Management response FG-Jaarverslag 2024

Hfdstk	Advies FG	Management response
4.1	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.	In 2024 is het concept gegevensbeschermingsbeleid 2025 - 2027 opgesteld. In lijn met het advies uit het FG-Jaarverslag wordt het gegevensbeschermingsbeleid samen met het FG-Jaarverslag voorgelegd aan het college van B&W ter vaststelling. Hiermee zetten we een belangrijke stap in het versterken van onze missie, visie en doelen rondom gegevensbescherming en zorgen we voor een duidelijke basis voor de naleving van privacywetgeving. Voor het opstellen van een visie op het gebruik van AI, is het belangrijk om eerst een duidelijk beeld te krijgen van wat AI voor onze gemeente kan betekenen. Daarom worden dit jaar AI-inspiratiesessies georganiseerd, waarin we de mogelijkheden, kansen en risico's van AI verkennen. Op basis van de inzichten uit deze sessies zal een visie worden opgesteld die richting geeft aan de verantwoorde en doordachte omgang met AI binnen de gemeente. Tot die tijd zijn de vastgestelde AI-richtlijnen van kracht. In deze richtlijnen wordt geadviseerd terughoudend om te gaan met het gebruik van AI-tools, en wordt benadrukt dat er geen persoonsgegevens of andere gevoelige gegevens mogen worden gedeeld.
4.2	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.	Om het eigenaar schap te stimuleren gaan wij werken aan een cultuur waarin gegevensbescherming wordt gezien als een gezamenlijke verantwoordelijkheid. Dit doen we door het promoten van best practices en het delen van succesverhalen. En de inspanningen en prestaties van medewerkers op het gebied van gegevensbescherming te belonen.
4.3	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.	Privacybewustzijn binnen de organisatie is essentieel, en daarom wordt in 2025 extra aandacht besteed aan het vergroten van het bewustzijn d.m.v. privacybewustwordingssessies. Zo maken nieuwe medewerkers hier direct kennis mee tijdens de welkomstdagen, waar de PO een presentatie geeft over privacy en informatiebeveiliging. Zo zorgen we ervoor dat privacybewustzijn vanaf de start een vast onderdeel is van hun werkzaamheden. Daarnaast worden er afspraken ingepland met teams binnen de organisatie om gerichte privacybewustwordingssessies te organiseren. Dit biedt medewerkers de kans om dieper in te gaan op privacyvraagstukken die relevant zijn voor hun werk, en helpt om privacy structureel te verankeren in de organisatie.

4.4	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.	Om ervoor te zorgen dat DPIA's efficiënt en zorgvuldig worden uitgevoerd, is in 2025 de DPIA-Handreiking vastgesteld, Deze handreiking vormt de basis voor een goed uitgevoerde DPIA en biedt medewerkers een duidelijke en gestructureerde aanpak. Door helder uit te leggen welke stappen moeten worden doorlopen, maken we het proces toegankelijker en begrijpelijker, zodat DPIA's niet als een complexe opgave worden ervaren. Daarnaast is hier ook eigenaarschap rondom DPIA's in uitgewerkt. Procesverantwoordelijken hebben de taak om DPIA's op te stellen en de voorgestelde maatregelen na oplevering snel door te voeren en aan te tonen. De verantwoordelijkheden bij de juiste medewerkers te beleggen draagt bij aan een efficiëntere werkwijze en voorkomt onnodige vertragingen in het implementeren van verbeteringen. Om verdere voorgang te waarborgen, is er in 2025 ook een nieuwe prioriteitenlijst opgesteld. Deze lijst helpt bij het gericht uitvoeren van DPIA's en zorgt ervoor dat de meest risicovolle verwerkingen de benodigde aandacht krijgen.
4.5	Herontwerp in 2025 het proces Ondermijning op basis van het beschikbaar wettelijk instrumentarium.	Wij onderschrijven het advies om het proces rondom ondermijning opnieuw te ontwerpen op basis van het beschikbare wettelijke instrumentarium. Dit traject zal in 2025 worden opgepakt; het proces wordt integraal herzien en vanaf de basis opnieuw uitgetekend. Dit zorgt voor een heldere, wetgevingsgerichte aanpak en een effectieve toepassing van de beschikbare middelen.
4.6	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.	In 2025 wordt onderzocht of een Privacy Management Systeem (PMS) kan worden geïmplementeerd om verschillende privacygerelateerde processen efficiënter en overzichtelijker te beheren. Zo biedt een PMS niet alleen de mogelijkheid om het register van verwerkingsactiviteiten op een gestructureerde manier bij te houden, maar ook andere belangrijke onderdelen zoals contractmanagement van de verwerkersovereenkomsten en het bijhouden van een datalekregister. Dit zijn allemaal adviespunten die in het FG-Jaarverslag worden benoemd, waarvoor een centrale en geïntegreerde oplossing wenselijk en mogelijk is. Tot die tijd wordt onze huidige werkwijze (halfjaarlijkse uitvraag naar wijzigingen) gehanteerd.

		Zodra duidelijk is welke applicaties geschikt zijn en hoe de functionaliteiten optimaal benut kunnen worden, kan worden gekeken naar de wenselijkheid en haalbaarheid van het online publiceren van (delen van) het register van verwerkingsactiviteiten.
4.7	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.	De mogelijkheden van een kwaliteitsmanagementsysteem zullen samen met een PMS worden onderzocht. Zie bovenstaand punt (4.6).
4.8	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.	Eind 2024 is een belangrijke stap gezet in het versterken van informatieveiligheid binnen de organisatie, met specifieke aandacht voor de rol van de CISO om hem in een onafhankelijke en sterkere positie te plaatsen. Voor het eerst is er CISO-Jaarverslag opgesteld, waarin voorliggende adviezen en aandachtspunten rondom informatieveiligheid worden benoemd. Vanaf heden zal dit verslag jaarlijks worden opgesteld door de CISO, waarop een management response volgt. Hiermee kunnen de aanbevelingen direct worden opgepakt en doorgevoerd. Daarnaast wordt de positie van de CISO verder versterkt door zijn structurele deelname aan het driemaandelijkse Privacy en Informatiebeveiliging overleg met de gemeentesecretaris. De CISO stelt voor ieder overleg memo's op met daarin de belangrijkste aandachtspunten en adviezen rondom informatieveiligheid. Zo wordt op het hoogste niveau de focus gezamenlijk gelegd op informatiebeveiliging. Daarnaast worden deze memo's ook gedeeld met de Concerncontroller en het Managementteam. Dit zorgt ervoor dat informatieveiligheid organisatiebreed wordt besproken en gedragen, waardoor adviezen niet alleen op strategisch niveau, maar in de gehele organisatie serieus worden genomen en opgepakt.
4.9	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	Om te waarborgen dat de transparantie over de verzameling en verwerking van persoonsgegevens naar betrokkenen altijd gegarandeerd is, worden de privacyverklaringen op de website continu geüpdatet en aangevuld. Vanaf 2025

	betrokkene zijn rechten kan uitoefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking.	wordt er bovendien een register bijgehouden waarin een duidelijk overzicht wordt gegeven van welke privacyverklaringen op de website staan, welke nog toegevoegd moeten worden en wanneer deze voor het laatst zijn geüpdatet. Dit register wordt halfjaarlijks bijgewerkt, gelijktijdig met het register van verwerkingen.
4.10	Zorg dat alle bewaartermijnen opgenomen zijn in het register van verwerkingsactiviteiten.	Met proceseigenaren worden afspraken ingepland voor het opnieuw invullen van het register, waaronder bewaartermijnen (zie punt 4.13). Dit zal worden gecontroleerd met DIV a.d.h.v. de selectielijst.
4.11	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	Zoals vermeld onder 4.6 wordt in 2025 onderzoek gedaan naar een PMS waarin onder andere een register van verwerkersovereenkomsten kan worden bijgehouden.
4.12	Blijf nota nemen van de driemaandelijkse memo's om tijdig bij te sturen en om niet voor verrassingen te komen staan bij ontvangst van het FG-Jaarverslag.	Het belang van de driemaandelijkse memo's wordt onderkend. De overleggen blijven driemaandelijks ingepland worden met de FG, CISO, PO, clustermanager en gemeentesecretaris. Daarnaast zal vanaf 2025 ook de concerncontroller hierbij aansluiten.
4.13	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.	Onderkend wordt dat een compleet en actueel register van verwerkingsactiviteiten van groot belang is voor de organisatie. Daarom wordt het register in 2025 volledig opnieuw ingevuld door de Privacy Officer en de proceseigenaren. Door deze aanpak worden alle verwerkingen vanaf de basis zorgvuldig vastgelegd, en kunnen proceseigenaren hier actief op toezien. Het uiteindelijke doel is om het register van verwerkingsactiviteiten onder te brengen in een applicatie (PMS), zoals in 4.6 werd benoemd. Tot die tijd wordt het register halfjaarlijks bijgewerkt, zodat de informatie actueel blijft.
4.14	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.	Zoals vermeld onder 4.6 zal dit jaar onderzoek worden gedaan naar een PMS waarin het register van datalekken kan worden bijgehouden. Tot die tijd registreert de PO de datalekken in TOPdesk en wordt het register van datalekken nauwkeurig bijgehouden conform het datalekkenprotocol.
4.1	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.	Zoals vermeld onder 4.3 zal de PO dit jaar meer worden ingezet op het vergroten van privacy-bewustzijn. Het awareness programma, dat onder andere bestaat uit interactieve onderdelen zoals een 'cyber escaperoom', zal in 2025 opnieuw worden opgezet en uitgevoerd.