Hfdst.	Prio	Advies	Management response
4.1	!	Stel de visie vast. Plaats de doelen in de tijd weg en zet ze om in gegevensbeschermingsbeleid en voer dit beleid uit. Betrek hier bij voorkeur zo veel mogelijk stakeholders bij. Indien externe factoren impact hebben op het beleid, onderzoek dan of de doelen en eventueel de visie bijgesteld moeten worden.	Het visie-document is op 24 januari 2023 door het college vastgesteld. Het gegevensbeschermingsbeleid, inclusief de uitvoering ervan, is vervat in een jaarplanning. In deze jaarplanning is ook de periodieke evaluatie van het visie-document opgenomen.
4.2		Zorg voor eigenaarschap bij de medewerkers die op dagelijkse basis met gegevensbescherming te maken hebben. De taken en verantwoordelijkheden moeten opnieuw betekenis gaan krijgen in de te wijzigen managementstructuur.	Ook in de nieuwe organisatiestructuur moet men zich bewust zijn van zijn/haar verantwoordelijkheden op het gebied van privacy. Nieuwe medewerkers, inclusief de nieuw aan te stellen managers, worden hier middels AVG-bewustwordingssessies op getraind. Zie punt 4.12 (bewustzijn) voor meer uitleg hierover. Op deze manier wordt eigenaarschap gestimuleerd. De structuur (wie is waarvoor verantwoordelijk) wordt periodiek geëvalueerd.
4.3		Concentreer zo veel mogelijk privacy werkzaamheden liefst bij één medewerker (privacy officer). Breid daarvoor het aantal uren dat de privacy officer besteed aan gegevensbescherming uit.	Op dit moment kent de gemeente één Privacy Officer (PO). De PO heeft een beperkt aantal uren beschikbaar en wordt ondersteund door diverse medewerkers, met verschillende achtergronden (juridisch en archief). Het advies van de FG is gehoord en wordt ter overweging meegenomen in de nieuwe organisatiestructuur. Ook wordt onderzocht of de rol van de Privacy Officer extern kan worden belegd. Behalve de wijziging over de uitvoering van DPIA's door externen als genoemd in punt 4.5 blijft voor nu de situatie zoals die is.

4.4	!	Probeer meer expertise en ervaring op te bouwen op het gebied van DPIA’s. Voer meer DPIA’s uit en in een hoger tempo.	Onderkend wordt dat onderzoeken naar privacy (Data Protection Impact Assessments: DPIA's) belangrijk zijn voor onze gemeente. Wij verwerken veel, soms zeer gevoelige (persoons)gegevens. De uitvoering van DPIA's is op dit moment belegd bij medewerkers die niet privacy als - primair - vakgebied hebben. Omdat deze medewerkers ook veel andere taken hebben en de uitvoering van DPIA's geborgd moet blijven, kunnen in 2023 ook externen ingezet worden om DPIA's uit te voeren. Het uitgangspunt is dat DPIA's bij nieuwe processen door externen worden uitgevoerd (bijkomend voordeel: kortere doorlooptijd) en DPIA's op al bestaande processen door interne medewerkers worden uitgevoerd, tenzij externe expertise vereist is. DPIA's worden uitgevoerd conform een prioriteringslijst. De lijst wordt periodiek geëvalueerd.
4.5	!	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.	De FG adviseert een applicatie (tooling) waar het register van verwerkingen en andere registraties (onder andere datalekken en verwerkersovereenkomsten) in onder zijn gebracht. De huidige werkwijze voor het register van verwerkingen (halfjaarlijkse uitvraag naar wijzigingen) is ook een passende (basis)maatregel voor onze organisatie. In lijn met het advies van de FG, heeft de gemeente (al eerder) bij de gemeente Alphen aan den Rijn te kennen gegeven graag met deze gemeente mee te onderzoeken of/hoe over te gaan tot aanschaf van een privacy-applicatie. Daarbij gezegd dat onze gemeente de gemeente Alphen aan den Rijn volgt, zover dat op het tempo van aanschaf aankomt. Tot die tijd wordt de huidige werkwijze (halfjaarlijkse uitvraag naar wijzigingen) gehanteerd. Dit conform de visie van de gemeente. In de jaarplanning is opgenomen dat dit jaar wordt nagegaan of tot publicatie van het register van verwerkingen op de website over kan worden gegaan. Bij voorkeur gebeurt dit (geautomatiseerd) als het register van verwerkingen in een applicatie wordt ondergebracht.

4.6		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.	De gemeente maakt nadere afspraken met de Chief Information Security Officer (CISO) over het uitbrengen van een (periodieke) rapportage over informatiebeveiliging. Er is periodiek overleg tussen medewerkers van informatiebeveiliging, privacy en openbare orde & veiligheid, zowel van de gemeente Kaag en Braassem als van de gemeente Alphen aan den Rijn. Dit overleg heeft als doel om (organisatiebreed) cybercrises te voorkomen en te beheersen, en om de continuïteit te borgen.
4.7		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.	Het advies om ook van de laatste verwerkingen in het register van verwerkingen de bewaartermijnen op te nemen en het register ook op dit punt actueel te houden wordt opgevolgd en meegenomen in de eerstvolgende evaluatie van het register.
4.8		Maak het register met verwerkersovereenkomsten compleet en houd het actueel, en voeg ook de onderlinge regelingen en gegevensleveringsovereenkomsten toe. Dit register dient bij voorkeur opgenomen te worden in de eerder geadviseerde applicatie.	Het register met verwerkersovereenkomsten wordt gecompleteerd en actueel gehouden. In de organisatie wordt nogmaals onder de aandacht gebracht dat verwerkersovereenkomsten (en contracten) op een centrale plek beheerd worden (contracten@kaagenbraassem.nl).
4.9		Blijf gebruik maken van de driemaandelijkse memo's om tijdig bij te sturen. Monitor dat de BVO een FG aanwijst. Stel een verbeterplan op naar aanleiding van de resultaten van de Wpg-audit.	Er wordt dankbaar gebruik gemaakt van de driemaandelijkse memo's van de FG. Dit wordt voortgezet. De status over een FG voor de BVO wordt nagegaan bij de BVO. Er wordt gewerkt aan een verbeterplan naar aanleiding van de Wpg-audit.
4.10		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. Het is daarom van groot belang dat dit register zo compleet en actueel mogelijk blijft.	Het belang van een compleet en actueel register wordt onderkend. Het register wordt (conform de huidige werkwijze) actueel en compleet gehouden.

4.11		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.	Er is in 2023 een nieuw datalekkenprotocol vastgesteld. Dit protocol wordt intern uitgedragen en periodiek geëvalueerd, inclusief de werking ervan.
4.12	!	Blijf doorgaan met het vergroten van privacy-bewustzijn. Ga verder met de introductiebijeenkomsten voor nieuwe medewerkers om het draagvlak voor en kennis van de AVG te vergroten. Monitor in 2023 het effect van het nieuwe awareness programma en stuur op deelname.	Samen met de gemeente Alphen aan den Rijn en met de collega's van informatiebeveiliging wordt de komende drie jaren een bewustwordingscampagne op het gebied van privacy en informatiebeveiliging gevoerd. Hierin worden ook nieuwe medewerkers meegenomen. Deze campagne sluit aan bij de visie en doelen van onze gemeente op het gebied van privacy. De campagne wordt periodiek geëvalueerd met de collega's van informatiebeveiliging.