FG-JAARVERSLAG 2025

Gemeente Alphen aan den Rijn

Functionaris gegevensbescherming mr. R.R. de Vries, 20 februari 2026

FG-Jaarverslag 2025 Alphen aan den Rijn

Inhoudsopgave

1. Managementsamenvatting 2

2. Inleiding 3

2.1 Achtergrond 3

2.2 Doelstelling 3

2.3 Aanpak 3

3. Leeswijzer 4

3.1 Parameters 4

3.2 Groeimodel 4

4. Parameters 5

4.1 Visie, doelen en beleid 5

4.2 Governance 6

4.3 Mensen en Middelen 6

4.4 Risicomanagement 7

4.5 Doelbinding 8

4.6 Register van verwerkingsactiviteiten 9

4.7 Kwaliteitsmanagement 9

4.8 Beveiliging 10

4.9 Informatieverstrekking 11

4.10 Bewaartermijnen 11

4.11 Doorgifte 12

4.12 Intern toezicht 13

4.13 Rechten betrokkenen 14

4.14 Datalekken 14

4.15 Bewustzijn 15

5. Conclusies 17

6. Aanbevelingen 19

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 Alphen aan den Rijn getroffen heeft om te kunnen waarborgen en aantonen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met de AVG.

De formatie voor privacy binnen de gemeente Alphen aan den Rijn was, hoewel verbeterd, nog niet op sterkte. Dat heeft ertoe geleid dat er te weinig privacy trainingen gegeven zijn. Hierdoor bestaat er nog onvoldoende privacy bewustzijn binnen de organisatie. Ook ontbreekt er nog een duidelijke governance op het gebied van gegevensbescherming. Onvoldoende privacy bewustzijn en onduidelijke governance zorgt voor onvoldoende gevoeld eigenaarschap.

De organisatie begrijpt wel steeds beter dat bij bepaalde nieuwe verwerkingen van persoonsgegevens een DPIA uitgevoerd moet worden. De volgende stap zou moeten zijn dat de implementatie van de beheersmaatregelen die voortvloeien uit de DPIA ook gemonitord en gecontroleerd wordt.

De visie op gegevensbescherming uit 2022 is nog steeds niet omgezet in beleid. Het opstellen en vervolgens uitvoeren van gegevensbeschermingsbeleid draagt ertoe bij dat de gemeente Alphen aan den Rijn in control kan komen met betrekking tot de bescherming van persoonsgegevens. Er is geen visie op het inzetten van AI binnen de gemeente.

Het register van verwerkingsactiviteiten wordt handmatig bijgehouden. Niet alleen legt dit een substantieel beslag op de tijd van de privacy-officers, ook is het efficiënter om het register in een Privacy Information Management System op te nemen waarin procesverantwoordelijken zelf de verwerkingen actueel en compleet kunnen houden.

De datalekken werden in 2025 correct geregistreerd en gemeld. Bij voorkeur zouden de datalekken ook opgenomen moeten worden in een Privacy Information Management System. Er wordt nu niet standaard onderzocht of de voorgenomen beheersmaatregelen om datalekken in de toekomst te voorkomen daadwerkelijk worden uitgevoerd dan wel effect sorteren.

Het ongestructureerde archief van Jeugdzorg leidt tot problemen bij inzageverzoeken. Dit archief zal zo snel mogelijk op orde moeten komen om aan de wettelijke termijnen te kunnen voldoen. Deze termijnen worden nu ruimschoots overschreden.

2. Inleiding

2.1 Achtergrond

Per 1 mei 2020 heeft de gemeente Alphen aan den Rijn de huidige functionaris gegevensbescherming (FG) aangewezen. Deze aanwijzing is overeenkomstig artikel 37 van de Algemene Verordening Gegevensbescherming (AVG) verplicht voor overheidsorganisaties. Hierbij is gekozen voor een constructie waarbij de FG gedeeld wordt met de gemeenten Nieuwkoop, 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 Alphen aan den Rijn 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 informeert de FG elke maand de gemeentesecretaris omtrent zijn bevindingen. Het is echter aan de gemeente om maatregelen te nemen en daarover verantwoording af te leggen. De aanpak van de FG is zoals de AVG voorschrijft altijd risico gestuurd, 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 Alphen aan den Rijn 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 Alphen aan den Rijn 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 Alphen aan den Rijn. 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 Alphen aan den Rijn 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 kan de volgende stap zijn 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.

Alhoewel er richtlijnen voor het gebruik van AI-tools zijn opgesteld, heeft de gemeente nog geen visie op AI ontwikkeld. Hierin zou opgenomen moeten worden wat de gemeente op het gebied van AI de komende vijf jaar wil bereiken en welke concrete doelen verwezenlijkt zouden moeten worden. AI is geen doel op zich maar kan een hulpmiddel zijn om organisatiedoelen efficiënter of effectiever te bereiken.

Vanaf 2 februari 2025 verplicht de AI-verordening organisaties werk te maken van AI-geletterdheid. Een belangrijke voorwaarde voor de verantwoorde inzet van AI is een toereikend kennisniveau bij medewerkers die met AI te maken krijgen. Het doel is dat alle relevante personen binnen de gemeentelijke organisatie geïnformeerde keuzes met betrekking tot AI-systemen kunnen maken. De gemeente moet inventariseren welke AI-systemen er gebruikt worden binnen de organisatie en welke kennis er al is. In 2025 was er nog geen plan om de AI-geletterdheid binnen de gemeente te bevorderen.

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 een visie op voor het gebruik van AI. Maak werk van AI-geletterdheid.

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: Ook in 2025 was nog niet vastgelegd welke verantwoordelijkheden, bevoegdheden en rapportagelijnen er zijn op het gebied van gegevensbescherming binnen de gemeentelijke organisatie. Maar privacy governance gaat verder dan alleen een document: leidinggevenden en medewerkers moeten ook weten wat er van hen verwacht wordt op het gebied van gegevensbescherming.

Advies:

- Zet een duidelijke governance-structuur voor privacy op;
- Draag deze governance ook uit binnen de organisatie.

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 lijst met privacy contactpersonen is al sinds 2020 onvolledig en niet actueel. Posities zijn vacant of het betreft personen die reeds geruime tijd niet meer werkzaam zijn bij de gemeente. Deze privacy-contactpersonen zijn een cruciale link naar de teams met betrekking tot het tijdig uitvoeren van DPIA's, het bijhouden van het register van verwerkingsactiviteiten en het voldoen aan de rechten van betrokkenen.

In 2025 waren er twee privacy-officers fulltime beschikbaar voor privacy werkzaamheden. Ten opzichte van voorgaande jaren is hierin verbetering gekomen maar de formatie was nog onvoldoende om alle werkzaamheden te kunnen uitvoeren. Dat is vooral te merken aan het geringe aantal privacy trainingen dat jaarlijks gegeven wordt. Wel is er financiële ruimte gemaakt om in 2026 een derde privacy officer te werven: een organisatie als de gemeente Alphen aan den Rijn dient minimaal te beschikken over drie fulltime privacy officers om het takenpakket goed aan te kunnen.

Advies:

- Breng de lijst met privacy contactpersonen op orde;
- Zorg voor minimaal drie fulltime privacy officers.

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: Er zit een stijgende lijn in het uitvoeren van DPIA's: in 2025 werden er zeven opgeleverd. Het betreft de DPIA's Vroegsignalering, Nazorg ex-gedetineerden, Toezicht WMO, Telefonieplatform Serviceplein, Kosten Jeugdzorg, Rittenregistratie, HRM-Youforce. Twee andere DPIA's waren eind 2025 in de afrondingsfase.

Het belangrijkste advies van de FG op de DPIA Ondermijning uit 2024 was het herontwerpen van het proces Ondermijning om het verwerken van persoonsgegevens zonder grondslag te voorkomen. In 2025 heeft het herontwerpen van het werkproces Ondermijning niet plaatsgevonden.

In 2024 bleken op Langeroode camera's te hangen in onder andere kleedkamers. Deze camera's zijn verwijderd, maar de verplichte DPIA op de andere camera's op het complex is in 2025 niet uitgevoerd.

Projecten binnen de gemeentelijke organisatie zijn vaak gericht op de aanbesteding, inrichting en ingebruikname van applicaties. Deze applicaties zullen veelal een verandering in het werkproces bewerkstelligen. Dit betekent dan ook dat de verwerking van persoonsgegevens aan verandering onderhevig kan zijn. Voor applicaties die veel en/of bijzondere persoonsgegevens verwerken zal dan mogelijk een DPIA uitgevoerd moeten worden. Daarom is het raadzaam het uitvoeren van een DPIA in de projectmanagementmethodiek mee te nemen.

Advies:

- Voer DPIA's uit vóórdat de verwerkingen van persoonsgegevens plaatsvinden;
- Monitor of de beheersmaatregelen ook daadwerkelijk uitgevoerd worden vóórdat de verwerkingen van persoonsgegevens plaatsvinden;
- Integreer het uitvoeren van DPIA's in het projectmanagement.

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: Begin 2024 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. Dit herontwerp heeft ook in 2025 niet plaatsgevonden.

De gemeente heeft in 2025 een datavisie opgesteld. In deze visie vormt het dataplatform het fundament waar informatie samengebracht en domein overstijgend benut wordt. Het is bedoeling om met een betere informatiepositie efficiënter en transparanter te werken en duidelijker verantwoording af te kunnen leggen.

In het werken met een dataplatform waar vanuit verschillende taakvelden persoonsgegevens worden samengebracht, schuilt echter wel een gevaar: persoonsgegevens moeten altijd verwerkt worden (i.e. verzameld zijn) voor een welbepaald, gerechtvaardigd doel. Dit betekent echter ook dat persoonsgegevens niet verder mogen worden verwerkt op een manier die onverenigbaar is met de doeleinden waarvoor ze oorspronkelijk zijn verzameld.

Is dat niet het geval, dan mogen deze persoonsgegevens dus niet verder verwerkt worden, tenzij beargumenteerd kan worden dat het doel van de verwerking dus verenigbaar is met het oorspronkelijke doel.

Advies:

- Herontwerp het proces Ondermijning;
- Bepaal bij het verzamelen van persoonsgegevens in het dataplatform vooraf voor welk doel dit gebeurt;
- Onderzoek vervolgens of de te verwerken persoonsgegevens echt noodzakelijk zijn om het doel te behalen en de verwerking verenigbaar is met het oorspronkelijke doel.

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 door één van de privacy-officers periodiek actueel gehouden. verwerkingen of wijzigingen zijn opgetreden. Het is echter efficiënter en qua governance zuiverder, als het register wordt bijgehouden door de procesverantwoordelijken in een Privacy Management System waarin de privacy-officers kunnen controleren of de procesverantwoordelijken deze taak correct uitvoeren.

Advies:

- Zorg voor een applicatie om het register van verwerkingsactiviteiten in op te nemen;
- Onderzoek of het mogelijk is om het register te publiceren ten behoeve van transparantie richting de inwoners.

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 teamleiders). 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:

- Ontwikkel en implementeer een kwaliteitsmanagementsysteem van periodieke controles op juistheid, nauwkeurigheid, actualiteit, volledigheid en correct gebruik van gegevens;
- Ontwikkel en implementeer een systeem dat het behalen van de doelen uit het gegevensbeschermingsbeleid en 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: Waar in 2024 alle accounthouders binnen Jeugdzorg nog toegang konden hebben tot alle dossiers, is er in 2025 meer scheiding aangebracht tussen de werkvoorraden per wijkteam. Idealiter kan elke professional slechts tot de eigen toegewezen dossiers toegang hebben. Wat in 2025 nog niet gerealiseerd was, is de scheiding tussen persoonsgegevens met betrekking tot toeleiding en persoonsgegevens met betrekking tot hulpverlening.

Advies:

- Zorg dat toegang tot dossiers die niet tot de persoonlijke werkvoorraad horen, zo veel mogelijk beperkt wordt;
- Breng in de applicatie een scheiding aan tussen persoonsgegevens met betrekking tot toeleiding en persoonsgegevens met betrekking tot hulpverlening;

De gemeente Alphen aan den Rijn had in 2025 nog geen incident responseplan vastgesteld om een cybercrisis het hoofd te kunnen bieden. Voor het bepalen van de kritieke processen wordt afgegaan op de Top kritieke bedrijfsprocessen van de Informatiebeveiligingsdienst van de VNG. Van de twaalf kritieke processen van deze lijst scoren er tien hoog of zeer hoog op

privacy, wat aangeeft dat nauwkeurigheid en bescherming van gegevens cruciaal zijn. Op basis van kritieke processen werd in 2025 nog geen business continuïteitsplan opgesteld.

In 2025 was nog geen ondersteunend systeem aanwezig zoals een Information Security Management Systeem waarmee de uitvoering van informatieveiligheidsbeleid kan worden gecontroleerd en bijgestuurd overeenkomstig een PDCA cyclus. De CISO is niet onafhankelijk gepositioneerd in de organisatie.

Advies:

- Ga verder de voorbereiding om een majeur beveiligingsincident te kunnen weerstaan.
- Oefen cybercrises aan de hand van scenario's;
- Stel een business continuïteitsplan op;
- Geef de CISO een onafhankelijk positie in de organisatie;
- Zorg voor de aanschaf en implementatie van een ISMS;

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. Het kan hier de verwerking van bijzondere en gevoelige persoonsgegevens alsmede persoonsgegevens van strafrechtelijke aard betreffen. Hoewel vanuit het perspectief van deze projecten 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.

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: De AVG vergt dat in het register van verwerkingsactiviteiten de bewaartermijnen van elke verwerking worden opgenomen. Op dit moment staan nog niet alle bewaartermijnen in het register. Ook kan niet volstaan worden met "wettelijke bewaartermijn" of "zolang noodzakelijk is" zoals nu soms het geval is. Bij een wettelijke bewaartermijn moet vermeld worden welke wet het betreft en hoelang de termijn is. Bij een eigen bewaartermijn moet gemotiveerd kunnen worden waarom tot een bepaalde duur besloten is.

Advies:

- Neem van alle verwerkingen in het register van verwerkingsactiviteiten ook de bewaartermijnen op;
- Geef daarbij aan op welke wettelijke bepaling deze zijn gebaseerd of een motivering van de noodzaak van de bewaartermijn;
- Indien geen bewaartermijnen in applicaties opgenomen kunnen worden, dienen de persoonsgegevens verwijderd te worden.

4.11 Doorgifte

Context: Persoonsgegevens kunnen op drie manieren doorgegeven worden aan 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.

Bevindingen: De verwerkersovereenkomsten die de BVO afgesloten heeft, zijn geregistreerd in Topdesk en gearchiveerd in een separate BVO omgeving in het zaaksysteem. Er is echter geen register waarin de verwerkersovereenkomsten die de gemeente Alphen aan den Rijn zelf afsluit worden opgenomen. Er is geen overzicht van de nog af te sluiten verwerkers-overeenkomsten. Hierdoor is geen behoorlijk beheer van de verwerkersovereenkomsten mogelijk. Daarnaast is er ook geen overzicht van samenwerkingsverbanden waar

gezamenlijke verwerkingsverantwoordelijkheid uit voortvloeit. Ook is nog niet duidelijk met welke partijen dataleveringsovereenkomsten gesloten zijn of nog moeten worden.

Advies:

- Leg een apart register aan met verwerkersovereenkomsten, onderlinge regelingen en gegevensleveringsovereenkomsten. Dit register dient bij voorkeur opgenomen te worden in de geadviseerde applicatie;
- Ga na welke overeenkomsten nog gesloten moeten worden en neem deze vervolgens in het register op.

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.

Op grond van de AVG dient de gemeente er zorg voor te dragen dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Bevindingen: De FG wordt steeds beter betrokken bij nieuwe ontwikkelingen die de bescherming van persoonsgegevens betreffen. Het is van groot belang dat de FG kennis kan nemen van deze ontwikkelingen omdat deze anders het toezicht niet goed kan uitoefenen. Vooral ontwikkelingen die een potentieel groot risico voor de bescherming van persoonsgegevens met zich meebrengen dienen in een vroeg stadium gemeld te worden aan de FG. Denk aan Jeugdzorg, cameratoezicht en de bouw van dasboards en rapportages op basis van het dataplatform.

De FG brengt elke maand een memo uit aan de gemeentesecretaris met zaken die hem opvallen of die naar zijn oordeel urgent zijn. Bij voorkeur hoort de FG geïnformeerd te worden over de opvolging van deze zaken. De FG is in 2025 goed betrokken geweest bij de DPIA's, zowel in het voorstadium als tijdens de uitvoering daarvan.

Advies:

- Betrek de FG in een zo vroeg mogelijk stadium bij besluiten of ontwikkelingen die de bescherming van persoonsgegevens (kunnen) betreffen;
- Geef telkens terugkoppeling op het FG-memo.

4.13 Rechten betrokkenen

Context: Iedere betrokkene wiens persoonsgegevens door de gemeente Alphen aan den Rijn 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: In 2024 zijn 30 inzageverzoeken ingediend op grond van artikel 12 AVG. Vier daarvan waren oneigenlijke inzageverzoeken. Elf verzoeken werden binnen de termijn afgehandeld. De gemeente dient de betrokkene onverwijld en in ieder geval binnen één maand na ontvangst van het verzoek informatie te verstrekken over het gevolg dat aan het verzoek is gegeven.

Er zijn acht inzageverzoeken gedaan naar jeugddossiers die bewaard worden in het archief dat de gemeente verkregen heeft bij de migratie van de persoonsgegevens van GO! Voor Jeugd naar de gemeente. Dit archief is niet gestructureerd en kan alleen ingezien worden door medewerkers met een SKJ-registratie aangezien hier mogelijk persoonsgegevens met betrekking tot hulpverlening in voorkomen. Omdat de privacy officers niet beschikken over een SKJ-registratie en vanuit Jeugdzorg geen capaciteit vrijgemaakt kon worden, heeft de afhandeling van deze inzageverzoeken aanzienlijke en daarmee ongewenste vertraging opgelopen.

Advies:.

- Zorg ervoor dat de termijn van één maand waarbinnen informatie verstrekt moet worden over het verzoek gegeven altijd gehaald wordt;
- Structureer zo snel mogelijk het Jeugdzorg archief zodat voldaan kan worden aan de termijn van het afhandelen van de inzageverzoeken.

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: Het aantal geregistreerde datalekken in 2025 bedraagt 60. Dit is vrijwel hetzelfde aantal als in 2024 (59). Een groot deel van de datalekken betreft het mailen naar verkeerde email adressen en het verzenden van brieven naar verkeerde postadressen. Van de datalekken zijn er zestien gemeld aan de Autoriteit Persoonsgegevens aangezien hier mogelijk sprake was van een risico voor de betrokkenen. De gemeente heeft 15 keer de betrokkenen geïnformeerd over een datalek ofwel omdat er sprake was van een hoog risico voor deze betrokkenen ofwel om excuses aan te bieden of extra uitleg.

Het beeld dat bestaat is vrijwel hetzelfde als in 2024. Het register van datalekken wordt verder goed bijgehouden maar dient bij voorkeur in een Privacy Management Information System bijgehouden te worden. Er wordt nu niet standaard onderzocht of de voorgenomen beheersmaatregelen om datalekken in de toekomst te voorkomen daadwerkelijk worden uitgevoerd dan wel effect sorteren.

Advies:

- Neem het register van datalekken op in een Privacy Management Information System;
- Monitor de voorgenomen beheersmaatregelen op uitvoering en effectiviteit.

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: Het contract met de externe partij om een awareness programma te verzorgen is in 2025 afgelopen. De belangrijkste activiteit van deze partij was voornamelijk het verzorgen van e-learnings op het gebied van privacy en informatieveiligheid. Daarnaast zijn door de privacy officers enkele trainingen gegeven. De FG geeft echter de voorkeur aan het op wekelijkse basis geven van privacy trainingen door de privacy officers voor kleine groepen tot tien personen. Deze trainingen kunnen digitaal gegeven worden zodat ook thuiswerkende medewerkers bereikt kunnen worden. Deze trainingen zouden een verplicht karakter moeten hebben. Ook zou privacy standaard in het on-board programma voor nieuwe medewerkers moeten worden opgenomen.

Advies:

- Blijf doorgaan met het vergroten van privacy-bewustzijn;
- Zorg daarnaast ook voor wekelijkse trainingen (fysiek of digitaal) voor de hele organisatie in kleine groepen;
- Neem privacy op in het on-board programma.

5. Conclusies

Door het omzetten van de visie op gegevensbescherming en de daarbij geformuleerde doelen in een effectief gegevensbeschermingsbeleid, kan de gemeente aan de voorkant komen in plaats van te reageren op de aanbevelingen en adviezen van de FG. Dit is een eerste stap richting privacy-volwassenheid.

De privacy officers moeten meer worden ingezet om wekelijkse privacy trainingen te geven. Door een groter privacy bewustzijn worden ook de taken en verantwoordelijkheden op het gebied van gegevensbescherming bij management en medewerkers duidelijker. Deze privacy governance moet voor de organisatie opnieuw opgesteld worden en daar ook betekenis gaan krijgen.

Privacy bewustzijn en een duidelijke, gedragen governance zorgen er ook voor dat het bij medewerkers en management duidelijk is wanneer een DPIA uitgevoerd moet worden en dat voorgenomen beheersmaatregelen die uit de DPIA voortvloeien ook daadwerkelijk uitgevoerd en gemonitord worden.

Het register van verwerkingsactiviteiten werd goed bijgehouden afgezien van het soms ontbreken van bewaartermijnen. Het register dient bij voorkeur ondergebracht worden in een applicatie. Hierdoor kunnen procesverantwoordelijken zelf hun eigen verwerkingen actueel en compleet houden.

Het archief van Jeugdzorg zal gestructureerd en toegankelijk gemaakt moeten worden om te kunnen beantwoorden aan de inzageverzoeken binnen de daarvoor gestelde termijn.

Op de volgende pagina wordt aangegeven in welke fase de gemeente zich in 2025 bevond met betrekking tot de invulling van de parameters en de prioriteit die de FG hier aan gegeven heeft voor het daarop volgende jaar. Ter vergelijking is dit ook voor 2024 aangegeven. Kapitale letters geven de verandering ten opzichte van het vorige jaar weer. De grijsgekleurde rijen komen terug in de belangrijkste aanbevelingen.

		Fase groeimodel		Prioriteit	
	Parameter	*2024*	*2025*	*2025*	*2026*
4.1	Visie, doelen en beleid	Basis	Basis	Hoog	Hoog
4.2	Governance	Initieel	Initieel	Hoog	Hoog
4.3	Mensen en Middelen	Initieel	**BASIS**	Hoog	**MIDDEN**
4.4	Risicomanagement	Initieel	**BASIS**	Hoog	Hoog
4.5	Doelbinding	Initieel	Initieel	Midden	**HOOG**
4.6	Register van verwerkingsactiviteiten	Initieel	Initieel	Hoog	Hoog
4.7	Kwaliteitsmanagement	Basis	Basis	Midden	Midden
4.8	Beveiliging	Basis	Basis	Midden	Midden
4.9	Informatieverstrekking	Basis	Basis	Laag	Laag
4.10	Bewaartermijnen	Initieel	Initieel	Laag	Laag
4.11	Doorgifte	Initieel	Initieel	Laag	Laag
4.12	Intern Toezicht	Initieel	**BASIS**	Hoog	**MIDDEN**
4.13	Rechten betrokkenen	Basis	**INITIEEL**	Hoog	**HOOG**
4.14	Datalekken	Basis	Basis	Midden	Midden
4.15	Bewustzijn	Basis	Basis	Hoog	Hoog

6. Aanbevelingen

De belangrijkste aanbevelingen zijn afgestemd op de parameters die zich in de fase *Initieel* of *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 gegevensbeschermingsbeleid op voor de periode 2026-2029;
2. Zet een governance-structuur voor gegevensbescherming op en geef deze betekenis;
3. Voer niet alleen DPIA's uit maar monitor ook de opvolging van de beheersmaatregelen.
4. Herontwerp het proces Ondermijning en bepaal bij het verzamelen van persoonsgegevens in het dataplatform vooraf voor welk doel dit gebeurt;
5. Breng het register van verwerkingsactiviteiten onder in een applicatie;
6. Structureer het Jeugdzorg archief;
7. Ga wekelijks privacy trainingen geven.