

MANAGEMENTREACTIE
OP DE TOEZICHTSRAPPORTAGE Q2 2021

Beleidsnotitie

Gemeente Almere



Versie en status	2.1 (let op: aanvulling start op pagina 4, inclusief reacties afdelingen)
Datum	10 september 2021
Opdrachtgever	Gemeente Almere
Team/taakveld	CIO Office / Privacy
Auteur	10 (2) e
Versie geschiedenis	1.0 besproken op 9 juli 2021

INLEIDING

Doel en verantwoording

De Functionaris Gegevensbescherming levert in zijn rol als interne toezichthouder een rapportage af aan de portefeuillehouder. De concerndirectie geeft middels deze managementreactie aan op welke wijze zij aan de adviezen van de FG opvolging gaat geven. 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.

Vanaf dit jaar voert Team Audit het onderzoek uit binnen de ambtelijke organisatie en verstrekt aan de FG een rapport met daarin de resultaten. Voor dit tweede rapport zijn 5 afdelingen bevraagd, daarnaast zijn de FG, Privacy Coördinatoren (PC) en ^{10(2)e} bevraagd. Aanvullend heeft men documenten beoordeeld om het bestaan ervan vast te stellen. Op basis van deze uitkomsten is de Toezichtsrapportage Q2 2021 door de FG opgesteld.

De afdelingen zijn tevens bevraagd over het onderwerp 'beleid en processen', dat het onderwerp was van de eerste audit. De FG heeft hiervoor geen aanvullende adviezen opgesteld.

De toezichtsrapportage is door de Functionaris Gegevensbescherming toegelicht op 3 juni in een gesprek met de gemeentesecretaris, concerncontroller en Privacy Information Officer. De teammanager audit&risk was verhinderd.

Managementreactie

Achtergrond

In 2019 heeft de directie aangegeven dat, ^{10(2)g, 11(1)} ^{10(2)e} e directie stelt mede op basis van advies van de prioriteiten, deze hebben in 2019 geleid tot een privacyplan.

De directie beseft zich ^{10(2)g, 11(1)} In 2020 is er, mede als gevolg van het Corona-virus veel druk geweest op de organisatie, zowel organisatiebreed als specifiek voor de privacy functie.

In het eerste kwartaal van 2021 is geconcludeerd, mede op basis van eerdere toezichtsrapportages van de FG, ^{10(2)g, 11(1)}

Op basis van het privacyplan voor 2021-2022 is hiervoor dekking opgenomen in de perspectiefnota. Dit plan is mede gebaseerd op eerdere toezichtsrapportages van de FG. ^{10(2)g, 11(1)} Vooruitlopend daarop heeft de gemeentesecretaris budget beschikbaar gemaakt om de voorbereidingen reeds in Q2 op te starten.

Reactie op beeld van FG over status privacy

De directie herkent het beeld dat de FG geeft en onderschrijft de bijbehorende adviezen. ^{10(2)g, 11(1)}

Dit wordt besproken met de afdelingsmanager. De afdelingsmanagers zijn zelf ook verantwoordelijk voor de beantwoording van deze audit, dit wordt meegenomen in de gesprekken met de 5 betrokken afdelingsmanagers.

De directie heeft gekozen voor een aanpak die (waar mogelijk) aansluit bij het programma Verbetering Informatiebeheer en Archivering (VIA).

De verantwoordelijkheid voor privacy ligt bij het afdelingsmanagement, door een (uitgebreid) privacyteam worden zij ondersteunt om concreet aan de slag gaan. Vooruitlopend op de dekking via de perspectiefnota zijn de eerste stappen genomen:

- werving gestart (intern/extern) van uitbreiding van het privacyteam met ^{10(2)g}
- eerste afdelingen zijn gestart met opstellen afdelingsprivacyplan op basis van template en met ondersteuning van privacycoördinator

Randvoorwaarde voor het slagen van het privacyplan is dat het afdelingsmanagement hiervoor zijn verantwoordelijkheid neemt en menskracht beschikbaar stelt. De directie zal meer aandacht en prioriteit vragen bij het afdelingsmanagement voor het privacybeleid en bijbehorende processen. ¹¹⁽¹⁾

Hierdoor krijgt het onderwerp privacy in de afdelingen onvoldoende aandacht, daar waar de verantwoording wel ligt.

De gemeentesecretaris zal met de ¹⁰⁽²⁾ (en eventuele ondersteuning van de FG) ^{10(2)g, 11(1)} bij het afdelingsmanagement in een kick-off sessie. Het is noodzakelijk zij hun verantwoordelijkheid nemen.

Via het privacyplan faciliteren ^{10(2)g}

aar waar het wringt binnen afdelingen met andere ambities zal dit bespreekbaar moeten worden met directie en college.

Naast het concernplan, dienen de afdelingen zelf ook afdelingsprivacyplannen op te stellen. Hierbij is de ¹⁰⁽²⁾ gevraagd om met een paar afdelingen als voortrekker te starten. De aanpak die daarbij wordt gehanteerd is het combineren van een algemene privacy bewustwording campagne met een meer op de betreffende afdeling toegesneden actieprogramma.

De directie heeft verzocht om te onderzoeken of het mogelijk is om ook beelden op afdelingsniveau te bepalen, of mogelijkheden te geven voor zelf-reviews. De voortgang op het privacyplan zal afdelingssspecifiek worden meegegeven in de volgende kwartalen.

Management reactie directie (aanvulling)

De directie ^{10(2)g}

^{10(2)g} We hebben daarom een informatiebijeenkomst georganiseerd onder leiding van de FG en de ^{10(2)g} voor alle afdelingsmanagers wat tot de eerste reacties heeft geleid. De privacy coördinatoren stappen daarnaast actief op afdelingen af om hen te helpen bij hun verantwoordelijkheden. Met een 5-tal afdelingen zijn we gestart met het opstellen van een afdelingsprivacyplan. De eerste activiteiten zijn opgestart, met name rond de Information Governance Overzichten in samenwerking met het programma VIA. Het uitgewerkt privacyplan met meetbare doelstellingen wordt begin oktober opgeleverd.

Status privacyplan (aanvulling)

Ter ondersteuning is voor de komende anderhalve jaar een projectleider aangetrokken, zij werkt het privacyplan uit en zorgt voor meetbare doelstellingen. Het privacyteam is inmiddels verder uitgebreid met ^{10(2)g}. Verdere werving wordt deze maand opgestart, deels zal dit met externe inhuur worden ingevuld.

Samen met de privacycoördinatoren zijn inmiddels 5 afdelingen gestart met het opstellen van een afdelingsprivacyplan. Met de overige afdelingen wordt gestart in de periode tot 1 november. Een aantal afdelingen hebben hun zorg geuit over de verschillende activiteiten de komende periode: het programma VIA, de invoering van MS teams, het programma Digivaardig en de activiteiten vanuit het privacyplan.

Vanuit het programma Digivaardig wordt vanaf eind september de verplichte module “Beschermen” over AVG en privacy aangeboden. Deze module dient door alle medewerkers te zijn gevolgd uiterlijk in Q1 2022. ^{10(2)g}

^{10(2)g} Vanuit informatiebeheer, privacy en informatieveiligheid wordt gewerkt aan een toelichting op de verantwoordelijkheden van afdelingsmanagers en proceseigenaren. De verantwoordelijkheden op het gebied van privacy worden op hoofdlijnen ook meegenomen in een specifiek hoofdstuk in de module “Beschermen” van het programma Digivaardig.

De portefeuillehouder, directie en FG hebben aangegeven dat inzicht in de volwassenheid en de risico's op afdelingsniveau wenselijk is. Onderzocht wordt of een beeld op afdelingsniveau van de risico's en ontwikkelingen rond privacy (evenals informatiebeheer en informatieveiligheid) kunnen worden meegenomen in de bedrijfsvoeringsmonitor op basis van een beperkt aantal KPI's.

In samenwerking met het programma VIA komt een informatiesessie voor de afdelingen in september over de Information Governance Overzichten (IGO's) ^{10(2)g}

^{10(2)g} Multidisciplinaire teams gaan vervolgens met de afdelingen deze IGO's verder invullen, hiervoor worden resources vanuit het privacyplan beschikbaar gesteld. Vanuit VIA zijn hiervoor geen verdere resources beschikbaar.

Vervolg toezichtsrapportages (aanvulling)

In het proces rond de toezichtsrapportages is een extra processtap toegevoegd waarin de betrokken 5 afdelingen om een reactie wordt gevraagd alvorens de rapportage wordt besproken met de directie en portefeuillehouder.

Alle managers ontvangen de toezichtsrapportages en de management reactie na bespreking met de portefeuillehouder.

Management reacties (aanvulling)

De afdelingsmanagers van de 5 afdelingen is verzocht een management reactie op te stellen, nav de toezichtsrapportage van de FG. ^{10(2)g} hebben deze management reactie opgeleverd, deze zijn als bijlage toegevoegd. ^{10(2)g} hebben (tot op heden) geen management reactie opgeleverd.

Management reactie ^{10(2)g}

Wij zijn uiteraard blij met het gegeven dat wij als ^{10(2)g} voorop lopen in de organisatie. Wij zijn ons terdege bewust van de vele persoonsgegevens die wij beheren en verwerken en willen deze met de grootst mogelijke zorgvuldigheid behandelen. Ondanks dat we er relatief goed voor staan, willen wij graag verder groeien in ons privacybewustzijn. Wij streven ernaar niet alleen voorop te lopen, maar ook te voldoen aan alle richtlijnen die wij nodig achten voor een goede bescherming van de privacy. Waar we uiteindelijk naar toe willen groeien, is een situatie waarin we als vanzelfsprekend de bedoeling van de privacywetgeving volgen. Om daar te komen, zijn een aantal dingen nodig. Het eerste is een goede ondersteuning vanuit FG/^{10(2)e} en vanuit een privacy coördinator met wie we een concreet plan voor de komende jaren kunnen opstellen. Ten tweede is dat een regelmatige presentatie of andere activiteit waarbij (een aspect van) privacy toegelicht en besproken wordt. Ten derde is het tijd, omdat het tijd kost dit soort zaken in een werkwijze te slijten. Kortom, onze afdeling is zeker bewust van haar eigen rol op het gebied van privacy en tegelijkertijd houden wij ook een pleidooi voor een goede centraal georganiseerde facilitering.

Wat ons verder nog opvalt aan de rapportages is ^{10(2)g, 11(1)}

^{10(2)g, 11(1)}

Management reactie ^{10(2)g}

Het MT-^{10(2)g} kan zich vinden in de adviezen van de FG over ^{10(2)g}. Voor een aantal adviezen geldt dat wij al maatregelen hadden getroffen. Maar wellicht is verdere doorontwikkeling mogelijk. Daarover gaan wij graag in gesprek met de FG. Het gaat hierbij met name om het volgende.

- Uit het rapport van de FG ^{10(2)g, 11(1)}

^{10(2)g, 11(1)}

<sup>10(2)10(2)
11(1g,
11(1)
11</sup>

- In het onboardingproces van nieuwe medewerkers wordt behandeld hoe verantwoord om te gaan met persoonsgegevens en vertrouwelijke informatie. Ook in het Personeelshandboek wordt hier aandacht aan besteed.
- Het belang van het op een verantwoordelijke manier omgaan met persoonsgegevens wordt behandeld in de door HRM georganiseerde digivaardigheidstrainingen. Deze trainingen worden dit najaar gegeven.

De verdere adviezen van de FG nemen wij mee bij de uitwerking van het privacyplan voor de afdeling HRM, dat we in november klaar willen hebben. Doel is om de AVG-aandachtspunten in onze werkprocessen scherper in beeld te krijgen. Zodoende kunnen we beter gerichte maatregelen treffen om onze werkprocessen te laten voldoen aan de AVG.

Tot slot hebben we het advies overgenomen om voor de afdeling HRM een privacy aanspreekpunten (PA) in te stellen. Vanuit het MT is teammanager ^{10(2)e} hiervoor nu verantwoordelijk. Het inhoudelijk aanspreekpunt is senior beleidsadviseur ^{10(2)e} ^{10(2)e}

Managementreactie ^{10(2)g}

De afdeling ^{10(2)g} is zich ervan bewust om de privacycoördinator/^{10(2)e}/FG om tijdig advies te vragen, zodra er sprake is van vraagstukken met betrekking tot de bescherming van persoonsgegevens. Hierbij moet worden gedacht aan vraagstukken op het gebied van technische en functionele autorisaties, datasecurity, datadistributie, etc.

Binnen de afdeling ^{10(2)g} is een teammanager aangesteld als aanspreekpunt. Het aanspreekpunt coördineert de activiteiten op het gebied van privacyvraagstukken. Er wordt in de komende periode meer aandacht besteed aan interne communicatie, zodat alle medewerkers binnen ^{10(2)g} op de hoogte zijn waar zij terecht kunnen met hun vragen, etc. op het gebied van privacy. Het aanspreekpunt beschikt over meer dan gemiddelde kennis van de AVG en de daarmee samenhangende richtlijnen.

^{10(2)g, 11(1)}

Dit wordt als onderdeel opgenomen in het privacyplan van de afdeling ICTAR, welke in samenwerking met de privacycoördinator wordt opgesteld.

^{10(2)g, 11(1)}

zal als onderdeel worden opgenomen in het privacyplan van de afdeling ICTAR. Het aanspreekpunt heeft zich ten doel gesteld om daar waar nodig deze wettelijke verplichting op te nemen in de werkprocessen.

^{10(2)g, 11(1)}

Gelet op de vele prioritaire opgaven waarmee ^{10(2)g} is en wordt geconfronteerd moet nog wel vastgesteld worden wanneer een dergelijke toetsing kan gaan starten.

Managementreactie ^{10(2)g}

De afdeling ^{10(2)g} beschikt over een grote hoeveelheid privacy gevoelige gegevens. We bewaken de privacy via geheimhoudingsverklaringen, logboeken en autorisatieschema's. Elke medewerker van W&I is zich bewust van het belang van privacy en de beveiliging van persoonsgegevens.

^{10(2)g, 11(1)}

^{10(2)g, 11(1)}

^{10(2)g, 11(1)}

Alle kennis zit centraal. De FG heeft ^{10(2)g, 11(1)}

^{10(2)g, 11(1)}

10(2)g, 11(1)

In verschillende overleggen komen diverse technische termen tevoorschijn waar nog niemand binnen 10(2)g van gehoord heeft zoals de DPIA. Tegelijkertijd wordt de verbinding met het project VIA nu wel deels gelegd maar lijkt meer mogelijk.

10(2)g

. Dat komt omdat voor de maanden oktober en november diverse concernbrede activiteiten op stapel staan: invoering MS Teams, opleiding Privacy, uitvoering verbeterprogramma VIA, Digitaal vaardig, teams meenemen in veranderspoor 2 en het nadere MTO. 10(2)g, 11(1)

11(1)

Privacy wordt een steeds groter item en wordt van een steeds groter belang in dit digitale tijdperk. Een investering per afdeling is onvermijdelijk anders 10(2)g, 11(1) 11(1)

Nog een kanttekening bij de uitgevoerde audit. 10(2)g, 11(1)

Veel zaken hebben we wel geregeld 10(2)g, 11(1) De vraag is dan gerechtvaardigd of een verklaring van een procesverantwoordelijke ook niet zou kunnen voldoen. 11(1)

11(1)

Wij zullen zelf de uitkomsten nog gaan evalueren en beoordelen waar we, gegeven de beperkte tijd, nog stappen in kunnen zetten.

11(1)

Managementreactie 10(2)g

Algemeen

10(2)g

Wij willen daarbij graag gebruik maken van de handreikingen die vanuit het concern worden gedaan, bijvoorbeeld in de vorm van een format voor een privacy-afdelingsplan, bijbehorende adviezen aan onze afdeling, beschikbaarheid van expertise en capaciteit, en voorlichtingsbijeenkomsten.

Awareness en privacy-ambassadeur

In de afgelopen 2 jaar hebben wij in de afdeling 10(2)g ingezet op 'awareness'. We hebben workshops georganiseerd voor alle medewerkers. Daaruit hebben we de belangrijkste vragen van onze medewerkers en de belangrijkste verbeterpunten gestedilleerd. Quick wins hebben we opgepakt. Verder hebben wij één van onze MT-leden aangewezen als privacy-ambassadeur. Niet zozeer om aanspreekpunt te zijn voor de hele afdeling, maar wel om het onderwerp regelmatig op de MT-agenda te zetten en te organiseren dat de meest urgente zaken kunnen worden opgepakt. Een privacy-aanspreekpunt, zoals de FG in het advies benoemt, hebben wij in onze afdeling nog niet. 10(2)g, 11(1)

Indien conform advies 3.2 van de FG een praktische training wordt georganiseerd, zullen wij daaraan één van onze kwaliteitsadviseurs en/of een senior-consulent laten deelnemen.

Aansluiten op concernbreed privacyplan

Wij onderschrijven de boodschap van de FG ^{10(2)g, 11(1)}

^{11(1), 10(2)g}

We zullen dit stap voor stap moeten doen. Van het concern vragen wij daarbij om meer duidelijkheid over de voorgenomen stappen en prioritering, de planning, en de beschikbare expertise en ondersteuning die is aangekondigd. Op basis daarvan willen wij komen tot realistische afspraken voor 2022 e.v.