FG-JAARVERSLAG 2024

Gemeente Kaag en Braassem

Functionaris gegevensbescherming mr. R.R. de Vries, 27 januari 2025

FG-Jaarverslag 2024 Kaag en Braassem

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 getroffen heeft om te kunnen waarborgen en aantonen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met de Algemene Verordening Gegevensbescherming (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 Kaag en Braassem heeft in 2024 wederom het basis privacy volwassenheidsniveau verder bestendigd en neemt derhalve passende maatregelen om de bescherming van persoonsgegevens te waarborgen.

Het gegevensbeschermingsbeleid is opgesteld maar moet nog worden vastgesteld. De gemeente kan dan de volgende stap maken door dit gegevensbeschermingsbeleid de komende vijf jaar dan ook uit te gaan voeren. Het onderhouden van het register van verwerkingsactiviteiten is nog steeds een klus voor de privacy officer. Een vervolgstap zou moeten zijn het aanschaffen van een applicatie waardoor de proceseigenaren zelf de verwerkingen van persoonsgegevens actueel kunnen houden. Het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie moet voortgang blijven vinden. Er waren in 2024 meerdere Data Protection Impact Assessments (DPIA's) in uitvoering maar de vaart moet er wel in blijven. Ook het daadwerkelijk uitvoeren van de hieruit voorkomende beheersmaatregelen verdient aandacht.

2. Inleiding

2.1 Achtergrond

De gemeente Kaag en Braassem dient op grond van artikel 24 AVG passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met deze verordening. Eén van deze maatregelen is de aanwijzing van een functionaris gegevensbescherming (FG). De FG is een onafhankelijke toezichthouder. 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 Kaag en Braassem voldoet aan haar verplichtingen die voortvloeien uit de AVG, heeft de FG door middel van interviews, gesprekken, documentatiestudie, het bijwonen van overleggen en adviseren bij Data Protection Impact Assessments een beeld kunnen vormen van de stand van zaken van de gegevensbescherming. Leidraad bij het beoordelen van de bevindingen is de door de FG in 2020 opgestelde Baseline Bescherming Persoonsgegevens.

Elke drie maanden zendt de FG een memo aan de gemeentesecretaris met de laatste stand van zaken zodat de ambtelijke organisatie beter kan inspelen op ontwikkelingen en eventueel kan bijsturen. 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 Kaag en Braassem aantonen dat passende maatregelen zijn genomen om de bescherming van persoonsgegevens te waarborgen. De FG beoordeelt dan in hoeverre de gemeente Kaag en Braassem passende maatregelen neemt. Per parameter wordt eerst aangegeven binnen welke context de wettelijke eisen gezien moeten worden. Aansluitend worden de bevindingen 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 Kaag en Braassem. 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 Kaag en Braassem 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 2022 werden vastgesteld, zijn omgezet in een concept-gegevensbeschermingsbeleid voor de periode 2023-2027. Het beleid was in 2024 nog niet vastgesteld.

In juni 2024 zijn de richtlijnen voor het gebruik van Artificiële Intelligentie (AI) toepassingen vastgesteld. In deze richtlijnen staan de do's en dont's risico's van het gebruik van AI. Afgeraden wordt gebruik te maken van ChatGPT en Co-pilot van Microsoft te gebruiken. Er is echter nog geen document waaruit een visie op het gebruik van AI toepassingen door de gemeente Kaag en Braassem blijkt voor de toekomst. Wel is duidelijk dat de gemeente zich bewust is van de gevaren die de toepassing van AI met zich meebrengt.

Advies: Stel het gegevensbeschermingsbeleid vast en voer dit beleid uit. Indien externe factoren impact hebben op het beleid, onderzoek dan of de doelen en eventueel de visie bijgesteld moeten worden. Stel een visie op voor het gebruik van AI indien de gemeente in de toekomst van deze technologieën gebruik wil maken. Begin dan in het klein met experimenteren.

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: De taken, bevoegdheden en rapportagelijnen zijn schriftelijk vastgelegd in een Privacy Governance document. Er is een cyber escaperoom georganiseerd voor het management waarna uitgebreid is gesproken over eigenaarschap binnen de organisatie, met specifieke aandacht voor de rol van de clustermanagers. Hierbij zijn onderwerpen aan bod

gekomen zoals het uitvoeren van DPIA's, het treffen van passende maatregelen, het opstellen van verwerkersovereenkomsten, het melden van datalekken en het stimuleren van deelname aan awareness-activiteiten. In de periode daarna is het bewustzijn bij het management is toegenomen. Dit valt onder andere af te leiden uit een hogere frequentie aan vragen over privacy en het stimuleren van medewerkers om aan de cyberbarometer mee te doen.

Advies: Blijf het eigenaarschap bij de verantwoordelijken 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 formatie voor privacy was in 2024 op sterkte: er is een interne privacy-officer. Het aantal uren dat de privacy-officer ter beschikking staat is 32 uur alsmede nog 4 uur voor informatiebeveiligingswerkzaamheden. De privacy officer werkt ook goed samen met de privacy officers van Nieuwkoop en Alphen aan den Rijn aangezien de gemeente Kaag en Braassem taken uitbesteed heeft aan Alphen aan den Rijn.

Advies: Zet voor zover er tijd overblijft de privacy-officer zo veel mogelijk in voor privacy-awareness bijeenkomsten. Zorg dat de privacy officer zich daarnaast ook kan blijven ontwikkelen.

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: Hoewel de DPIA Ondermijning reeds geruime tijd is afgerond, hebben de aanbevelingen nog geen opvolging gekregen. De DPIA Jeugdhulp is in 2024 opgeleverd maar de uitvoering van de daarin geadviseerde beheersmaatregelen is nog niet gestart. Ditzelfde

geldt voor de DPIA Bodycam. De DPIA SOZ Jeugdhulp van de Serviceorganisatie Zorg Holland Rijnland waarin Kaag en Braassem met andere gemeenten in participeert, vordert erg traag. De DPIA Bibob en DPIA Omgevingswet staan nog niet op de planning. Dat geldt wel voor de DPIA Datamask. De DPIA PGB Jeugd moet nog worden besproken met Informatiebeveiliging.

Advies: Probeer vaart te houden in het uitvoeren van de DPIA's, ook al is er afhankelijkheid van andere partijen. Zorg dat de voorgestelde beheersmaatregelen snel na oplevering van de DPIA en het FG-Advies daarop uitgevoerd worden en toon dit ook aan.

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 2023 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.

Advies: 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: Het register van verwerkingsactiviteiten wordt weer geactualiseerd. Zolang als de procesverantwoordelijken zelf (of hun medewerkers) het register niet bijhouden en/of aanvullen zal dit echter een periodieke exercitie van de privacy officer blijven. Een praktische oplossing hiervoor kan een applicatie zoals een Information Security Management System

zijn. Naast het managen en monitoren van de informatieveiligheidshuishouding kan met een dergelijke applicatie ook het register van datalekken, de DPIA's, het register van verwerkingsovereenkomsten en de verzoeken van betrokkenen bijgehouden worden.

Advies: Onderzoek samen met de Bedrijfsvoeringsorganisatie Rijn en Braassem (BVO) en de gemeente Alphen aan den Rijn de mogelijkheid van een applicatie voor het register van verwerkingsactiviteiten. Onderzoek ook of het wenselijk en mogelijk is om het register op de website te plaatsen.

4.7 Kwaliteitsmanagement

Context: Kwaliteitsmanagement zorgt ervoor dat processen worden ingezet om onjuiste of onnauwkeurige gegevens te corrigeren, ontbrekende gegevens aan te vullen, gegevens te verwijderen, de verwerking te beperken of toestemming voor verwerking in te trekken. Het verwerkingssysteem is zo ontworpen dat persoonsgegevens kunnen worden gecorrigeerd, stopgezet, beperkt of overgedragen. Als dit op verzoek van de betrokken persoon gebeurt, wordt die persoon op de hoogte gehouden van de status van de afhandeling.

Kwaliteitsmanagement wordt toegepast wanneer de gemeente effectieve procedures heeft om de rechten van betrokkenen, zoals het recht op inzage en rectificatie, correct te waarborgen. Dit is echter alleen een reactieve benadering. Een proactieve aanpak maakt ook deel uit van kwaliteitsmanagement, waarbij een systeem van regelmatige controles wordt opgezet om de juistheid, nauwkeurigheid, actualiteit, volledigheid en juiste gebruik van gegevens te waarborgen, en om te identificeren wie indien nodig persoonsgegevens moet corrigeren.

Bevindingen: Er bestaat nu geen systeem dat proactief de intrinsieke kwaliteit van persoonsgegevens bewaakt en/of verbetert. Daarnaast ontbreekt een systeem dat bewaakt of de in een gegevensbeschermingsbeleid gestelde doelen of acties in een jaarplan behaald worden. Successen zijn derhalve afhankelijk van individuele inzet en commitment.

De verantwoordelijkheid voor de implementatie van de beheersmaatregelen die voortkomen uit DPIA's, ligt in eerste instantie bij de procesverantwoordelijken (directeuren en clustermanagers). Het is echter aan te raden de voortgang van de uitvoering van de verbeterplannen centraal te monitoren. Bij onvoldoende voortgang kan dan actie ondernomen worden.

Advies: Onderzoek de mogelijkheden van een kwaliteitsmanagementsysteem van periodieke controles op de juistheid, nauwkeurigheid, actualiteit, volledigheid en correct gebruik van de gegevens. Ontwikkel en implementeer daarnaast een systeem dat het behalen van de doelen uit het gegevensbeschermingsbeleid en de uitvoering van de beheersmaatregelen uit het jaarplan bewaakt.

4.8 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: De CISO heeft een jaarverslag uitgebracht over 2024 met daarin de stand van zaken omtrent informatieveiligheid. In dit verslag worden ook enkele belangrijke aanbevelingen gedaan die de FG ook onderschrijft. Het betreft hier onder andere de onduidelijke positie in de organisatie en de inzetbaarheid van Informatieveiligheid en de CISO en de relatie met de BVO Rijn en Braassem. Hierdoor bestaan lacunes in het bewustzijn en kennis over risico's, incidenten, continuïteitsmaatregelen en beschikbaarheidseisen.

Op grond van artikel 32 AVG moet de gemeente passende technische en organisatorische maatregelen treffen om een beveiligingsniveau te waarborgen dat is afgestemd op het risico. Hierbij kan onder andere gedacht worden aan maatregelen om continu de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te waarborgen en het vermogen om in geval van een fysiek of technisch incident de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te herstellen.

Voor zover de FG kan zien is er nog geen plan opgesteld hoe om te gaan met een cybercrisis en welke maatregelen vooraf genomen kunnen worden om een dergelijke crisis te voorkomen alsook maatregelen die de ongewenste gevolgen kunnen verzachten. Daarnaast is er nog geen continuïteitsplan opgesteld voor het geval een dergelijke crisis plaatsvindt.

Advies: Probeer de positie van Informatieveiligheid in het algemeen en die van de CISO in het bijzonder te versterken. Ga verder met het voorbereiden van de organisatie en het bestuur op een mogelijk groot beveiligingsincident. Oefen cybercrises aan de hand van scenario's.

4.9 Informatieverstrekking

Context: Inwoners en andere betrokkenen die persoonsgegevens aan de gemeente verstrekken, hebben het recht om te weten voor welke doeleinden, op welke manier en door wie deze gegevens worden gebruikt. De gemeente heeft daarom een informatieplicht. Deze informatieplicht geldt ook wanneer de gemeente persoonsgegevens van anderen ontvangt.

Bevindingen: Bij het voorkomen dan wel tegengaan van ondermijnende activiteiten, zullen persoonsgegevens worden verzameld. Hoewel vanuit het perspectief van deze werkzaamheden het wellicht onwenselijk is dat betrokkenen vooraf op de hoogte gesteld worden van de voorgenomen verwerkingen van persoonsgegevens, zal de gemeente door te

verzuimen transparantie te bieden, niet kunnen verantwoorden en aantonen dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking.

Hierbij geldt dat het verstrekken van informatie des te belangrijker is omdat hier ook bijzondere en gevoelige persoonsgegevens kunnen worden verwerkt alsmede persoonsgegevens van strafrechtelijke aard.

Advies: Verstrek bij nieuwe verwerkingen vooraf informatie over de verkrijging en verzameling van persoonsgegevens om transparantie aan betrokkene te garanderen over de gegevensverzameling en de verwerking, zodat de betrokkene zijn rechten kan uitoefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking.

4.10 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: Volgens de AVG dient de gemeente indien mogelijk de bewaartermijnen in het register op te nemen. Er wordt nog groot onderhoud gepleegd op het register. Dit is een uitgelezen mogelijkheid om ook alle bewaartermijnen op te nemen in het register. Bij een eigen bewaartermijn dient een motivering van de duur van de termijn opgenomen te worden.

Advies: Zorg dat alle bewaartermijnen opgenomen zijn in het register van verwerkingsactiviteiten.

4.11 Doorgifte

Context: Persoonsgegevens kunnen op drie manieren worden gedeeld met externe partijen. Allereerst gebeurt dit met partijen die in opdracht van de gemeente werkzaamheden uitvoeren waarbij persoonsgegevens worden verwerkt. In deze situatie is de gemeente de verwerkingsverantwoordelijke en de externe partij de verwerker. Het is dan vereist om een verwerkersovereenkomst af te sluiten. Daarnaast deelt de gemeente persoonsgegevens in situaties waarbij meerdere verwerkingsverantwoordelijken gezamenlijk de doelen en middelen voor de verwerking bepalen. In dit geval zijn ze gezamenlijk verwerkingsverantwoordelijk en moet er een onderlinge regeling worden getroffen. Als de gemeente persoonsgegevens doorgeeft aan een andere verwerkingsverantwoordelijke, is het raadzaam een dataleveringsovereenkomst af te sluiten.

Het is belangrijk dat het opstellen, beoordelen en aanpassen van de bovengenoemde overeenkomsten onderdeel is van het contractmanagement. Hiermee wordt voorkomen dat bij gewijzigde omstandigheden aanpassing van de overeenkomsten niet vergeten wordt. Periodiek kan dan ook bijgehouden worden of de overeenkomsten nog voldoen aan de eisen.

Bevinding: De verwerkersovereenkomsten zijn opgenomen in het zaaksysteem. Idealiter zouden verwerkersovereenkomsten gekoppeld moeten zijn aan de onderliggende hoofdovereenkomsten (contracten). Door middel van een contractmanagementsysteem kunnen dan ook de verwerkersovereenkomsten gemonitord en actueel gehouden worden.

Advies: Maak het register van verwerkersovereenkomsten compleet, houd het actueel en voeg ook de onderlinge regelingen en dataleveringsovereenkomsten toe. Dit register dient bij voorkeur opgenomen te worden in de eerder geadviseerde applicatie of in een contractmanagementsysteem.

4.12 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.

Het driemaandelijkse memo van de FG helpt de organisatie om tijdig bij te sturen zodat er geen verassingen in het FG-Jaarverslag opdoemen.

Advies: Blijf nota nemen van de driemaandelijkse memo's om tijdig bij te sturen en om niet voor verassingen te komen staan bij ontvangst van het FG-Jaarverslag.

4.13 Rechten betrokkenen

Context: Iedere betrokkene wiens persoonsgegevens door de gemeente Kaag en Braassem 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: Een verzoek om inzage kan digitaal worden ingediend waarbij identificatie plaatsvindt door middel van Digid. Volgens het zaaksysteem is in 2024 slechts één verzoek om inzage in persoonsgegevens ingediend op grond van artikel 15 AVG. De verzoeker was geen bekende van gemeente. Er zijn verder geen gegevens van de verzoeker verwerkt.

Advies: Zonder een actueel en compleet register van verwerkingsactiviteiten is het vrijwel ondoenlijk om volledig te kunnen achterhalen binnen welke gemeentelijke processen persoonsgegevens van een betrokkene worden verwerkt. Houd daarom dit register altijd zo compleet en actueel mogelijk.

4.14 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: In 2024 zijn zeventien datalekken opgenomen in het datalekkenregister. Hiervan zijn twee datalekken op juiste gronden gemeld bij de Autoriteit persoonsgegevens. Eén van deze twee datalekken is ook gemeld aan de betrokkene. De andere datalekken vormden geen risico voor de rechten en vrijheden van betrokkenen.

Advies: Neem bij voorkeur het register van datalekken op in de applicatie die geadviseerd wordt voor het register van verwerkingsactiviteiten. Blijf datalekken monitoren en evalueren om te voorkomen dat dezelfde fouten gemaakt worden, ook al is er geen of weinig risico aan verbonden.

4.15 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: In samenwerking met de gemeente Alphen aan den Rijn is voor de periode 2023-2025 een externe partij ingehuurd om een awareness programma te verzorgen. Dit programma gaat over zowel informatieveiligheid als privacy. Net als over 2023 heeft deze partij over 2024 een rapportage uitgebracht waaruit zou blijken dat de gemeenten Alphen aan den Rijn en Kaag en Braassem een sterke groei hebben doorgemaakt op de onderwerpen Werken vanuit huis, Gegevens bewaren en Veilige meldcultuur. Op drie andere onderwerpen zijn risico's te ontwaren: Overweeg alvorens te handelen, Veilige applicaties gebruiken en Actie ondernemen. Net als de vorige rapportage is die over 2024 niet gesplitst per

gemeentelijke organisaties. Hierdoor kan geen specifiek beeld van de gemeente Kaag en Braassem verkregen kan worden. Daarnaast hebben er dusdanig weinig medewerkers (<5), per afdeling gereageerd op diverse enquête-items dat de gegevens van vrijwel alle afdelingen van Kaag en Braassem zijn onderdrukt en dus niet weergegeven.

Advies: Blijf doorgaan met het vergroten van privacy-bewustzijn. Zorg voor periodiek terugkerende presentaties en trainingen (fysiek of digitaal) voor de hele organisatie in kleine groepen.

5. Conclusies

De gemeente Kaag en Braassem heeft in 2024 het basis privacy-volwassenheidsniveau vastgehouden en neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen.

De gemeente kan nu het gegevensbeschermingsbeleid vaststellen en dit beleid ook gaan uitvoeren. Het actueel en compleet houden van het register van verwerkingsactiviteiten moet doorgang blijven vinden. Het verhogen van het privacy-bewustzijn binnen de gemeentelijke organisatie verdient blijvende aandacht. Gestarte DPIA's moeten afgemaakt worden en de daaruit voorkomende beheersmaatregelen aansluitend uitgevoerd.

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. Eventueel 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	Hoog
4.2	Governance	Basis	Basis	Midden	Midden
4.3	Mensen en Middelen	Basis	Basis	Midden	LAAG
4.4	Risicomanagement	Basis	Basis	Hoog	Hoog
4.5	Doelbinding	-	INITIEEL	-	HOOG
4.6	Register van verwerkingsactiviteiten	Basis	Basis	Hoog	Hoog
4.7	Kwaliteitsmanagement	-	INITIEEL	-	LAAG
4.8	Beveiliging	Basis	Basis	Midden	Midden
4.9	Informatieverstrekking	-	INITIEEL	-	LAAG
4.10	Bewaartermijnen	Basis	Basis	Laag	Laag
4.11	Doorgifte	Basis	Basis	Laag	Laag
4.12	Intern Toezicht	Basis	Basis	Laag	Laag
4.13	Rechten betrokkenen	Basis	Basis	Laag	Laag
4.14	Datalekken	Basis	Basis	Midden	Midden
4.15	Bewustzijn	Basis	Basis	Hoog	Hoog

6. Aanbevelingen

De belangrijkste aanbevelingen zijn gebaseerd op de parameters waar de meeste winst op het gebied van privacy te halen valt en een hoge prioriteit hebben. Uiteraard is het raadzaam ook de andere adviezen in dit FG-Jaarverslag op te volgen.

1. Stel het gegevensbeschermingsbeleid voor de periode 2024-2029 vast en voer dit beleid daadwerkelijk uit.
2. Breng het register van verwerkingsactiviteiten onder in een applicatie. Zoek daarin de samenwerking met de gemeente Alphen aan den Rijn.
3. Voer het tempo van DPIA's weer op en herontwerp het proces Ondermijning in overeenstemming met de eisen van de AVG.
4. Blijf privacy-bewustzijn aandacht geven.