FG-JAARVERSLAG 2023

Gemeente Nieuwkoop

Functionaris gegevensbescherming mr. R.R. de Vries, 7 maart 2024

FG-Jaarverslag 2023 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 is goed op weg naar een basis privacy volwassenheidsniveau. Naar aanleiding van de in 2023 vastgestelde visie op gegevensbescherming is gegevensbeschermingsbeleid opgesteld. Dit beleid geeft aan hoe de doelen bereikt gaan worden waardoor de gemeente uiteindelijk haar visie kan verwezenlijken.

Het inrichten en compleet maken van het register van verwerkingsactiviteiten in het ISMS is gestart en zal in 2024 doorgang vinden. Het uitvoeren van Data Protection Impact Assessments kwam in 2023 goed op stoom. Beide zaken zullen wel commitment en inzet van het management vergen.

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

Het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie begint nu een grotere vlucht te krijgen. Ga daar mee door 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 en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Deze eisen zijn vertaald naar concrete en praktisch hanteerbare normen, ook wel 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 mate waarin de parameters zijn ingevuld 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 • 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 • 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 visie en doelen voor de komende vijf jaar die in 2023 werden vastgesteld, zijn omgezet in gegevensbeschermingsbeleid. Het beleid geeft aan hoe deze doelen bereikt gaan worden waardoor de gemeente uiteindelijk haar visie kan verwezenlijken. Dit beleid zal worden vastgesteld in 2024 en vormt opnieuw een stap in privacy-volwassenheid: 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.

Steeds meer gemeenteambtenaren maken gebruik van ChatGPT. Het betreft hier is een chatbot die gebruikmaakt van kunstmatige intelligentie om uitgebreide antwoorden te geven op open vragen. Het model is getraind met data verzameld van het internet en gebruikersvragen. Het is belangrijk om in het gebruik hiervan persoonsgegevens te beschermen vanwege de gevoelige informatie die in gebruikersvragen kan voorkomen. Naast privacyrisico's zijn er andere gevaren, zoals het risico op manipulatie en misbruik, waarbij het model mogelijk ongepaste of beledigende inhoud kan genereren. Ook kan het soms onnauwkeurige of misleidende informatie verstrekken, wat kan bijdragen aan desinformatie.

De gemeente Nieuwkoop is bezig met het ontwikkelen van beleid voor het gebruik van ChatGPT of andere kunstmatige intelligentie-ontwikkelingen. Dit is nodig omdat anders het gevaar ontstaat dat het gebruik van dergelijke technologieën onbedoeld wordt geïntroduceerd met mogelijk onvoorziene gevolgen. Het is daarom raadzaam om beleid te ontwikkelen dat aangeeft wanneer en waarom kunstmatige intelligentie kan worden toegepast, met aandacht voor de daaraan verbonden risico's. Dit beleid zou ook ethische kwesties moeten behandelen, zoals verantwoordelijkheid voor de gegenereerde inhoud en de invloed op menselijke interacties.

Advies: Stel gegevensbeschermingsbeleid vast en voer dit beleid uit. Bij voorkeur worden hier zo veel mogelijk stakeholders bij betrokken. Indien externe factoren impact hebben op

het beleid, onderzoek dan of de doelen en eventueel de visie bijgesteld moeten worden. Stel 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 volledig doordrongen van de verantwoordelijkheden op dit gebied. Hier bestaan ook raakvlakken met het onderwerp privacy-bewustzijn. De governance moet betekenis krijgen bij de medewerkers die hier elk een eigen taak en verantwoordelijkheid hebben. Zo moeten bijvoorbeeld medewerkers een datalek kunnen herkennen en op de juiste wijze melden en horen proceseigenaren te weten wanneer een DPIA uitgevoerd moet worden. Het vergroten van het privacy-bewustzijn speelt hierbij een belangrijke rol.

Advies: Zorg dat de taken en verantwoordelijkheden betekenis krijgen binnen de gemeente en niet alleen woorden op papier zijn.

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 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. Uiteraard zou een fulltime medewerker zich vanzelfsprekend het best kunnen focussen op de werkzaamheden. De Ciso zal begin 2024 de organisatie verlaten. Deze functie was een combifunctie met een andere functie binnen I&A. De FG wil hierbij een lans breken voor een onafhankelijke en fulltime invulling voor de

toekomstige Ciso. Zo kan deze functionaris het best de toegewezen taken uitvoeren en het toezicht op de informatieveiligheid waarborgen.

Advies: Zet de goede werkzaamheden van het PIT voort. Breid de functie van privacy officer bij voorkeur uit tot een volledige fte. Stel in 2024 een nieuwe Ciso aan in een onafhankelijke rol.

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 wordt door de gemeente nagedacht hoe het proces Ondermijning zodanig in te richten dat de bescherming van persoonsgegevens op de juiste wijze gewaarborgd is. In 2023 was nog geen verbeterplan opgesteld.

In 2023 is een DPIA opgesteld door Burgerzaken voor het aanpassen van het identificeren van inwoners aan de balie. Hiertoe bestond de wens een applicatie aan te schaffen voor de verificatie van paspoorten waarbij tevens de mogelijkheid bestaat om aan de hand van gezichtsherkenning te kunnen verifiëren of de toonder van het paspoort tevens de houder is. De FG heeft een advies uitgebracht op deze DPIA: er is weliswaar een noodzaak tot het aanschaffen van een applicatie om paspoorten te kunnen verifiëren, echter er is geen zwaarwegend belang aanwezig dat de toepassing van biometrie rechtvaardigt.

Er stonden eind 2023 meerdere DPIA’s op de rol of werden reeds uitgevoerd. Deze zullen waarschijnlijk in 2024 hun beslag krijgen. Dit is een positieve ontwikkeling. Houd er wel rekening mee dat bij het vullen van het ISMS met verwerkingsactiviteiten ook aangegeven moet worden of er voor deze verwerkingen ook (nog) een DPIA uitgevoerd moet worden. Hier kan wellicht meer werk uit komen dan verwacht. Tijd en capaciteit moet dan wel voorhanden zijn.

Advies: Stel een verbeterplan op naar aanleiding van de uitkomsten van de DPIA Ondermijning en voer dat uit. Ga verder met het uitvoeren van de DPIA’s die op de rol staan. Houd rekening met extra werk dat voort kan komen uit het vullen van het ISMS.

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.

Ten behoeve van de informatievoorziening op het gebied van Beschermd Wonen zou het Regionale Team Maatschappelijke Zorg van de regio Holland Rijnland persoonsgegevens verzamelen en verwerken met als resultaat het Dashboard Beschermd Wonen Holland Rijnland. Eén van de persoonsgegevens die men voor dit doel wilde verwerken was het Burgerservicenummer (BSN). Dit is een uniek persoonsnummer dat in de eerste plaats bedoeld is voor het contact tussen burgers en de overheid. In alle andere gevallen is het verwerken van BSN pas toegestaan als dat expliciet in een wet aangegeven wordt. In een overheidssituatie moet echter wel aangegeven worden dat het verwerken van het BSN noodzakelijk is voor het te bereiken doel. Aangezien in deze situatie geen sprake was van het uitvoeren van een wettelijk taak maar het genereren van bedrijfsinformatie, kon de noodzakelijkheid van het verwerken van het BSN niet worden aangetoond en was er geen sprake van een adequate doelbinding.

Advies: Ontwikkel een visie op datagedreven werken vóórdat databronnen gecombineerd gaan worden en persoonsgegevens gekoppeld. Ga prudent om met het verwerken van het Burgerservicenummer.

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 is volop bezig het inrichten van het Information Security Management Systeem (ISMS). Hoewel de FG veel vertrouwen in de effectiviteit van ISMS heeft, moet dit systeem wel goed gevuld worden. Het vullen van dit systeem kost tijd en menskracht. Omdat dit vaak conflicteert met de andere drukke werkzaamheden van het management, zal het belang van het ISMS goed duidelijk gemaakt moeten worden.

Om het ISMS effectief toe te kunnen passen, zijn een breed draagvlak en commitment bij het management belangrijk. Managers moeten daartoe het belang van het systeem gaan inzien.

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: Om te kunnen voldoen aan de eisen uit de BIO is een Informatiebeveiligingsbeleid 2020-2024 opgesteld. In het Jaarplan I&A 2023 werden op het gebied van Informatieveiligheid een aantal projecten opgenomen om uit te voeren in 2023. Hiervan zijn de projecten *Onderzoek omvang en diepgang business continutiteitsplan*, *Back-up en herstelbeleid* en *Encryptiebeleid* echter in 2023 niet gestart. Het project *ISMS inrichten en uitrollen* heeft de status Voltooid, echter het ISMS-onderdeel register van verwerkings-activiteiten is pas gedeeltelijk gevuld.

Advies: Voer de nog niet gestarte projecten uit het Jaarplan I&A 2023 alsnog uit om zo passende waarborgen voor de beveiliging van persoonsgegevens te kunnen treffen. Zorg dat het register van verwerkingsactiviteiten in 2024 volledig gevuld wordt.

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 verwerkingsverantwoordelijk is een dataleveringsovereenkomst gewenst.

Bevinding: Er is een register van verwerkersovereenkomsten opgezet. Dit register is zeker niet compleet. Er is nog geen overzicht van samenwerkingsverbanden waaruit gezamenlijke verwerkingsverantwoordelijkheid uit voortvloeit. Ook is nog niet duidelijk of er partijen zijn met wie dataleveringsovereenkomsten gesloten moeten worden.

Advies: Ga na welke overeenkomsten nog gesloten moeten worden. Maak het register met verwerkersovereenkomsten compleet en voeg ook onderlinge regelingen en gegevensleveringsovereenkomsten toe. Neem dit register op in het ISMS.

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: In 2022 is een externe audit uitgevoerd naar de verwerkingen van persoonsgegevens die vallen onder de Wet politiegegevens. Onduidelijk is wat de stand van zaken is van het verbeteren van de tekortkomingen in de bescherming van deze persoonsgegevens. Op korte termijn zal een tweede EDP-audit uitgevoerd moeten worden door een externe auditor, zoals aangegeven is in het auditrapport van Baker Tilly.

Advies: Stel zo snel mogelijk een verbeterplan op naar aanleiding van de resultaten van de Wpg-audit en voer dit plan uit. Wijs als één van de eerste maatregelen een Wpg-FG aan.

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 2023 geen verzoeken binnengekomen tot inzage, rectificatie of wissen van persoonsgegevens. 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 Excelbestand waarin voor 2023 twaalf datalekken geregistreerd zijn. In verband met het risico voor de rechten en vrijheden van een betrokkene, zijn vijf datalekken gemeld aan de Autoriteit Persoonsgegevens en één van deze vijf aan de betrokkene zelf omdat er sprake was van gevoelige en strafrechtelijke persoonsgegevens. Hiermee zijn zowel intern als extern richting de Autoriteit Persoonsgegevens en betrokkene afdoende stappen genomen.

De Procedure melding datalekken functioneert goed. Het datalek wordt door de ontdekker/veroorzaker gemeld in Topdesk. De privacy officer en de FG krijgen hier automatisch ook een melding van. Naast de registratie in Topdesk worden de datalekken ook opgenomen in het Register Datalekken waarin tevens de opvolging en eventuele maatregelen geregistreerd worden.

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: Er zijn in 2023 zeven bewustwordingssessies gehouden bij diverse teams. Voor 2024 zijn staan ook weer verschillende bijeenkomsten gepland. Omdat alle medewerkers over een minimale basiskennis van gegevensbescherming moeten kunnen beschikken, is op het gebied van privacy-bewustzijn permanent onderhoud nodig. Daarnaast is het aan te raden maatwerktrainingen uit te voeren voor afdelingen of medewerkers die vaak met gevoelige en bijzondere persoonsgegevens werken.

Advies: Er is in 2023 behoorlijk meer aandacht besteed aan het vergroten van het privacy-bewustzijn: houd deze goede ontwikkeling gaande. 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 laten zien in 2023 goed op weg te zijn richting een basis privacy volwassenheidsniveau. De visie op gegevensbescherming is omgezet in gegevensbeschermingsbeleid voor de komende vijf jaar. De privacy governance begint langzaamaan nu ook voor de medewerkers betekenis te krijgen. Het inrichten en compleet maken van het register van verwerkingsactiviteiten in het ISMS is gestart en zal in 2024 doorgang vinden. Het uitvoeren van DPIA's kwam in 2023 goed op stoom. Hetzelfde geldt voor het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie.

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	
		2022	2023	2022	2023
4.1	Visie, doelen en beleid	Basis	Basis	Hoog	Hoog
4.2	Governance	Basis	Basis	Hoog	Hoog
4.3	Mensen en Middelen	Basis	Basis	Midden	Midden
4.4	Risicomanagement	Initieel	**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	Midden
4.13	Bewustzijn	Initieel	**BASIS**	Hoog	Hoog

6. Aanbevelingen

De belangrijkste aanbevelingen zijn afgestemd op de parameters die zich in de fasen *Initieel* en *Basis* bevinden en waarbij de prioriteit *Hoog* is. Uiteraard is het raadzaam ook de andere adviezen in dit FG-Jaarverslag op te volgen.

1. 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.
2. Zorg dat de privacy governance bij alle medewerkers betekenis krijgt.
3. Rond het invullen van het register van verwerkingsactiviteiten in het ISMS af in 2024.
4. Ga door met dit tempo van uitvoeren van DPIA's. Zorg ervoor dat managers gaan inzien dat zij daarin een belang hebben.
5. Blijf het privacy-bewustzijn te bevorderen. Maak presentaties gericht op specifieke groepen.