling deze zijn gebaseerd of een motivering van de noodzaak van de bewaartermijn.

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 echter geen 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: Per 1 januari 2024 is de FG ook aangewezen als FG voor de Wet politiegegevens. Over elk jaar zal de FG separaat een jaarverslag uitbrengen over de bescherming van politiegegevens zoals dit vereist is overeenkomstig deze wet.

Eind 2022 is een extern Wpg auditrapport opgeleverd over de periode 2019 t/m 2021 naar de verwerkingen van persoonsgegevens die vallen onder de Wet politiegegevens. Naar aanleiding van het afkeurend oordeel van de externe auditor heeft deze geadviseerd om het jaar daarop nogmaals een (extra) externe audit uit te voeren. Deze externe audit is in 2024 uitgevoerd maar in dat jaar is geen auditrapport opgeleverd door de externe auditor.

Onduidelijk is wat de stand van zaken is van het verbeteren van de tekortkomingen in de bescherming van deze persoonsgegevens.

De externe audits voor de Wet politiegegevens moeten elke vier jaar worden uitgevoerd. De Autoriteit Persoonsgegevens (AP) heeft aangegeven dat de tweede audit de periode 1 januari 2021 tot en met 31 december 2024 betreft, waarna de AP de aanlevering van de auditrapportages verwacht vanaf 1 maart 2025 tot uiterlijk 1 maart 2026. Het is dan zinvol om het verbeterplan aan te passen aan de uitkomsten van de extra externe audit. Dan kunnen vroegtijdig tekortkomingen worden geïnventariseerd en vervolgens verbetermaatregelen worden geïmplementeerd voordat de externe audit start. Met de uitvoering van een externe audit vanaf het derde kwartaal in 2025 is er dan voldoende tijd om uiterlijk 1 maart 2026 de auditrapportage aan te leveren bij de AP.

Advies: Zorg dat het externe auditrapport 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 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: Er zijn in 2024 zes verzoeken binnengekomen tot inzage, rectificatie of wissen van persoonsgegevens. De verzoeken zijn binnen de termijn afgehandeld dan wel afgewezen. Toegang tot uitoefening van rechten van betrokkenen is digitaal geregeld door middel van DigiD en redelijk eenvoudig te verkrijgen onder het kopje Privacy op de gemeentelijke website.

Advies: Test deze omgeving met enige regelmaat om te onderzoeken of de procedure efficiënt en effectief verloopt.

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. Het betreft hier een Excel bestand waarin voor 2024 elf datalekken geregistreerd zijn. In verband met het risico voor de rechten en vrijheden van een betrokkene, is één van deze datalekken gemeld aan de Autoriteit Persoonsgegevens. Daarnaast staan er nog twee datalekken dubbel in het bestand en zijn twee als datalek geregistreerde incidenten naar de mening van de FG geen datalek. Tevens heeft de FG van twee datalekken geen Topdesk melding ontvangen. Ook zijn twee andere meldingen helemaal niet in Topdesk gemeld.

De Procedure melding datalekken functioneert in principe goed. Na de melding in Topdesk is het echter beter en overzichtelijker als het datalek onmiddellijk geregistreerd wordt in de daarvoor bedoelde module in het ISMS in plaats van in een Excel bestand.

Advies: Neem het register van datalekken op in het ISMS. 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: Omdat alle medewerkers over een minimale basiskennis van gegevensbescherming moeten kunnen beschikken, is op het gebied van privacy-bewustzijn permanent onderhoud nodig. Het aantal privacy trainingen moet echt omhoog. Hiermee wordt het privacy bewustzijn groter. Dit zorgt ook voor een beter gevoelde governance en leidt tot meer draagvlak voor het bijhouden van het ISMS.

Advies: Voer het aantal privacy trainingen flink op in 2025. Zorg ervoor dat er een cyclus ontstaat om het draagvlak voor en de kennis van de AVG te vergroten.

5. Conclusies

De gemeente Nieuwkoop heeft in 2024 het basis privacy volwassenheidsniveau grotendeels bestendigt. De privacy governance blijft echter wel aandacht verdienen in het licht van het gebruik van het Information Security Management System en dan vooral ten aanzien van het inrichten en compleet maken van het register van verwerkingsactiviteiten. Het uitvoeren van DPIA's vindt gestaag plaats en dit tempo dient minimaal aangehouden te worden. Het registreren van de datalekken dient na de initiële melding in Topdesk bij voorkeur plaats te vinden in het ISMS. Het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie moet voortvarender en gestructureerd opgepakt worden.

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	
		2023	2024	2024	2025
4.1	Visie, doelen en beleid	Basis	Basis	Hoog	**MIDDEN**
4.2	Governance	Basis	Basis	Hoog	Hoog
4.3	Mensen en Middelen	Basis	Basis	Midden	**LAAG**
4.4	Risicomanagement	Basis	Basis	Hoog	Hoog
4.5	Doelbinding	Initieel	Initieel	Midden	Midden
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	Midden	**HOOG**
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 bij alle medewerkers betekenis krijgt.
2. Rond het invullen van het register van verwerkingsactiviteiten in het ISMS af.
3. Ga door met dit tempo van uitvoeren van DPIA's.
4. Registreer de datalekken in het ISMS.
5. Maak meer werk van privacy-bewustzijn. Maak presentaties gericht op specifieke groepen.