



## Advies van de FG naar aanleiding van het periodiek onderzoek

### Eerste periode 2019

P.M.H. Korremans - Functionaris Gegevensbescherming

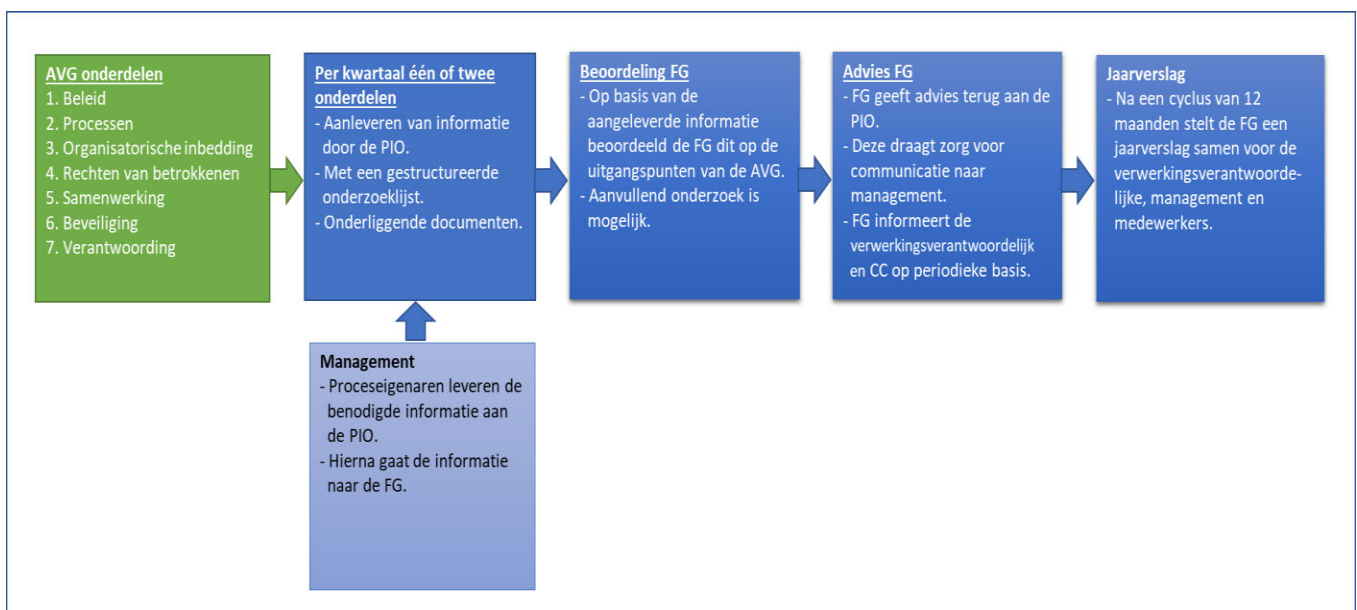
11 oktober 2019

### Inleiding

De Algemene Verordening Gegevensbescherming (AVG) die medio 2018 is ingevoerd geeft regels ter bescherming van persoonsgegevens. Het verplicht de organisatie om aantoonbaar 'in control' te zijn ten aanzien van alle wettelijke beginselen van de AVG.

De organisatie dient zorgvuldig om te gaan met persoonsgegevens. De organisatie verwerkt immers bij de uitoefening van haar taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties. In de AVG wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de organisatie transparant te zijn welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan strikt noodzakelijk. Bovendien dient de organisatie passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot persoonsgegevens tegen te gaan en daardoor onrechtmatig gebruik van persoonsgegevens te voorkomen. Daarnaast heeft de organisatie ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van de gemeentelijke organisatie.

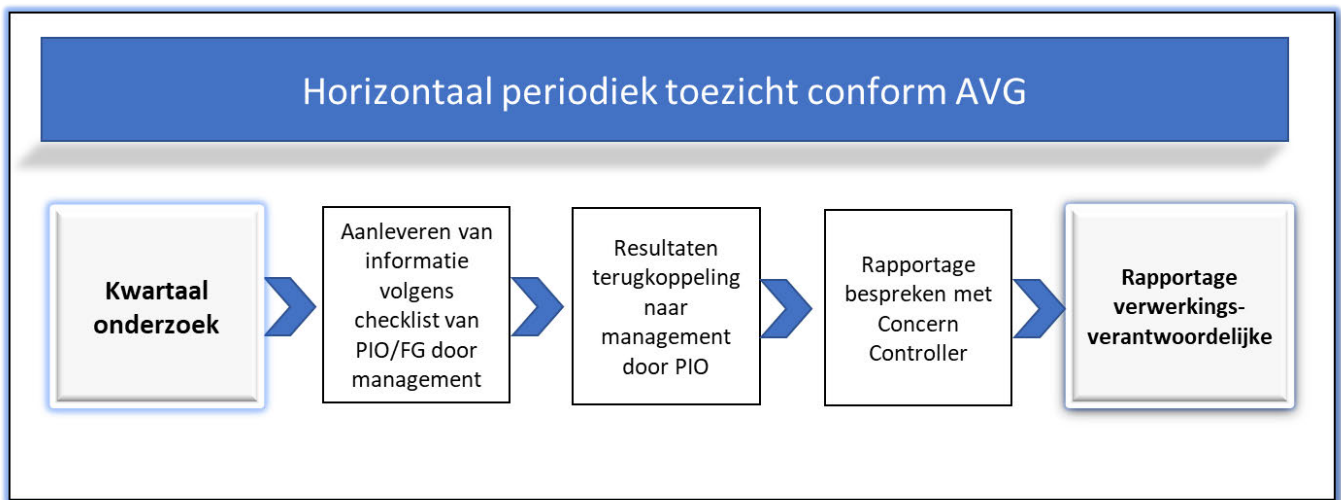
Onder de verantwoordelijkheid van het college van Burgemeester en Wethouders vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om persoonsgegevens van eigen inwoners, inwoners van andere gemeenten, zakenrelaties, medewerkers en externen. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Intern houdt de Functionaris Gegevensbescherming (FG) toezicht op de naleving van de AVG.





## Horizontaal toezicht

De AVG geeft de kaders aan op welke onderdelen het toezicht dient plaats te vinden. De organisatie voert in een cyclus van 12 maanden dit toezicht uit. Per kwartaal wordt dit onderzoek op onderdelen uitgevoerd en voorzien van een advies door de FG. De directie en de verwerkingsverantwoordelijke worden na afloop van ieder kwartaal geadviseerd door de <sup>10(2)</sup>e en de FG. Met deze aanpak voldoet de organisatie aan haar wettelijke verplichting om onderzoek uit te voeren inzake de Algemene Verordening Gegevensbescherming.



## Het toezicht omvat de volgende onderdelen:

- Beleid
- Processen
- Organisatorische inbedding
- Rechten van betrokkenen
- Samenwerking
- Beveiliging
- Verantwoording

## Werkwijze

De <sup>10(2)</sup>e heeft in samenspraak met de Functionaris Gegevensbescherming (FG) een lijst met vragen opgesteld die betrekking heeft op de bovengenoemde AVG onderdelen. Deze wordt door de <sup>10(2)</sup>e samen met de Privacy Coördinatoren (PC) en het management besproken, ingevuld en voorzien van een toelichting. Op basis van de antwoorden en een toelichting beoordeelt de FG deze en voorziet het van een advies. Dit advies wordt verwerkt in een rapport en besproken in het directieoverleg en vervolgens met de verwerkersverantwoordelijke tijdens het kwartaaloverleg waar ook Concern Control aanwezig is. De verwerkingsverantwoordelijke (portefeuillehouder) en de directie kunnen dit advies verder bespreken met College, de Directie, de procesverantwoordelijke en de medewerkers.



### Onderzoekresultaten

Als eerste zijn het privacybeleid en de processen beoordeeld binnen de organisatie. Aan de hand van een 50-tal vragen heeft er een inventarisatie plaatsgevonden in hoeverre de organisatie voldoet aan de AVG. In de afgelopen periode is de organisatorische inbedding beoordeeld aan de hand van een 70-tal vragen. Op een aantal gebieden voldoet de organisatie aan de AVG, maar er zijn een aantal gebieden die meer aandacht vragen vanuit de organisatie.

In zijn algemeenheid kan worden gesteld dat de gemeentelijke organisatie dermate complex is qua verwerking van persoonsgegevens dat zij nog niet kan voldoen aan alle verplichtingen van de AVG. In de afgelopen jaren is er veel werk verzet om zorg te dragen voor een professionele ondersteuning van de organisatie. Het hieronder staande model laat zien dat er een groei kan worden gerealiseerd van een 'informeel' naar een 'geoptimaliseerd' niveau. Op dit moment bevindt de organisatie zich op niveau 2 en zal de komende jaren aan haar volwassenheid moeten werken door het nemen van maatregelen.

Het voorliggende Privacy Volwassenheidsmodel heeft gebruik gemaakt van CMMI én ISOMM



### Advies op de verschillende onderdelen

#### Privacybeleid

De organisatie beschikt over een privacybeleid dat is bekrachtigd door de directie en het college van B&W. Dit beleid heeft een hoog ambitie niveau dat zelfs verder reikt dan de wettelijke AVG verplichtingen. Het beschreven beleid geeft bijzonder goed aan welke maatregelen noodzakelijk zijn om te voldoen aan de uitgangspunten van de AVG.

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

[Redacted text block]

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

<sup>11(1)</sup>

[Redacted text block]



Op het gebied van privacy bewustwording zijn er de afgelopen jaren verschillende bijeenkomsten gehouden. <sup>10(2)g, 11(1)</sup>

[Redacted text]

11(1)

[Redacted text]

Voor de komende jaren heeft de organisatie een budget vastgesteld voor het ondersteunen van proceseigenaren en het verplichte toezicht op het privacybeleid. <sup>10(2)g, 11(1)</sup>

[Redacted text]

### Processen

Het verwerkingsregister is aanwezig en hiermee voldoet de organisatie aan de AVG verplichting. Met veel inzet is dit register tot stand gekomen voor 25 mei 2018. Het register is <sup>10(2)g, 11(1)</sup>

[Redacted text] De FG adviseert <sup>10(2)g, 11(1)</sup>

[Redacted text]

11(1)

[Redacted text]

Het register wordt ook gepubliceerd zodat burgers kennis kunnen nemen van alle processen die de organisatie uitvoert. Hiervoor is het Excel overzicht in PDF vorm op de website van de gemeente Almere geplaatst. <sup>10(2)g, 11(1)</sup>

[Redacted text] Dit laatste is overigens geen verplichting!

Onder mandaat worden door derde partijen verwerkingen van persoonsgegevens uitgevoerd. Hiervoor worden mandaatsbesluiten genomen door de verwerkingsverantwoordelijke waardoor er rechtmatig processen door derden kunnen worden uitgevoerd. <sup>10(2)g, 11(1)</sup>

[Redacted text]

11(1)

De organisatie verwerkt persoonsgegevens op basis van een wettelijke grondslag. Verwerkingen vinden veelal plaats in het kader van een wettelijke taak die de organisatie uitvoert. Het doel van een verwerking ligt vast en deze kan alleen doorbroken worden indien er een nieuw doel wordt vastgesteld met daarbij een wettelijke grondslag waarop de verwerking kan plaatsvinden.

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

[Redacted text]



11(1)

Het verzamelen van persoonsgegevens dient volgens de AVG proportioneel te zijn. Hiermee wordt voorkomen dat er bovenmatig gegevens worden verzameld. Bij het uitvoeren van de wettelijke taken hebben de medewerkers een grote mate van verantwoordelijkheid om niet meer dan noodzakelijk gegevens te verwerken waarmee de risico's op inbreuken op de privacy minimaal zijn. In een aantal domeinen worden grote hoeveelheden bijzondere persoonsgegevens verwerkt. Dit is noodzakelijk voor het uitvoeren van de taken, <sup>10(2)g, 11(1)</sup>

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

11(1)

Hiernaast is het van belang dat persoonsgegevens niet langer worden bewaard dan strikt noodzakelijk. Op dit punt is de bewaartermijn essentieel. Uit een eerder onderzoek door de FG <sup>10(2)</sup>

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

11(1)

Op het moment dat de organisatie (management) overweegt om nieuwe processen, software en/of gebruik van nieuwe technologieën te gaan toepassen, is er een verplichting vanuit de AVG om de risico's van de betrokkenen (burgers) in kaart te brengen en beschermde maatregelen te nemen. Het is een verplichting om 'Privacy by Design (PbD)' toe te passen. Een methode en ervaring is beschikbaar voor de organisatie.

De FG constateert dat <sup>10(2)g, 11(1)</sup>

11(1)

In het privacybeleid is opgenomen dat er van alle bestaande verwerkingen met een hoge impact een Data Protection Impact Assessment (DPIA) wordt gemaakt. Deze risico-inventarisatie is een verplichting vanuit de AVG waarmee wordt bereikt dat een bestaande verwerking periodiek wordt

10(2)g, 11(1)

10(2)g, 11(1)

[illegible]

10(2)g, 11(1)