FG-JAARVERSLAG 2023

Gemeente Kaag en Braassem

Functionaris gegevensbescherming mr. R.R. de Vries, 26 januari 2024

FG-Jaarverslag 2023 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 2023 het basis privacy volwassenheidsniveau bestendigd en neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen.

Er is een visie op gegevensbescherming opgesteld. De gemeente moet nu wel een volgende stap maken door de visie en de daarbij geformuleerde doelen om te zetten in een effectief gegevensbeschermingsbeleid voor de komende vijf jaar. Wellicht kan dan de eerste stap gezet worden naar een hoger privacy volwassenheidsniveau. Het register van verwerkingsactiviteiten wordt steeds completer. Ten aanzien van dit register is de volgende stap het inzetten 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 wel een nieuwe impuls krijgen. Het tempo van uitvoeren van Data Protection Impact Assessments (DPIA's) is in 2023 opgevoerd maar mag nog hoger.

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 aan de hand van de mate waarin de parameters zijn ingevuld 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 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 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 • 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 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 nog niet omgezet in gegevensbeschermingsbeleid. Het beleid geeft aan hoe deze doelen bereikt gaan worden waardoor de gemeente uiteindelijk haar visie kan verwezenlijken. Dit 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 Kaag en Braassem heeft nog geen beleid ontwikkeld voor het gebruik van ChatGPT of andere kunstmatige intelligentie-ontwikkelingen. Er bestaat het gevaar dat het gebruik van dergelijke technologieën onbedoeld wordt geïntroduceerd met mogelijk onvoorziene gevolgen. Het is 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 op 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: Naar aanleiding van de reorganisatie in 2023 waarbij een extra managementlaag is toegevoegd, is een nieuw Privacy Governance document opgesteld. Dit document moet nog wel vastgesteld worden. De aanpassing van taken, bevoegdheden en rapportagelijnen is hiermee dan schriftelijk vastgelegd, maar het is ook belangrijk dat ze in de praktijk worden doorgevoerd en gehandhaafd. Het moet voor alle medewerkers duidelijk zijn wie wanneer verantwoordelijk is voor privacy.

Advies: Let op eigenaarschap bij de verantwoordelijken voor gegevensbescherming. De taken en verantwoordelijkheden moeten opnieuw betekenis gaan krijgen in de gewijzigde managementstructuur.

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: Na de overstap van de privacy-officer naar een managementfunctie is tijdelijk een externe adviseur aangetrokken. In november 2023 is weer een vaste privacy-officer in dienst gekomen. Het aantal uren dat de privacy-officer ter beschikking staat is toegenomen tot 32 uur. Daarnaast is nog 4 uur beschikbaar voor informatiebeveiligingswerkzaamheden. Hiermee is uitvoering gegeven aan het advies uit het FG-Jaarverslag 2022 (4.3).

Advies: Zet de nieuwe privacy-officer vooral ook in voor privacy-awareness bijeenkomsten zodat deze ook goed bekend raakt met alle medewerkers van de organisatie.

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: De DPIA Ondermijning is in 2023 afgerond. Op basis van de daarin opgesomde beheersmaatregelen en het FG-advies zal in 2024 een verbeterplan opgesteld moeten worden om de werkprocessen overeenkomstig de vereisten van de AVG te laten plaatsvinden. Ook is in 2023 de DPIA City Control opgeleverd en is begonnen met de DPIA Jeugdhulp en de DPIA SOZ Jeugdhulp.

Advies: Houd bestaande DPIA's in 2024 tegen het licht om deze actueel te houden en inventariseer in welke werkprocessen nog DPIA's uitgevoerd moeten worden.

4.5 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 halfjaarlijkse uitvraag naar wijzigingen van verwerkingsactiviteiten aan procesverantwoordelijken is in principe een passende maatregel om het register up to date te houden. Echter, het register wordt nu maar één keer per jaar geactualiseerd op actualiteit.

Het register is ingericht op hoofdprocessen naar het VNG-model. Om het register naar een hoger niveau te brengen zou per hoofdproces gedifferentieerd kunnen worden naar afzonderlijke verwerkingen per hoofdproces. Een stap naar de volgende fase kan ook zijn het publiceren van het register op de gemeentelijke website in het kader van transparantie richting de inwoners.

Idealiter zijn het de procesverantwoordelijken zelf (of hun medewerkers) die het register bijhouden en aanvullen. 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 of het wenselijk en mogelijk is om het register op de website te plaatsen.

4.6 Beveiliging

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

Bevindingen: Er worden nu geen rapportages over de informatieveiligheid uitgebracht waarin door de CISO verslag gedaan wordt over de stand van zaken omtrent informatieveiligheid.

Indien toegang tot persoonsgegevens permanent of voor langere tijd niet mogelijk is, kan dat een inbreuk betekenen in verband met persoonsgegevens. Om langdurige stagnatie van de kritieke bedrijfsprocessen van de gemeente te voorkomen dient conform de BIO een proces voor continuïteitsbeheer te worden ingericht. Onderdeel van dit proces vormt het opstellen van het continuïteitsplan. In dit plan zijn de acties vastgelegd die dienen te worden uitgevoerd, nadat een calamiteit is ontstaan. De gemeente Kaag en Braassem beschikt nog niet over een dergelijk continuïteitsplan.

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. Verder is vereist het instellen van een procedure voor regelmatige tests, beoordelingen en evaluaties om de doeltreffendheid van de genomen technische en organisatorische beveiligingsmaatregelen voor de verwerking te controleren.

Er is nog geen plan opgesteld hoe om te gaan met een cybercrisis en welke maatregelen vooraf genomen kunnen worden om een dergelijke crisis te voorkomen als ook maatregelen die de ongewenste gevolgen kunnen verzachten.

Advies: Zorg dat er weer een rapportage over informatieveiligheid opgesteld wordt. Ga verder met het voorbereiden van de organisatie en het bestuur op een groot beveiligingsincident. Oefen cybercrises aan de hand van scenario's.

4.7 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. Vrijwel alle bewaartermijnen zijn in het register van verwerkingsactiviteiten opgenomen. Voor enkele verwerkingen staat nog slechts “Conform Archiefwet”. Bij een eigen bewaartermijn dient een motivering van de duur van de termijn opgenomen te worden.

Advies: Probeer ook van de laatste verwerkingen de juiste bewaartermijnen op te nemen en te motiveren zodat dit onderdeel compleet is. Zorg dat het register op dit onderdeel actueel blijft.

4.8 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: In 2021 werden de verwerkersovereenkomsten in het contractenregister bijgehouden. Vanaf 2022 werden deze overeenkomsten bijgehouden in een apart register. In 2023 zijn de verwerkersovereenkomsten 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 met 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.

4.9 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: Ook tijdens de mutaties in de functie van privacyofficer is een goede samenwerking blijven bestaan tussen de FG en de medewerkers die zich met informatieveiligheid en gegevensbescherming bezig houden. Ook heeft de samenwerking niet geleden onder de veranderingen in de managementstructuur. Het driemaandelijkse memo van de FG helpt de organisatie om tijdig bij te sturen zodat er geen verassingen in het FG-Jaarverslag opdoemen.

Op grond van de Wet Politiegegevens (Wpg) is eind 2022 een externe audit uitgevoerd naar de verwerkingen van politiegegevens (persoonsgegevens die gegenereerd worden in het kader van uitvoering van de politietaken door de boa's). Er wordt gewerkt aan het verbeteren van de zaken die nog niet op orde waren. In het audit rapport is aangegeven dat een externe her-audit moet plaatsvinden om te controleren of een en ander inmiddels op orde is.

Advies: Blijf gebruik maken van de driemaandelijkse memo's om tijdig bij te sturen. Zorg dat alle aanbevelingen uit de Wpg-audit uitgevoerd worden.

4.10 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 zijn in 2023 drie verzoeken om inzage in persoonsgegevens ingediend op grond van artikel 15 AVG. Deze verzoeken hadden slechts betrekking op welke organisaties de persoonsgegevens in de Basisregistratie Personen mogen inzien. De verzoeken zijn correct afgehandeld.

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 zo compleet en actueel mogelijk.

4.11 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 2023 zijn twaalf incidenten opgenomen in het incidentregister. Hiervan zijn acht datalekken waarvan er twee op juiste gronden zijn gemeld bij de Autoriteit persoonsgegevens. 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. Blijf de afhandeling van datalekken door de Servicedesk monitoren.

4.12 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. Deze partij heeft over 2023 een rapportage (met een nulmeting) uitgebracht waaruit een lichte toename blijkt van het privacy bewustzijn. Helaas ziet de rapportage op beide gemeentelijke organisaties als één geheel zodat niet specifiek een beeld van de gemeente Kaag en Braassem verkregen kan worden.

Verder blijkt uit de rapportage dat slechts ongeveer een derde van de medewerkers participeert in het programma. Dit is weliswaar volgens het adviesbureau niet onder het landelijk gemiddelde, maar is naar de mening van de FG onvoldoende om een adequaat

privacy bewustzijnsniveau te creëren. Daarnaast bleek ook dat het in Kaag en Braassem lastig was om voldoende medewerkers te laten participeren in een georganiseerde escaperoom.

Een andere conclusie is dat 60% van de leidinggevenden aangeeft niet over voldoende middelen te beschikken om het gewenste gedrag omtrent informatiebeveiliging en privacy te stimuleren. Dit is echter niet het beeld dat de FG heeft van de leidinggevenden van de gemeente Kaag en Braassem. Vermoedelijk ligt deze uitkomst aan het feit dat de rapportage de twee gemeenten als één organisatie beschouwt.

Advies: Blijf doorgaan met het vergroten van privacy-bewustzijn. Ga weer introductiebijeenkomsten voor nieuwe medewerkers organiseren. Pas voor 2024 het awareness programma aan zodat de resultaten ook specifiek voor Kaag en Braassem zichtbaar en meetbaar zijn. Zorg daarnaast ook voor een jaarlijkse presentatie (fysiek of digitaal) voor de hele organisatie in kleine groepen.

5. Conclusies

De gemeente Kaag en Braassem heeft in 2023 het basis privacy-volwassenheidsniveau bestendigd en neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen.

De gemeente kan een volgende stap maken door de visie op gegevensbescherming en de daarbij geformuleerde doelen om te zetten in een effectief gegevensbeschermingsbeleid. 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 weer hernieuwde aandacht. Bestaande DPIA's moeten onderhouden worden en nieuwe DPIA's geïnventariseerd.

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	
		2022	2023	2022	2023
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	Midden
4.4	Risicomanagement	Basis	Basis	Hoog	Hoog
4.5	Register van verwerkingsactiviteiten	Basis	Basis	Hoog	Hoog
4.6	Beveiliging	Basis	Basis	Midden	Midden
4.7	Bewaartermijnen	Basis	Basis	Laag	Laag
4.8	Doorgifte	Basis	Basis	Laag	Laag
4.9	Intern Toezicht	Basis	Basis	Laag	Laag
4.10	Rechten betrokkenen	Basis	Basis	Laag	Laag
4.11	Datalekken	Basis	Basis	Midden	Midden
4.12	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 op basis van de vastgestelde visie en doelen op gegevensbeschermingsbeleid op voor de periode 2024-2029.
2. Breng het register van verwerkingsactiviteiten onder in een applicatie. Zoek daarin de samenwerking met de gemeente Alphen aan den Rijn en de BVO.
3. Onderhoud oude DPIA's en inventariseer nieuwe DPIA's.
4. Start weer met de privacy-trainingen voor de nieuwe medewerkers. Pas het awareness programma aan zodat er specifiek informatie voor de gemeente Kaag en Braassem beschikbaar is. Ga ook zelf presentaties geven.