FG-JAARVERSLAG 2022

Gemeente Nieuwkoop

Functionaris gegevensbescherming mr. R.R. de Vries, 8 Februari 2023

FG-Jaarverslag 2022 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 in 2022 weer stappen gezet richting een basis privacy volwassenheidsniveau. Er is een visie op gegevensbescherming opgesteld. De gemeente kan nu een volgende stap maken door de visie en de daarbij geformuleerde doelen om te zetten in een effectief gegevensbeschermingsbeleid voor de komende vijf jaar.

De gemeente heeft een applicatie tot zijn beschikking om het register van verwerkingsactiviteiten in te kunnen zetten als een effectief instrument om de bescherming van persoonsgegevens te verbeteren. Deze applicatie zal daartoe wel eerst goed ingericht moeten worden. Dit zal een effectief implementatieplan en commitment van het management vergen.

Het uitvoeren van Data Protection Impact Assessments moet een vanzelfsprekendheid worden zodra er bij het verwerken van persoonsgegevens mogelijk sprake is van een hoog risico. Deze vanzelfsprekendheid kan onder meer ontstaan na het betekenis krijgen van de privacy governance binnen de gemeente. Ook het verbeteren van het privacybewustzijn kan daar een grote bijdrage aan leveren. Het verhogen van het privacy-bewustzijn stond echter in 2022 op een laag pitje en zal het volgende jaar weer met hernieuwde energie opgepakt moeten worden.

.

.

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 FG heeft een Baseline Bescherming Persoonsgegevens opgesteld waarin de eisen van de AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) vertaald zijn naar concrete, hanteerbare normen (parameters) die duidelijk maken wat de gemeente Nieuwkoop moet doen om in overeenstemming met de wet de bescherming van persoonsgegevens van de betrokkenen te waarborgen. Door het toepassen van de parameters uit deze Baseline kan de gemeente tevens aantonen dat passende maatregelen voor het waarborgen van de bescherming van persoonsgegevens worden getroffen.

Op basis van de mate van invulling van de parameters toetst de FG in hoeverre de gemeente Nieuwkoop passende maatregelen treft om te waarborgen en aan te tonen dat de verwerkingen van persoonsgegevens in overeenstemming met de AVG worden uitgevoerd.

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 redelijk om (onmiddellijk) van de gemeente Nieuwkoop een volmaakte naleving van de eisen uit de AVG te verwachten. Wellicht is deze toestand ook onbereikbaar. Dit ontslaat de gemeente echter niet van de verplichting te streven naar continue verbetering. De parameters moeten daarom ook worden gezien als de bouwstenen van een groeimodel, waarbinnen de gemeente zelf haar ambitie en volwassenheidsniveau kan bepalen.

Binnen dit groeimodel 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: Het duidelijk voor ogen hebben van een visie op de bescherming van persoonsgegevens is essentieel voor de inbedding, vooruitgang en ontwikkeling hiervan. Een visie geeft richting en verwoordt de ambitie van de gemeente op het gebied van de bescherming van persoonsgegevens. Uit de ontwikkelde visie worden de doelen afgeleid. Het bereiken van deze doelen leidt tot het realiseren van de visie. De doelen moeten specifiek, meetbaar, aanvaardbaar, realistisch en tijdgebonden omschreven worden. Het gegevensbeschermingsbeleid geeft aan op welke wijze voldaan wordt aan de van toepassing zijnde wet- en regelgeving. Input voor het gegevensbeschermingsbeleid zijn ook de doelen die de gemeente zichzelf gesteld heeft.

Bevindingen: In samenwerking met de gemeenten Alphen aan den Rijn, Kaag en Braassem en Waddinxveen is in 2022 gewerkt aan het afronden van een visie op gegevensbescherming voor de komende vijf jaar. Bij deze visie zijn doelen opgesteld. Door het behalen van deze doelen kan de gemeente uiteindelijk deze visie verwezenlijken. Dit is weer een stap in privacy-volwassenheid: de gemeente komt dan uit de positie waarin zij reactief de aanbevelingen van de FG opvolgt naar een situatie waarin zij nu zelf in control is bij het verbeteren van de bescherming van persoonsgegevens. Hiermee is uitvoering gegeven aan het advies uit het FG-Jaarverslag 2021 (4.1).

Advies: Stel de visie vast. Plaats de doelen in de tijd en zet deze om in gegevensbeschermingsbeleid en voer dit beleid uit. Betrek bij voorkeur hier zo veel mogelijk stakeholders bij. Indien externe factoren impact hebben op het beleid, onderzoek dan of de doelen en eventueel de visie bijgesteld moeten worden.

4.2 Governance

Context: Het waarborgen van de bescherming van persoonsgegevens ligt niet alleen bij de privacy-officer. Meerdere personen binnen de gemeente zijn in meer of mindere mate betrokken om aan de vereisten van wet- en regelgeving te kunnen voldoen. Een heldere verdeling van taken en bevoegdheden en duidelijke rapportagelijnen zorgen ervoor dat op een juiste wijze invulling wordt gegeven aan de eisen van het gegevensbeschermingsbeleid en de AVG.

Bevindingen: In 2022 is een nieuw governance document opgesteld met daarin een verdeling van taken, verantwoordelijkheden en rapportagelijnen met betrekking tot gegevensbescherming. Hiermee is uitvoering gegeven aan het advies uit het FG-Jaarverslag 2021 (4.2). Echter, alleen een document is niet voldoende om de bescherming van persoonsgegevens effectief te beleggen. De governance zal ook betekenis moeten krijgen bij

de medewerkers die hier een taak hebben. Het vergroten van het privacy-bewustzijn speelt hierbij een grote 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: De bescherming van persoonsgegevens legt beslag op de tijd van de medewerkers en middelen van de gemeente. Dit kan zijn door extra inzet van medewerkers, het inschakelen van externe expertise of de aanschaf van bepaalde applicaties of systemen. Op basis van de governance-afspraken worden keuzes gemaakt in het toewijzen van de beschikbare schaarse middelen om de gewenste resultaten te behalen.

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.

Met het aantreden van een nieuwe privacy-officer is het aantal uren dat deze kan besteden aan gegevensbescherming in 2022 uitgebreid naar 24 uur per week, naast andere taken. Hoewel idealiter een fulltime medewerker zich het best kan focussen op de werkzaamheden, is dit zeker een positieve ontwikkeling: het belang van de bescherming van persoonsgegevens wordt hiermee onderkend.

Advies: Zet de goede werkzaamheden van het PIT voort. Breid de functie van privacy officer bij voorkeur uit tot een volledige fte.

4.4 Risicomanagement

Context: Het managen van risico's is een continu proces dat de risico's op het gebied van gegevensbescherming inventariseert, beoordeelt en een passende aanpak daarvan bewaakt. Risicomanagement richt zich op het beheersen van risico's bij het verwerken, waaronder verzamelen, opslaan en doorgeven van persoonsgegevens. Door middel van het toepassen van *Privacy by design* en het uitvoeren van DPIA's worden bij de ontwikkeling, de inrichting en de inzet van verwerkingen van persoonsgegevens de risico's in kaart gebracht en zoveel mogelijk beperkt dan wel weggenomen.

Bevindingen: Reeds in het FG-Jaarverslag 2020 heeft de FG heeft de gemeente Nieuwkoop geadviseerd het in gebruik nemen van Djuma aan te grijpen om een DPIA uit te voeren naar de meest risicovolle (hoog risico) verwerkingen van persoonsgegevens. Deze DPIA's hebben in 2022 niet plaatsgevonden. Bij één van de belangrijkste applicaties voor de gemeentelijke dienstverlening is het zaak dat risico's met betrekking tot de inrichting geïdentificeerd worden waarna beheersmaatregelen getroffen kunnen worden.

Eind december 2022 is de DPIA met betrekking tot verwerkingen van persoonsgegevens in het kader van het tegengaan van ondermijning opgeleverd. Deze DPIA is uitgevoerd door een externe partij. De FG was in eerste instantie goed betrokken bij het bepalen van de scope van de uitvoering, maar deze is later zonder medeweten van de FG gewijzigd. De implicaties daarvan zullen mogelijk later blijken zodra de FG zijn advies op de DPIA geschreven heeft.

Er wordt nog steeds onvoldoende eigenaarschap gevoeld wordt bij procesverantwoordelijken ten aanzien van het initiëren en uitvoeren van DPIA's. Dit kan liggen aan het gebrek aan kennis met betrekking tot de verplichtingen die voortvloeien uit de AVG. Eigenaarschap bij het management wordt ook verkregen door het inregelen van de juiste governance. Managers moeten een DPIA niet als een straf of extra werk ervaren maar als essentiële voorbereiding die problemen (lees: datalekken) in de toekomst voorkomt.

Advies: Voer alsnog DPIA's uit naar (hoog risico) verwerkingsactiviteiten in Djuma. Verhoog het eigenaarschap bij procesverantwoordelijken zodat het vanzelfsprekend wordt dat bij nieuwe verwerkingen onderzocht wordt of een DPIA nodig is.

4.5 Doelbinding

Context: Een van de beginselen van de AVG is dat gegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doel. Het doel moet zijn bepaald alvorens de gemeente tot verwerken overgaat. 'Welbepaald' houdt in dat deze doelomschrijving duidelijk moet zijn en niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens wel of niet nodig zijn voor dat doel. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. 'Uitdrukkelijk omschreven' houdt in dat de gemeente het doel waarvoor de verwerking plaatsvindt, helder en duidelijk moet hebben omschreven. 'Gerechtvaardigd' betekent dat de verwerking alleen met een wettelijke grondslag mag plaatsvinden.

Bevindingen: Knelpunten op het gebied van veiligheid leiden ertoe dat steeds vaker samenwerkingsverbanden op grote schaal persoonsgegevens gaan delen, opslaan en analyseren. Voor de gemeente Nieuwkoop betreft dat onder andere samenwerkingsverbanden zoals het Zorg en Veiligheidshuis (ZVH) en het Regionaal Informatie- en Expertise Centrum (RIEC).

Het ZVH stuurt op samenwerking en regievoering op de aanpak van personen die overlast of criminaliteit veroorzaken en/of dringend zorg nodig hebben. Het RIEC richt zich op de bestrijding van ondermijnende criminaliteit. Hierbij worden informatie, expertise en krachten van de verschillende overheidsinstanties verbonden en vindt stimulering en ondersteuning plaats van publiek-private samenwerking bij de aanpak van ondermijning.

Deze samenwerkingsverbanden opereren vaak op basis van signalen van eerste vermoedens van onrechtmatige activiteiten waarna (bijzondere) persoonsgegevens gegevens met elkaar gedeeld en geanalyseerd worden. Het ontvangen, delen en analyseren van deze signalen zijn verwerkingen in de zin van de AVG.

Het doel van deze verwerkingen is veelal niet duidelijk genoeg omschreven hetgeen in strijd is met de AVG. Hier komt bij dat indien een doel niet of onvoldoende omschreven is, het lastig wordt de grondslag van de verwerking te bepalen. Hierdoor kunnen deze verwerkingen onrechtmatig zijn.

Advies: Voordat persoonsgegevens uitgewisseld gaan worden in samenwerkingsverbanden moeten de doeleinden van de verwerkingen van de persoonsgegevens concreet bepaald zijn en duidelijk omschreven.

4.6 Register van verwerkingsactiviteiten

Context: Om de naleving van de AVG aan te kunnen tonen dient de gemeente een register bij te houden van verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden. Deze vastlegging maakt duidelijk hoe de verschillende organisatieonderdelen de werkprocessen ondersteunen en welke beveiligingsmaatregelen (op hoofdlijnen) zijn getroffen voor de verwerkingen en betrokkenen. Het register maakt tevens toezicht op de (rechtmatigheid van de) verwerkingsactiviteiten mogelijk alsmede het kunnen voldoen aan de rechten van betrokkenen.

Bevindingen: De gemeente Nieuwkoop is bij het inrichten van het Information Security Management Systeem (ISMS) gestuit op enkele personele hobbels. Hierdoor heeft het opzetten van het register van verwerkingsactiviteiten in het ISMS vertraging opgelopen. De FG heeft echter nog veel vertrouwen in de effectiviteit van ISMS en de nieuwe privacy officer die vanaf 1 november 2022 met de werkzaamheden belast is.

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. Dit gaat niet vanzelf.

Advies: Zorg voor een goed plan van aanpak om het nieuwe ISMS te implementeren en om draagvlak te krijgen bij de toekomstige gebruikers.

4.7 Beveiliging

Context: De gemeente is gehouden technische en organisatorische maatregelen te treffen voor de verwerking van persoonsgegevens op een passend beveiligingsniveau. Deze beveiligingsmaatregelen zijn bedoeld om persoonsgegevens te beschermen tegen onbevoegde of onopzettelijke openbaring van, toegang tot, vernietiging van, verlies van

toegang tot en wijziging van persoonsgegevens en enige andere vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.

Bevindingen: Om te kunnen voldoen aan de eisen uit de BIO is een Informatiebeveiligingsbeleid 2020-2024 en een Uitvoeringsplan Informatiebeveiligingsbeleid 2020-2022 opgesteld. In 2022 is een vervolg gegeven aan het uitvoeringsplan van het informatiebeveiligingsbeleid 2020-2022. Helaas is het niet gelukt alle projecten in 2022 volledig te realiseren. De belangrijkste oorzaken hiervoor zijn dat het uitvoeringsplan erg ambitieus en de planning te optimistisch is. De CISO is in het laatste kwartaal van 2022 wegens gezondheidsredenen uitgevallen waardoor een aantal werkzaamheden nog niet zijn uitgevoerd.

Na de constatering van de FG eind 2021 dat in bepaalde gevallen ongeoorloofde toegang tot persoonsgegevens in Djuma mogelijk was, heeft de gemeente in 2022 een probleemanalyse van de ongeoorloofde toegang gemaakt. Op basis van deze analyse is een actieplan opgesteld om deze ongeoorloofde toegang te voorkomen dan wel te beperken. Hiertoe zijn onder andere de uitgangspunten voor de inrichting van vertrouwelijkheden aangescherpt, zaaktypen met bijzondere persoonsgegevens waar nodig verder afgeschermd, zijn met terugwerkende kracht bestaande zaaktypen afgeschermd conform de nieuwe vertrouwelijkheidsinstellingen en is een extra check ingevoerd van de privacy officer bij de creatie van nieuwe zaaktypen.

Uit dit actieplan is ook op te maken dat betrokkenen zich realiseren dat in het zaaksysteem de menselijke factor de zwakste schakel is: de betrokken teams hebben extra uitleg gekregen over het gebruik van vertrouwelijkheden en voor nieuwe medewerkers is een Djuma training verplicht.

Advies: Voer de nog niet uitgevoerde acties uit het uitvoeringsplan Informatiebeveiligingsbeleid 2020-2022 alsnog uit om zo passende waarborgen voor de beveiliging van persoonsgegevens te kunnen treffen. Stel ook een nieuwe uitvoeringsplan op voor de komende periode. Rond het actieplan voor Djuma verder af in 2023 en blijf de bescherming van persoonsgegevens binnen dit zaaksysteem monitoren.

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. Dat is nu niet het geval. Niet

volstaan kan worden met “wettelijke bewaartermijn” of “zolang nodig is voor het doel van de verwerking”.

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: Zoals vereist krachtens de Wet Politiegegevens (Wpg) heeft de gemeente vóór het einde van 2022 een extern audit naar de verwerkingen van politiegegevens (persoonsgegevens die gegenereerd worden in het kader van uitvoering van de politietaken door de boa’s) uit laten voeren. Het rapport was vóór 1 januari 2023 nog niet aan de Autoriteit Persoonsgegevens toegezonden. Eén van de conclusies uit dit rapport is dat er een

FG is aangesteld die toezicht houdt op het naleven van de Wpg. Dit is echter niet correct. Een aparte Wpg-FG moet nog aangewezen worden. Dit kan ook de huidige (AVG-)FG zijn.

Advies: Stel binnen drie maanden een verbeterplan op naar aanleiding van de resultaten van de Wpg-audit. Wijs 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. Deze transparantie is nodig om de betrokkene of diens wettelijke vertegenwoordiger in staat te stellen zonder onevenredige kosten en/of moeite zijn gegevens te laten corrigeren, te wissen of de gemeente aan te spreken op de onrechtmatige verwerking van persoonsgegevens.

Bevindingen: Er zijn in 2022 geen verzoeken binnengekomen tot inzage, rectificatie of wissen van persoonsgegevens. Toegang tot uitoefening van rechten van betrokkenen is weliswaar digitaal geregeld door middel van DigiD, het vergt wel enig zoeken op de website om deze ingang te vinden.

Advies: Maak de gemeentelijke website toegankelijker voor het doen van verzoeken tot inzage, rectificatie en wissen van persoonsgegevens.

4.12 Datalekken

Context: Het adequaat reageren op een datalek kan mogelijk nadelige gevolgen voor de betrokkenen voorkomen dan wel beperken. Daarnaast kan hier van geleerd worden zodat een dergelijk datalek niet meer voorkomt. Datalekken moeten altijd gemeld worden aan de privacy-officer en bij een (hoog) risico aan de Autoriteit Persoonsgegevens en de betrokkene.

Bevindingen: De gemeente Nieuwkoop beschikt over een register datalekken. Het betreft hier een Excelbestand waarin voor 2022 vijf datalekken geregistreerd zijn. In verband met het risico voor de rechten en vrijheden van een betrokkene, is één datalek zowel gemeld aan de Autoriteit Persoonsgegevens als aan de betrokkene. De manager van de afdeling waar het datalek plaatsvond heeft vervolgens afdoende intern en richting betrokkene maatregelen genomen.

De Procedure melding datalekken is geactualiseerd en aangepast: een medewerker die een mogelijk datalek constateert, kan dit nu melden 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 begrip van en voor de bescherming van persoonsgegevens hebben. Daarom is het van groot belang dat medewerkers niet alleen door middel van allerlei vormen van voorlichting en educatie de basisprincipes van de AVG leren kennen, maar ook dat hiermee begrip en draagvlak voor de bescherming van persoonsgegevens gecreëerd wordt. Op het gebied van de bescherming van persoonsgegevens is privacy bewustzijn vaak de achilleshiel van een organisatie. Een organisatie kan haar processen en verwerkingen nog zo beveiligd, geregistreerd en ingericht hebben met procedures en protocollen, als medewerkers zich niet bewust zijn van de implicaties en verantwoordelijkheden van gegevensbescherming, zullen de maatregelen die de gemeente neemt, onvoldoende effect sorteren.

Bevindingen: In 2022 is met de communicatieadviseur een Communicatiekalender Informatiebeveiliging en privacy opgesteld. Hierin staat opgenomen welke voorlichtingsactiviteiten in 2022 hebben plaatsgevonden. In tegenstelling tot het vorige jaar beperkten de activiteiten zich tot het plaatsen van berichten over gegevensbescherming op het intranet. Er hebben geen bijeenkomsten of trainingen plaatsgevonden.

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 moet in 2023 echt meer aandacht besteed worden aan het vergroten van het privacy-bewustzijn. Zet daarom een cyclus van voorlichtingsbijeenkomsten op om het draagvlak voor en de kennis van de AVG te vergroten.

5. Conclusies

De gemeente Nieuwkoop heeft in 2022 weer stappen gezet richting een basis privacy volwassenheidsniveau. Er is een visie op gegevensbescherming opgesteld. De gemeente kan nu een volgende stap maken door de visie en de daarbij geformuleerde doelen om te zetten in een effectief gegevensbeschermingsbeleid voor de komende vijf jaar.

De nieuwe privacy governance staat nu op papier maar zal nu ook in de werkprocessen betekenis moeten krijgen. Het inrichten en compleet maken van het register van verwerkingsactiviteiten moet doorgang blijven vinden. Er moet veel meer vaart gezet worden achter het uitvoeren van DPIA's. Het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie moet in 2023 echt 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	
		2021	2022	2021	2022
4.1	Visie, doelen en beleid	Initieel	**BASIS**	Hoog	Hoog
4.2	Governance	Initieel	**BASIS**	Hoog	Hoog
4.3	Mensen en Middelen	Basis	Basis	Midden	Midden
4.4	Risicomanagement	Initieel	Initieel	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	Initieel	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 de visie op gegevensbescherming en de doelen vast. Neem deze doelen op in gegevensbeschermingsbeleid voor de periode 2023-2028.
2. Zorg dat de nieuwe privacy governance ook betekenis krijgt.
3. Maak van het Information Securtity Management System een dynamisch instrument voor de bescherming van persoonsgegevens. Richt het daarom zorgvuldig in.
4. Schroef het tempo van uitvoeren van DPIA's op. Zorg ervoor dat managers gaan inzien dat zij daarin een belang hebben.
5. Zet een cyclus van trainingen en bijeenkomsten op om het privacy-bewustzijn te bevorderen.