

Management reactie

Doel en verantwoording

De rapportage van de Functionaris Gegevensbescherming in zijn rol als interne toezichthouder AVG is vergezeld van een managementreactie. Deze managementreactie wordt aangeboden door de Concerndirectie aan de portefeuillehouder. De concerndirectie legt in lijn met de privacy governance (zoals vastgelegd in het bestuurlijk privacybeleid) en ambtelijke verantwoordelijkheden hiermee verantwoording af over de maatregelen die zij neemt naar aanleiding van de rapportage van de interne toezichthouder. De portefeuillehouder krijgt daardoor een volledig overzicht van de onafhankelijke adviezen van de toezichthouder en de wijze waarop de concerndirectie deze wil opvolgen.

Het toezichtsplan van de Functionaris Gegevensbescherming omvat een opdeling in deelrapportages. Het advies over het tweede deel is in december aangeboden. Deze omvat onderdelen op het gebied van organisatorische inbedding. Het advies voor het derde deel wordt in nxxx verwacht.

Reactie op gestelde beeld

De concerndirectie merkt op ¹¹⁽¹⁾

. ¹¹⁽¹⁾

Wij zullen daarom met de FG in gesprek gaan om in een volgende rapportage specifieker en feitelijker advies te krijgen opdat wij daar op ook specifiek op kunnen reageren en acteren.

De concerndirectie beseft zich dat voor de gemeentelijke organisatie een groeipad nodig is om het in mei 2018 door het college vastgestelde privacybeleid handen en voeten te geven. In april 2019 heeft de directie met de Privacy Information Officer gesproken over het privacy plan voor 2019. Hierbij is aangegeven dat gezien de huidige veranderopgaven binnen de organisatie de voorkeur uitgaat naar een risicogerichte aanpak, waarbij zoveel mogelijk wordt aangesloten bij reguliere control- en verantwoordingsprocessen.

In de eerste helft van 2019 heeft de nadruk gelegen op het samenstellen van het privacy team en opbouwen van het privacy management (incl. verbetering processen rond privacy verzoeken/klachten). Op speerpunten heeft dit geleid tot het volgende plan voor de 2^{de} helft van 2019:

Privacy plan 2019 - risicogedreven

- Awareness
 - sociaal domein
 - management
- Ontwikkelen beleid en richtlijnen:
 - Beleid voor Onderzoek
 - Anonimiseringsrichtlijn
- Risico management (privacy, informatiebeheer, informatieveiligheid)
 - Mee in P&C processen
- Procesmatig werken
 - Pilots - Privacy by design (aansluiting bij lopende trajecten, o.a. Sociaal Domein)
 - IGO's (basis informatie van processen en eerste inzicht risico's)

Reactie op de adviezen van de FG

De directie stelt mede op basis van advies van de Privacy Information Officer prioriteiten en zal de overige adviezen van de FG (en de komende toezichtsrapportages) waar mogelijk meenemen in privacy plan 2020. Indien adviezen niet worden opgevolgd zal bij het privacy plan 2020 worden aangegeven welke gevolgen en risico's dit heeft voor de organisatie. Op dit moment wordt gewerkt aan de jaarrapportage 2019 en het plan voor 2020.

In onderstaand overzicht wordt een reactie per advies aangegeven en een overzicht van huidige acties.

Onderwerp	Advies uit toezichtsrapportage	Reactie management	Huidige acties
Positionering van de FG, PIO en PC	2.1 ¹¹⁽¹⁾ [Redacted]	Vroegtijdig meenemen van de privacy aspecten bij nieuwe ontwikkelingen rond de verwerking van persoonsgegevens ^{10(2)g} [Redacted] In 2019 is aandacht gegeven aan het ontwikkelen en testen van een aanpak voor Privacy by Design. In 2020 dient te worden gewerkt aan meer bewustwording binnen de organisatie zodat privacy bij design daadwerkelijk wordt toegepast. De ^{10(2)g} en privacycoördinatoren adviseren de organisatie daarbij. Bij risicovolle en/of maatschappelijk gevoelige nieuwe initiatieven worden de noodzakelijke/verplichte	^{10(2)g} [Redacted]

		gegevensbeschermingseffectbeoordeling uitgevoerd. De FG wordt hierbij verplicht om een advies gevraagd zodat de verantwoordelijke een onderbouwd besluit kan nemen.	
	2.2 Het advies is ¹¹⁽¹⁾ [redacted]	Op verschillende wijzen wordt binnen de gemeente ethische discussies gevoerd (bijvoorbeeld Moreel Beraad, toepassing van De Ethische Data Assistent, Datawerkplaats). Privacy dient hierin zeker meegenomen te worden en de ^{10(2)e} zal hierin een rol te krijgen.	
	2.3 Het advies ¹¹⁽¹⁾ [redacted]	In het privacyplan 2020 zal aandacht worden gegeven aan de wijze waarop de aandacht voor privacy en AVG verder wordt versterkt binnen de organisatie. Ten behoeve van de komende jaren zullen we inzichtelijk maken welke structurele inzet nodig is en de middelen die daarbij nodig zijn, mede gebaseerd op de ervaring van het afgelopen jaar.	^{10(2)g} [redacted]
	2.4 Het advies is ¹¹⁽¹⁾ [redacted] AVG.	In 2018 is gekozen voor een FG als toezichthouder en de overige taken bij de ^{10(2)e} belegd. In dat kader zien wij op dit moment geen noodzaak om de capaciteit voor de toezichthoudende taken uit te breiden, wij nemen dit mee bij de bepaling van inzet voor de komende jaren.	
Privacy management verantwoordelijkheid en	2.5 Het advies van de FG is ¹¹⁽¹⁾ [redacted]	Bij het plan 2020 zullen we aangeven wat nodig is om afdelingsmanagers te ondersteunen in die verantwoordelijkheid en de betrokkenheid van de gemeentesecretaris/directie daarbij. De ^{10(2)e} adviseert hierin zowel gemeentesecretaris/directie als afdelingsmanagement.	

	<p>2.6 Het advies van de FG is ¹¹⁽¹⁾ [redacted]</p> <p>[redacted] Bij de verantwoording kan de FG zijn advies toevoegen waardoor er wordt voldaan aan het verantwoordingsbeginsel conform de AVG.</p>	<p>In mei 2018 is het privacybeleid vastgesteld waarin is aangegeven dat het college jaarlijks verantwoording aflegt aan de raad over het gevoerde privacybeleid. Met de portefeuillehouder is eerder dit jaar afgesteld dat dit wordt aangevuld met een jaarlijks overzicht van alle incidenten die gemeld zijn aan de Autoriteit Persoonsgegevens.</p>	<p>Opstellen jaarverslag door PIO en goedkeuring door conerndirectie.</p>
Organisatieverantwoordingen	<p>2.7 Het advies van de FG is ¹¹⁽¹⁾ [redacted]</p> <p>[redacted]</p>	<p>In onze reactie op de 1^e toezichtsrapportage is aangegeven dat ¹¹⁽¹⁾ [redacted] Bij eventuele nieuwe besluiten over gemandateerde verwerkingen dient dit wel te worden meegenomen. Bij het opstellen van het privacyplan 2020 wordt opnieuw bepaald waaraan prioriteit dient te worden gegeven.</p>	<p>^{10(2)g} [redacted]</p>
Processen en autorisaties	<p>2.8 De FG adviseert ¹¹⁽¹⁾ [redacted]</p> <p>[redacted]</p>	<p>Afdelingsmanagers/proceseigenaren zijn verantwoordelijk voor correcte autorisaties. In het afgelopen jaar is de gemeente overgegaan naar Rol Based Access Control. Vanuit ICTAR wordt gekeken op welke wijze de afdelingsmanagers hierin ondersteund kunnen worden. Middels een audit dient te worden bepaald of de implementatie van RBAC die privacy voldoende waarborgt.</p> <p>^{10(1)b, 10(2)g} [redacted]</p> <p>[redacted] ^{10(1)b, 10(2)g} [redacted]</p>	<p>^{10(2)g} [redacted]</p> <p>[redacted] ^{10(2)g} [redacted]</p>

	<p>2.9 Het advies van de FG is ¹¹⁽¹⁾ [redacted]</p> <p>[redacted]</p>	<p>De gemeente brede observaties van de FG ¹¹⁽¹⁾ [redacted]</p> <p>[redacted] 10(1)b, 10(2)g [redacted]</p> <p>[redacted] 10(1)b, 10(2)g [redacted]</p>	<p>We brengen in kaart welke bedrijfsprocessen hier door de FG worden bedoeld.</p>
Privacy en medewerkers	<p>2.10 Het advies van de FG is ¹¹⁽¹⁾ [redacted]</p> <p>[redacted]</p>	<p>Het advies om ¹¹⁽¹⁾ [redacted] nemen wij niet over.</p> <p>Naar onze mening is ¹¹⁽¹⁾ [redacted]</p> <p>[redacted]</p> <p>[redacted] Daarnaast zijn bewustwording en het toezien op het correct omgaan met privacy belangrijk; werkinstructies kunnen daarbij eveneens behulpzaam zijn.</p>	
	<p>2.11 Het advies van de FG ¹¹⁽¹⁾ [redacted]</p> <p>[redacted]</p>	<p>Dit advies zal worden gedeeld met de verantwoordelijke afdelingsmanager.</p>	<p>In 2020 is inhoudelijke toetsing van het personeelshandboek gepland.</p>
	<p>2.12 De FG ¹¹⁽¹⁾ [redacted]</p> <p>[redacted]</p> <p>[redacted] Voldoen aan de bescherming van gevoelige persoonsinformatie vraagt van medewerkers bewustwording en actief handelingsgedrag.</p>	<p>Opleiding en bewustwordingsprogramma's van GA medewerkers is een belangrijk programma onderdeel van informatiebeveiliging en privacy.</p> <p>^{10(1)b, 10(2)g} [redacted]</p>	<p>Onderzoeken of en zo ja in welke mate ^{10(2)g} [redacted] erplicht gesteld kunnen worden van GA medewerkers</p>

--	--	--	--

Tot slot

Wij zien een verhoogde aandacht voor het onderwerp privacy binnen de gemeente. Het privacy team wordt steeds vaker benaderd voor incidentele adviezen van het gebruik van foto's tot het selecteren en implementeren van nieuwe systemen in lijn met het privacybeleid. Sinds de zomer is het privacy team volledig ingevuld en worden samen met de afdelingen afspraken gemaakt om het privacybeleid verder te implementeren binnen de verschillende afdelingen. Hierbij krijgt bewustwording de eerste prioriteit.

Het privacy team is daarnaast actief bij de afhandeling van inbreuken ivm persoonsgegevens (datalekken), privacyverzoeken en privacyklachten. Deze geven inzichten in de risico's binnen de organisatie en mogelijkheden voor verbetering. Dit zal in de jaarrapportage van 2019 en het plan voor 2020 verder worden toegelicht.