INFORMATIE
BEVEILIGINGS
DIENST

Handreiking

Positionering en taken van de FG

Versiebeheer

Versie	Wijzigingen	Datum
1.13	Definitieve eerste versie	Juni 2018
2.0	Omgezet naar IBD format	Mei 2019
2.1	Kleine aanpassingen	December 2019
2.2	Handreikingen positionering FG en handreiking rol en taken FG samengevoegd. Gerelateerde producten, BIO-controls en controls uit het AVG borgingsproduct toegevoegd. Inhoudelijke aanpassingen.	Juni 2020

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Gerelateerde producten en AVG borgingsproduct- en BIO controls

Dit product is gerelateerd aan:

- Handreiking IB-functieprofiel Chief Information Security Officer (CISO) BIO
- Voorbeeld jaarrapportage FG – College van B&W
- Voorbeeld jaarrapportage FG – Gemeenteraad

Dit product is gerelateerd aan de volgende AVG borgingsproduct-controls:

- Processen: 2 en 3 (register van verwerkingsactiviteiten); 11 t/m 14 (DPIA)
- Organisatorische inbedding: 1 (FG aangesteld), 12.4 (FG advies vragen bij bewustwording)
- Rechten van betrokkenen: 1.3 (contactgegevens FG)
- Beveiliging: 3.4 (FG betrokken bij IB-beleid)
- Verantwoording: 7.1 (FG doet periodiek verslag)

Dit product is gerelateerd aan de volgende BIO-controls:

- 18.1.4.1: iedere organisatie heeft een FG

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Inhoudsopgave

1. Inleiding

1.1 Doel en doelgroep

Het doel van deze handreiking is een handvat te bieden bij de aanwijzing en positionering van de Functionaris voor de Gegevensbescherming (**FG**) binnen gemeenten en meer duidelijkheid te bieden over de taken van deze FG. Hoe verhoudt de FG zich tot de rest van de organisatie? Hoe en met wie werkt de FG samen? Waar verschilt de positie van de FG met die van de Chief Information Security Office (**CISO**) en Privacy Officer (**PO**)? En welke taken heeft de FG? Op deze en andere vragen biedt deze handreiking antwoorden.

De doelgroep van deze handreiking is het college van burgemeester en wethouders (**het college van B&W**), de gemeenteraad, de hoogste leidinggevende, het management, de FG, PO en andere privacy adviseurs en functionarissen.
Daarnaast is deze handreiking bedoeld voor de FG zelf om zo meer duidelijkheid te verschaffen over zijn positionering en taken in de gemeentelijke organisatie.

Wij wijzen erop dat dit slechts een handreiking op hoofdlijnen is, omdat iedere gemeentelijke organisatie weer anders is ingericht.

1.2 Onderwerpen handreiking

De handreiking bestaat uit twee delen. Het eerste deel gaat over de positionering van de FG (hoofdstuk 2) en het tweede deel over de taken van de FG, de rolverdeling tussen de FG, CISO en PO en ten slotte komen de kennis en vaardigheden van de FG aan de orde (hoofdstuk 3).

2. Positionering van de FG

2.1 Aanwijzing FG

De Algemene Verordening Gegevensbescherming (**AVG**) verplicht de bestuursorganen van gemeenten en gemeentelijke samenwerkingsverbanden om een FG aan te stellen als zij verwerker of verwerkingsverantwoordelijke zijn. Dit zijn bijvoorbeeld de burgemeester, het college van B&W, de gemeenteraad en de rekenkamer.

De gemeentelijke verwerkingsverantwoordelijken en verwerkers hebben de keuze om ieder een eigen of gezamenlijk een FG aan te stellen. Het is raadzaam dat alle gemeenteorganen binnen een gemeente gezamenlijk één FG aanstellen. Dit omdat de verwerkingen van persoonsgegevens van deze organen in hoge mate verweven zijn.

Ook kunnen verschillende (regio)gemeenten ervoor kiezen om gezamenlijk één FG aan te stellen. Het college van B&W zal over het algemeen het voortouw nemen bij de aanstelling van een gezamenlijke FG voor bestuursorganen binnen één gemeente.

Binnen samenwerkingsverbanden met verschillende gemeenten dient eerst bepaald te worden of aanwijzing van een eigen FG voor het samenwerkingsverband vereist is. Dat is het geval wanneer het samenwerkingsverband verwerkingsverantwoordelijke of verwerker is. Vervolgens wordt vaak de FG van één van de deelnemende gemeenten aangesteld als FG van het samenwerkingsverband. Dit heeft tot voordeel dat verschil van mening tussen FGs voorkomen wordt en er dus makkelijker beslissingen gemaakt kunnen worden. Denk aan de beslissing of het nodig is om een datalek te melden bij de AP of de betrokkene(n).

De voorwaarde voor een gezamenlijke FG is dat deze persoon goed bereikbaar is vanuit elk deel van de organisatie en daadwerkelijk in staat is om de wettelijke taken van een FG in de praktijk uit te voeren. Het is dus belangrijk dat een FG eerst wordt gevraagd of hij beschikbaar is voor de rol voordat hij als FG wordt toegevoegd.

Wanneer de gemeentelijke verwerkingsverantwoordelijke(n) overheidstaken uitbesteden aan

privaatrechtelijke organisaties wordt het aanwijzen van een FG aangeraden (hoewel er in dat geval geen verplichting tot aanwijzing bestaat op grond van de AVG).

2.2 Plichten van de verwerkingsverantwoordelijke

De FG moet niet vereenzelvigd worden met de verwerkingsverantwoordelijke of de verwerker. De verwerkingsverantwoordelijke en de verwerker blijven verantwoordelijk voor de naleving van de verplichtingen op grond van de AVG, niet de FG.[1] De FG dient adviserend op te treden ten aanzien van de verwerkingsverantwoordelijke, maar is niet medeverantwoordelijk voor de eindbeslissing van de verwerkingsverantwoordelijke.

De verwerkingsverantwoordelijke heeft op grond van de AVG ook verplichtingen in relatie tot (de positie en taken van) de FG. De belangrijkste verplichtingen zijn:

1. Waarborgen autonomie en onafhankelijkheid van de FG
2. Betrekken van de FG bij privacy aangelegenheden
3. Ondersteuning bieden en middelen verschaffen aan de FG

2.2.1 Waarborgen autonomie en onafhankelijkheid

De FG dient autonoom in onafhankelijkheid zijn werkzaamheden uit te kunnen voeren. Daartoe zijn de volgende zaken van belang:

- **Geen instructies**. De FG mag geen instructies ontvangen vanuit de gemeentelijke organisatie over de manier waarop hij zijn taken moet uitvoeren. De FG rapporteert rechtstreeks aan het hoogst leidinggevende niveau van de gemeente, zodat het voor het hoogste management (gevraagd en ongevraagd) duidelijk is wat de staat is van de bescherming van persoonsgegevens bij de betreffende gemeente.

- **Geen belangenconflict**. De FG mag ook geen taken of plichten mag uitvoeren die strijdig zijn met zijn taken . Zo mag een FG geen taken hebben waarbij hij het doel en middelen van de gegevensverwerking bepaalt of waarbij hij een aanzienlijke operationele verantwoordelijkheid draagt voor gegevensverwerkingsprocessen. Dat houdt in dat de FG niet ook (hoofd)verantwoordelijke voor (privacy) compliance mag zijn of mag beslissen over de aanschaf van IT systemen. Zie voor nadere uitleg paragraaf 3.2. van deze handreiking.

- **Positionering binnen gemeentelijke organisatie**. De FG moet binnen de gemeentelijke organisatie gepositioneerd worden op een plaats die de autonomie en onafhankelijkheid van de FG waarborgt. Het ligt voor de hand om voor de FG functie een staffunctie in te richten, zonder enige inbedding in de hiërarchie. Dit betekent dat de FG gepositioneerd kan worden onder het hoogste bestuurlijke gezag. Een voorbeeld kan worden genomen aan de positionering van de gemeentelijke concerncontroller.[2]

- **Ontslagbescherming**. Een FG heeft dezelfde ontslagbescherming als leden van een ondernemingsraad. Ervan uitgaande dat een FG integer handelt kan hij pas ontslagen worden na toestemming van de kantonrechter. De kantonrechter verleent slechts toestemming, indien het aannemelijk is dat de beëindiging geen verband houdt met de werkzaamheden van de FG. De FG zou niet ontslagen kunnen worden, omdat hij zijn taken goed uitvoert. De stap naar de kantonrechter beoogt een waarborg te geven voor het onafhankelijk optreden van de FG. De FG mag wegens zijn functioneren niet worden benadeeld met betrekking tot promotiekansen of de verdeling van werk. De FG kan via de kantonrechter nakoming van deze verplichtingen vorderen. De toestemming van de kantonrechter is niet vereist wanneer de FG schriftelijk met de beëindiging van zijn dienstbetrekking heeft ingestemd, of wanneer het ontslag geschiedt wegens een dringende aan de werknemer/FG onverwijld medegedeelde reden of bij beëindiging van de werkzaamheden van de onderneming.

- **Verankering in beleid**. Om de onafhankelijke rol van de FG te verantwoorden dient een beschrijving van de waarborging van de onafhankelijkheid, samen met de rol- en taakverdeling van de FG, vastgelegd te worden in interne privacybeleidstukken.

[1] Dit wordt benadrukt in een onderzoek van de AP naar FG's bij ziekenhuizen van 24 juni 2019. De AP maakt een expliciet onderscheid tussen aanbevelingen aan de verwerkingsverantwoordelijke en aanbevelingen aan de FG.
[2] Ook dit is echter weer afhankelijk van de inrichting van de gemeentelijke organisatie.

2.2.2 Betrekken bij alle privacyaangelegenheden

Het is van cruciaal belang dat de FG zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die de bescherming van persoonsgegevens raken. De FG moet betrokken worden bij vergaderingen van het management en moet uitgenodigd en geraadpleegd worden bij datalekken en beslissingen met gevolgen voor gegevensbescherming. Dat geldt voor alle privacy aangelegenheden van alle gemeentelijke diensten en (bij samenwerkingsverbanden) in alle ketens. Dit moet ingebed zijn in het standaardbeleid van de organisatie. Wat betreft DPIAs, vereist de AVG expliciet dat de FG geraadpleegd wordt.

2.2.3 Middelen

Gemeenten hebben te maken met gegevensverwerkingen waarbij gevoelige gegevens worden verwerkt, in allerhande samenwerkingsverbanden in verschillende ketens. De gemeentelijke verwerkingsverantwoordelijken zijn verplicht om de FG voldoende middelen te verstrekken om zijn taak uit te voeren. Deze middelen moeten in verhouding staan met de complexiteit van gegevensverwerkingen binnen gemeenten. Wanneer onvoldoende middelen worden geboden handelt de verwerkingsverantwoordelijke in strijd met de AVG.

Een gemeentelijke verwerkingsverantwoordelijke moet de FG ten minste de volgende middelen bieden:

- **Tijd**. Voldoende tijd om zijn taken te kunnen vervullen. Dat betekent dat de FG een minimaal aantal uren moet hebben om zijn taken goed te kunnen uitvoeren. Een paar uur per week is daarvoor onvoldoende. Dit geldt temeer als de FG geen ondersteuning heeft en de gemeente nog niet het gewenste volwassenheidsniveau heeft. Ook een FG die alleen op afroep beschikbaar is, komt onvoldoende toe aan de wettelijke taken van de FG omdat hij binding mist met de organisatie en alleen incident gedreven toezicht kan houden. Op basis van de grootte en structuur van de organisatie, kan het nodig zijn een FG-team aan te stellen. In dergelijke gevallen dienen de interne structuur van het team en de taken en verantwoordelijkheden van elk lid duidelijk vastgelegd te worden.

- **Ondersteuning**. Actieve ondersteuning bij de uitvoering van zijn functie, zonder dat invloed uitoefent op de werkzaamheden van de FG. Dit betekent dat de FG rechtstreeks toegang moet hebben tot onder meer het college, de gemeenteraad en de gemeentesecretaris. Bovendien moet gewaarborgd worden dat deze verwerkingsverantwoordelijken het advies van de FG naar behoren in overweging nemen. Als wordt afgeweken van het advies van de FG moet de verwerkingsverantwoordelijke dat schriftelijk en gemotiveerd doen. In de praktijk wordt deze vastlegging veelal gedaan door de gemeentesecretaris.

- **Financiële middelen, infrastructuur & personeel**. Adequate ondersteuning op het vlak van financiële middelen, infrastructuur (kantoren, faciliteiten, apparatuur) en personeel waar van toepassing.

- **Toegang**. Toegang tot andere diensten binnen de organisatie, zodat de FG voor de gegevensbescherming de benodigde essentiële informatie, ondersteuning, of bijstand kan ontvangen.

- **Opleidingsbudget**. Ondersteuning t.a.v. zijn professionele ontwikkeling (voldoende opleidingsbudget).

- **Bescherming**. Dit geldt zowel voor de FG die in dienst is, als voor de externe FG. Dit betekent dat de FG niet kan worden ontslagen en de dienstverleningsovereenkomst niet op oneigenlijke gronden mag worden beëindigd.

2.3 Met wie werkt de FG samen en wat is zijn rol daarin?

2.3.1 De interne organisatie

Het is belangrijk dat de FG contact heeft met de hele interne organisatie. Op deze manier weet de FG wat er in de gemeente speelt en kan hij zijn toezichtstaak goed uitvoeren. Zie over de vereiste betrokkenheid van de FG nader paragraaf 2.2.2. Daarnaast is van belang dat de FG wordt gepositioneerd binnen de organisatie op een plek waar de autonomie en de onafhankelijkheid zijn gewaarborgd (zie hierover nader paragraaf 2.2.1).

2.3.2 Het college van B&W en de gemeenteraad

De FG dient in onafhankelijkheid zijn werkzaamheden te kunnen verrichten en mag geen instructies ontvangen (zie hierover nader paragraaf 2.2.1). Dit mag er echter niet toe leiden dat de FG geïsoleerd van het college van B&W en de gemeenteraad komt te staan. Het college van B&W/de gemeenteraad enerzijds en de FG anderzijds dienen elkaar juist gemakkelijk te kunnen vinden. De FG moet immers rechtstreeks rapporteren aan deze (en andere) verwerkingsverantwoordelijken. De FG zou dan ook actief (in staat gesteld worden om) het contact met het bestuur te zoeken en te onderhouden. Aan de andere kant betekent dat dat de verwerkingsverantwoordelijke regelmatig het gesprek met de FG moet aangaan over de verwerking van persoonsgegevens in de gemeentelijke organisatie en de risico's die daaraan zijn verbonden. Ook moet de verwerkingsverantwoordelijke de FG ondersteunen in de uitvoering van zijn taken (zie hierover nader paragraaf 2.2.3).

2.3.3 Chief Information Security Officer (CISO)

Een gemeente moet voor de verwerking van persoonsgegevens informatiebeveiligingsmaatregelen treffen. De taken van de CISO heeft duidelijke raakvlakken met de taken van de FG. Het aspect 'vertrouwelijkheid van informatie'behoort immers ook tot het taakgebied van de CISO. Voor zover de CISO binnen de gemeente ook verantwoordelijkheid is voor het implementeren van informatiebeveiligingsbeleid of de aanschaf van IT systemen kan deze rol conflicteren met de toezichthoudende rol van de FG en daarvoor vereiste onafhankelijkheid. De AP heeft met betrekking tot deze raakvlakken aangegeven dat het combineren van de CISO en FG rol geen goede combinatie is, om zo de onafhankelijkheid te waarborgen en belangenverstrengeling te voorkomen (art. 38 lid 6 AVG).[3] Zie hierover nader de tabel in paragraaf 3.2 over de taakverdeling tussen de FG, CISO en PO.

2.3.4 Privacy Officer (PO)

De rol van een Privacy Officer (PO) is om bij te dragen aan privacy compliance van de gemeente. Deze rol kan verschillend van aard zijn per gemeente, zoals louter juridisch of meer coördinerend. Sommige organisaties hebben ook een Chief Privacy Officer (CPO) die een leidinggevende rol heeft in het privacyteam ten aanzien van privacy compliance.

De PO heeft een andere rol heeft dan de FG. Zo beschikt de PO niet over toezichthoudende bevoegdheden. De PO heeft een uitvoerende rol en is verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid van de gemeentelijke organisatie en het ondersteunen van de uitvoering. Dit doet hij in nauwe samenwerking met de FG en de CISO. De taken van de PO die zien op verantwoordelijkheid voor privacy compliance kunnen conflicteren met de toezichthoudende rol van de FG en daarvoor vereiste onafhankelijkheid. Het combineren van de FG rol en de PO rol is daarom niet wenselijk. Los daarvan kan het nodig zijn voor de FG om privacy adviseurs aan te stellen die hem helpen met de uitvoering van zijn FG taken. Zie hierover nader de tabel in paragraaf 3.2 over de taakverdeling tussen de FG, CISO en PO.

2.3.5 Andere interne partijen

De FG werkt ook samen met de riskmanager, auditor en accountant. De riskmanager houdt zich net zoals de FG en de CISO bezig met risico's, maar kijkt veel breder dan alleen privacy- en informatiebeveiligingsrisico's. Zo gaat het bij deze rol om de impact van bijvoorbeeld een bepaald type datalek op de bedrijfscontinuïteit. De interne of externe auditor controleert of processen en bedrijfsonderdelen voldoen aan de vooraf bepaalde eisen. De accountant controleert de jaarrekening in opdracht van de gemeenteraad en beoordeelt of de gemeente voldoet aan eisen uit wet- en regelgeving voor zover het gaat om financiële risico's. Met betrekking tot privacy zijn aansprakelijkheidsrisico's en verzekeringen tegen datalekken interessant voor de accountant. Het is verstandig om de FG-jaarrapportage te publiceren vóór de accountantscontrole, zodat de accountant hiermee rekening kan houden.

Daarnaast kan de FG samenwerken met privacysleutelpersonen binnen de verschillende afdelingen van de gemeente. Het is raadzaam om per team of afdeling een persoon aan te wijzen die het privacy aanspreekpunt is binnen het team of afdeling zodat deze als eerste lijn kunne optreden bij privacyvragen. Al deze privacy sleutelpersonen, die privacy naast hun reguliere werkzaamheden in hun takenpakket hebben, komen vervolgens regelmatig bijeen om hun bevindingen op het gebied van privacy te bespreken. Op deze wijze blijft de FG op de hoogte van de ontwikkelingen op de werkvloer.

[3] Opgemerkt door de AP tijdens een bijeenkomst van de Nederlandse beroepsvereniging van Functionarissen voor Gegevensbescherming (NGFG) van 22 november 2017.

2.3.6 De ondernemingsraad

De ondernemingsraad (OR) heeft instemmingsrecht als het gaat om maatregelen die voorgesteld worden ter bescherming van de persoonsgegevens van werknemers en verwerking daarvan (art. 27 lid 1 sub k WOR, Wet op de ondernemingsraden). Denk hierbij bijvoorbeeld aan reglementen voor sollicitaties en klachtenprocedures. Het instemmingsrecht geldt ook voor voorzieningen die gericht zijn op waarneming van, of controle op aanwezigheid, gedrag of prestaties van werknemers. Dit zijn personeelvolgsystemen (art. 27 lid 1 sub l WOR), zoals heimelijk cameratoezicht en software voor de controle op e-mail- en internetgebruik.[4]

Concreet betekent dit dat de OR instemmingsrecht heeft ten aanzien van regelingen die de privacy van medewerkers raken. De verwerking mag dus niet starten voordat instemming is verkregen. De FG zal dus met enige regelmaat met de OR samenwerken. Instemming van de OR is overigens niet nodig bij de benoeming van de FG.

Daarnaast heeft de OR ook een adviesrecht over voorgenomen besluiten tot invoering of wijziging van een belangrijke technologische voorziening (art. 25 lid 1 sub k WOR). Hierbij kunnen privacyaspecten een rol spelen. Er kan samenhang zijn met het instemmingsrecht. Zo zal bij het aanbrengen van een camerabewakingssysteem mogelijk ook persoonsgegevens van werknemers betrokken zijn. In dat geval heeft het OR zowel een adviesrecht als – voor zover het gaat over de verwerking van persoonsgegevens van werknemers – een instemmingsrecht.

2.3.7 Betrokkenen

Betrokkenen (burgers en personeel) moeten eenvoudig met de FG contact kunnen opnemen om te informeren naar verwerkingen van hun persoonsgegevens door de gemeente en om hun AVG-rechten uit te kunnen oefenen (art. 38 lid 4 AVG). Bekendmaking van de rechtstreekse contactgegevens van de FG is dan ook verplicht (art. 37 lid 7 AVG).[5] Zo kan de gemeente bijvoorbeeld een specifiek telefoonnummer of contactformulier beschikbaar stellen. De rechtstreekse contactgegevens moeten duidelijk gecommuniceerd worden naar inwoners. Het is niet vereist om ook de naam van de FG te communiceren. De communicatie van de naam van de FG is wel aan te raden in de interne gemeentelijke organisatie. Als betrokkenen zich met vragen tot de AP hebben gericht zal de toezichthouder hen in eerste instantie zo veel mogelijk doorverwijzen naar de FG.

2.3.8 Autoriteit Persoonsgegevens (AP)

Het is de bedoeling van de wetgever dat zich tussen de FG en de AP een soepel samenspel ontwikkelt. Zo heeft de AP aangegeven dat een FG altijd contact kan opnemen met de AP voor *guidance*. Dit is in lijn met het feit dat de FG geen vertegenwoordiger is van de AP, maar de contactpersoon van de verwerkingsverantwoordelijke. De AP behoudt dan ook haar taken en (boete)bevoegdheden, ook ten aanzien van organisaties die een FG hebben aangesteld. Dit betekent o.a. dat als de AP onderzoek doet naar de gemeentelijke organisatie de AP in eerste instantie contact opneemt met de verwerkingsverantwoordelijke. Daarbij zal de FG wel worden meegenomen in de cc. Zie ook paragraaf 2.1, onder ad 3, over samenwerken met de AP.

[4] Voorbeelden van de AP, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/ondernemingsraad.
[5] Intern is het aan te bevelen om de naam van de FG kenbaar te maken. Bekendmaking naar buiten toe is aan te bevelen, maar niet verplicht. Doe dit in overleg met de FG.

3. Taken van de FG

3.1 Takenpakket van de FG

De kerntaken van de FG zijn als volgt:

1. Adviseren
2. Toezien op naleving
3. Samenwerking met en contactpunt van de AP
4. Optreden als contactpunt voor betrokkenen

Daarnaast kan de verwerkingsverantwoordelijke aanvullende andere taken bij de FG beleggen. De aanvullende taken mogen natuurlijk niet strijdig zijn met de toezicht functie. Over de vraag of het bijhouden van het verwerkingsregister strijdig is met de toezichtfunctie bestaat verschik van mening. De European Data Protection Board (EDPB) noemt het bijhouden van het register als mogelijke taak, [6] terwijl de AP aangeeft dat het bijhouden van het register geen taak is van de FG maar dat de FG het register louter controleert op compliance met de AVG.[7] De IBD adviseert om het standpunt van de AP te volgen en de taken van de FG in relatie tot het register te beperken tot de controle ervan.

De FG dient bij de uitvoering van zijn taken een risico gebaseerde aanpak te hanteren (gelet op de aard, omvang, de context en de verwerkingsdoeleinden). Dit betekent dat de FG zijn activiteiten moet prioriteren en zijn werkzaamheden in eerste instantie moet richten op die verwerkingen die een hoog risico met zich brengen. Het is sterk aanbevolen om deze risico gebaseerde aanpak vast te leggen in (FG) beleid.

3.1.1 Adviseren

Algemeen

De taak van de FG is om de verwerkingsverantwoordelijke en haar medewerkers te informeren en adviseren over hun verplichtingen op grond van de AVG, de Uitvoeringswet AVG en andere privacywetgeving. Zoals aangegeven is de verwerkingsverantwoordelijke verplicht om de FG vooraf te raadplegen bij alle aangelegenheden over de verwerking van persoonsgegevens. Het advies van de FG kan daarom gezien worden als een vorm van preventief toezicht.

De FG houdt bij zijn werkzaamheden rekening met de belangen van de betrokkenen. De FG geeft gevraagd en ongevraagd advies van laag tot hoog in de organisatie: aan medewerkers, afdelingshoofden, de algemeen directeur, het managementteam en de verwerkingsverantwoordelijke(n), zoals het college van B&W. Hij is vertrouwenspersoon binnen de organisatie. Ook is hij sparringpartner, bijvoorbeeld voor het collegelid met de portefeuille gegevensbescherming (dit kan de burgemeester of een wethouder zijn).

De FG legt verslag af over de stand van zaken is ten aanzien van privacy compliance bij de gemeente. Hij brengt rechtstreeks verslag uit aan de hoogst leidinggevende van de verwerkingsverantwoordelijke. [8] Dit is dus het college van B&W, de portefeuillehouder gegevensbescherming in het college van B&W, de gemeenteraad en de gemeentesecretaris.

De FG heeft geen formele bevoegdheid om een bindend advies te geven, maar zijn oordeel is ‘zwaarwegend’. De verwerkingsverantwoordelijke kan het advies van de FG alleen gemotiveerd terzijde leggen en dient het afwijkende besluit vast te leggen. Naast het advies kan een FG ook richtsnoeren verstrekken aan de verwerkingsverantwoordelijke over passende maatregelen en om aan te tonen dat de verwerkingsverantwoordelijke de regels naleeft (overweging 77 AVG).

Data protection impact assessment (DPIA)

Een DPIA is verplicht voor verwerkingen met een hoog privacyrisico.[9] De verwerkingsverantwoordelijke moet bij de uitvoering van een DPIA advies vragen van de FG (art. 35 lid 2 AVG). Bij deze advisering kan het gaan om:

---

[6] Zie WP29, Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), (WP243rev.01), 13 december 2016 laatstelijk herzien 5 april 2017, p. 19.

[7] Aangegeven door de Autoriteit Persoonsgegevens in een overleg met de IBD / VNG.

[8] Zie het FG voorbeeldrapportage voor de gemeenteraad en het college van B&W.

[9] Zie voor meer over de vraag of een DPIA verplicht is de DPIA factsheet.

- of er al dan niet een DPIA moet worden uitgevoerd;
- welke methodologie moet worden uitgevoerd;
- of de DPIA intern kan worden uitgevoerd, of zou moeten worden uitbesteed;
- welke waarborgen (waaronder technische en organisatorische maatregelen) moeten worden toegepast om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de DPIA al dan niet correct is uitgevoerd en of de conclusies (de verwerking al dan niet uitvoeren en welke waarborgen toepassen) al dan niet in overeenstemming zijn met de AVG.

De FG is in principe niet betrokken bij de uitvoering van een DPIA, zodat hij vrij is om te adviseren over de uitkomsten daarvan. De FG moet toezien op de uitvoering van zijn advies (art. 39 lid 1 sub c AVG). Als de verwerkingsverantwoordelijke het advies van de FG niet opvolgt, moet de besluitvorming hierover worden gemotiveerd en worden vastgelegd.

Adviseren over techniek en beveiliging
Advisering over technische beveiligingsmaatregelen, naast organisatorische beveiligingsmaatregelen, behoort ook tot de taken van de FG. Indien de FG niet over technische kennis beschikt kan de FG hierover sparren met bijvoorbeeld de CISO of security adviseur. Wanneer de FG functie wordt uitbesteed aan een externe partij met een juridische achtergrond wordt in de praktijk vaak de advisering en over techniek uitgesloten van de dienstverleningsovereenkomst. De gemeente moet in dat geval waarborgen dat de externe partij wordt bijgestaan door iemand met technische kennis.

Adviseren naar aanleiding van audits
De FG kan op eigen initiatief een audit laten uitvoeren. De FG ontvangt de uitkomsten daarvan. De FG geeft op basis hiervan zijn bevindingen met een eigen aanvullend advies aan de verwerkingsverantwoordelijke (college en gemeenteraad). Zie paragraaf 3.1.2 over het auditplan.

Datalekken
Het doen van een (voorlopige) melding van een datalek is de verantwoordelijkheid van de verwerkingsverantwoordelijke. Bij een datalek dient de verwerkingsverantwoordelijke de FG te raadplegen over de vraag of een beveilingingsincident al dan niet gemeld moet worden bij de AP en de betrokkene(n). De eindbeslissing hierover ligt bij de verwerkingsverantwoordelijke.

3.1.2 Toezien op naleving

De FG moet erop toezien dat binnen de gemeente de regels van de AVG worden naleeft (art. 39 lid 1 sub b AVG). De FG verzamelt informatie over gegevensverwerkingen, beoordeelt of deze verwerkingen aan de AVG voldoen en doet vervolgens aanbevelingen aan verwerkingsverantwoordelijke of verwerker. Dit is voornamelijk een toetsing of controle achteraf. Hierbij kan de FG zich laten ondersteunen door (externe) specialisten. De wijze waarop de FG in de praktijk invulling geeft aan zijn toezichthoudende taak op basis van zijn bevoegdheden, hangt sterk af van de aard van de organisatie en de gegevens die worden verwerkt.

Bevoegdheden FG
De FG beschikt niet over sanctiebevoegdheden, maar het college van B&W dient de controlebevoegdheden van de FG te faciliteren, dan wel te ondersteunen. Op deze manier is het toezicht geloofwaardig en effectief. Deze controlebevoegdheden dienen overeen te komen met de taakomschrijvingen van de FG in de AVG (art. 39 AVG) en de bevoegdheden die gelden voor het toezicht binnen de overheid (art. 38 lid 2 AVG). Hiervoor dient de FG ter vervulling van zijn taak over bevoegdheden te beschikken die gelijkwaardig zijn aan de bevoegdheden zoals geregeld in titel 5.2 van de Algemene wet bestuursrecht (Awb). De bestuursrechtelijke bevoegdheden uit de Awb dienen uiteraard vertaald te worden naar de situatie waarin de FG zich bevindt. Daarnaast dient vooraf de reikwijdte van de bevoegdheden te worden bepaald. Voor welke gemeente(n) of onderdelen daarvan is de FG bevoegd? Vastlegging van de bevoegdheden en de reikwijdte daarvan in een interne regeling of een door het college van B&W getekend statuut is aan te bevelen. Bovendien is het in dit kader van belang dat de FG een zaak kan escaleren. Zoals aangegeven dient de FG direct toegang te hebben tot de hoogste leidinggevende en/of het college om te rapporteren wat hij heeft geconstateerd.

Ad hoc en structureel toezicht
Bij de toezichttaak van de FG kan een onderscheid worden gemaakt tussen ad hoc toetsing en structurele toetsing.

- Bij de ad hoc of incidentgedreven toetsing laat de FG zich als het ware leiden door de waan van de dag. De toetsing vindt plaats naar aanleiding van vragen of klachten van betrokkenen of ontwikkelingen binnen de gemeente. Onvoldoende is als de FG alleen incident gedreven toezicht houdt. Dat neemt niet weg dat de FG door aanwezigheid en zichtbaarheid in de organisatie sneller op de hoogte is van (zorgwekkende) privacyaangelegenheden.

- Bij structurele toetsing controleert de FG periodiek de opzet, bestaan en werking van gegevensverwerkende processen en andere initiatieven. De FG heeft verschillende instrumenten tot zijn beschikking:

    - Met een auditplan kan de FG handen en voeten geven aan het uitvoeren van de structurele toetsing. Zo kan in het auditplan staan dat hulp nodig is van (externe) expertise, zoals een technische informatiebeveiligingsspecialist ter toetsing van beveiligingsmaatregelen. Het auditplan biedt ook input voor het jaarverslag.
    - Het jaarverslag is een instrument om verslag af te leggen aan het bestuur. Dit is vaak verslaglegging op hoger niveau, aangezien de details doorgaans niet relevant zijn voor het bestuur.[10]
    - Onderzoek bij elke nieuwe verwerking. Een andere optie is om te werken met zogenaamde pre-DPIAs die door de betreffende afdeling / samenwerkingsverband moeten worden ingevuld bij elke nieuwe verwerking. In dat vooronderzoek wordt getoetst of daadwerkelijk een verplichting bestaat tot het uitvoeren van een DPIA. Het ingevulde vooronderzoek wordt voorgelegd aan de FG zodat hij kan toezien of de juiste afweging is gemaakt om al dan niet een DPIA uit te voeren. Als dit proces is ingebed in de organisatie geeft het tegelijkertijd een goed beeld aan de FG van alle nieuwe verwerkingen en kunnen mogelijk onrechtmatige verwerkingen tijdig geïdentificeerd worden.

Bij het uitoefenen van het toezicht heeft de FG verschillende bevoegdheden;

- *Inzage en (klachten)onderzoek*

De FG kan zelfstandig onderzoek doen naar aanleiding van bijvoorbeeld een klacht van een betrokkene. De FG zal, om zijn toezichthoudende rol goed uit te kunnen oefenen, bevoegd dienen te zijn om inzage te vragen van zakelijke gegevens. Hiervan mag de FG desgewenst kopieën maken. Het gaat hierbij niet uitsluitend om fotokopieën. Ook kan het noodzakelijk zijn kopieën te maken van (gedeelten van) geautomatiseerde gegevensbestanden. De verwerkingsverantwoordelijke moet hieraan meewerken.

Voorbeeld voor een aanpak van klachten: zorg voor duidelijke documentatie van het proces en de genomen beslissingen. Het begint bij het contact opnemen met de klager om de achtergrond goed te begrijpen. Tegelijk kan de FG dan toetsen of de klager wel betrokkene is en dus een belang heeft bij de klacht. Wellicht zijn de bezwaren van de klager al tijdens deze intake weg te nemen. Vervolgens dient de FG onderzoek te doen naar de oorzaak van de klacht, dit te toetsen aan de AVG, eventuele experts inschakelen en een verslag te maken van de hieruit voortvloeiende bevindingen. Neem de klager waar mogelijk mee in dit proces, zodat hij of zij merkt dat de gemeente de klacht serieus neemt en de mogelijkheid bestaat om tussentijds feedback te ontvangen. Als laatste stap voor afronding zou de klager de mogelijkheid kunnen krijgen om te reageren op het rapport en deze feedback te verwerken. Bij de afronding kan de FG aanbevelingen aan de gemeente geven en een bevestiging aan de klager.

- *Vragen van inlichtingen*

De FG kan actief inlichtingen verkrijgen over de verwerking van persoonsgegevens. Dit kunnen bijvoorbeeld inlichtingen zijn over de toegang tot systemen. De verwerkingsverantwoordelijke is verplicht aan de FG binnen de door hem gestelde redelijke termijn alle medewerking hieromtrent te verlenen.

- *Betreden van ruimten*

De FG kan daarnaast actief alle ruimten (waaronder de serverruimten) betreden, indien dit noodzakelijk is voor de uitoefening van zijn taak.

[10] Zie het voorbeeld jaarrapportage voor de gemeenteraad en het college.

3.1.3 Samenwerken met AP

Ten aanzien van de verwerking van persoonsgegevens is de FG voor de AP het eerste aanspreekpunt voor de toezichthouder. Daarom is het van belang dat de AP beschikt over de contactgegevens van de FG. Dit is ook een verplichting op grond van art. 37 lid 7 AVG. Daarnaast kan de FG zelf het initiatief nemen om contact op te nemen met de AP om advies te vragen. In beide gevallen maakt de FG onderscheid tussen zijn eigen verantwoordelijkheid en die van de organisatie.

Onderdeel van deze samenwerking is ook dat de AP contact kan opnemen met de FG, bijvoorbeeld naar aanleiding van klachten. Zo kunnen betrokkenen een klacht indienen bij de AP op grond van art. 77 AVG en een handhavingsverzoek indienen bij de AP op grond van de Algemene wet bestuursrecht (Awb). In beide gevallen is het aannemelijk dat de AP verdere inlichtingen opvraagt bij de FG. Het is ook denkbaar dat de AP een onderzoek start en rechtstreeks contact opneemt met de verwerkingsverantwoordelijke van de gemeente. Het is raadzaam om interne afspraken te maken over de communicatie met de AP in het geval zij (al dan niet onaangekondigd) een onderzoek start.

3.1.4 Optreden als contactpunt voor betrokkenen

De FG is contactpunt voor betrokkenen. Voor een nadere uitleg wordt verwezen naar paragraaf 2.3.7.

3.2 Taakverdeling tussen de FG, CISO en PO

In de volgende tabel wordt de taakverdeling tussen de FG, CISO en PO weergegeven. Deze taakverdeling is sterk afhankelijk van de gemeentelijke organisatiestructuur. Let op dat dit schema niet uitputtend is.

Taken	FG	CISO	PO	Toelichting
Ondersteuning bij het opstellen van een DPIA	X		X	Vanuit zijn positie en professie kan de PO (samen met een multidisciplinair team[11]) de gemeente inhoudelijk (juridisch) adviseren bij de uitvoering van een DPIA. De FG dient zich in deze fase terughoudend op te stellen, zodat hij onbevangen een advies over de resultaten van de DPIA kan geven. De FG moet de ingevulde DPIA controleren en toetsen.
Opstellen en bijhouden register van verwerkingsactiviteiten			X	Het opstellen en het bijhouden van het register ligt bij de verwerkingsverantwoordelijke en verwerker en wordt doorgaans uitgevoerd door een PO. De informatie hiervoor komt van de vakafdelingen. Deze taak wordt in de richtsnoeren van de EDPB genoemd als een van de mogelijke additionele taken van een FG.[12] De AP heeft echter aangegeven dat het bijhouden van het register geen taak is van de FG maar dat de FG het register louter controleert en toetst op compliance met de AVG.[13] De IBD adviseert om het standpunt van de AP te volgen.
Controleren en toetsen van het register van verwerkingsactiviteiten	X			Zodra het register is opgeleverd wordt dit voorgelegd aan de FG die het register controleert. De FG legt zijn bevindingen voor aan de verwerkingsverantwoordelijke.
Opstellen van verwerkersovereenkomsten			X	Het opstellen en bijhouden van verwerkingsovereenkomsten is een taak die bij de uitvoerende afdelingen thuishoort. De PO kan hierbij ondersteunen en adviseren. De FG toetst later op basis van het register of alle verwerkersovereenkomsten zijn afgesloten.
Adviseren over technologie en beveiliging omtrent gegevensverwerking	X	X		Vanuit zijn positie en professie kan de CISO de gemeente inhoudelijk en bij privacyvraagstukken (op casusniveau) adviseren. Ook de FG adviseert hierover.
Melding van datalekken	X	X	X	De verwerkingsverantwoordelijke is verantwoordelijk voor de juiste en tijdige melding van het datalek bij de AP en het documenteren van datalekken (in een logboek van alle datalekken). De PO en de CISO hebben hierin een uitvoerende en adviserende rol. Het is verstandig om de afdeling waar het datalek zich heeft voorgedaan te betrekken bij de melding aan de AP. Dit bevordert de privacy awareness. De FG heeft een adviserende rol en wordt geraadpleegd bij een datalek. De eindbeslissing of gemeld wordt ligt bij de verwerkingsverantwoordelijke.
Adviseren over de juridische aspecten van de verwerking van persoonsgegevens	X		X	De FG geeft advies over de verwerking van persoonsgegevens. Zeker op globaal niveau dient de FG betrokken te zijn bij alle aangelegenheden op het gebied van gegevensbescherming. Dit moet ingebed zijn in het interne beleid en de werkprocessen van de gemeente. Advisering kan tevens gezien worden als preventief toezicht. Ook de PO adviseert over privacy compliance. Er bestaat dus enige overlap in taken van de FG en de PO. Echter de PO heeft geen toezichttaak en daarmee gepaard gaande eis van onafhankelijkheid. De PO houdt zich bezig met uitvoerende taken zoals het opstellen en onderhouden van privacybeleid en overeenkomsten en het uitonderhandelen daarvan. Deze taken liggen minder voor de hand voor de FG's, om zo te voorkomen dat 'de slager zijn eigen vlees keurt'. Een goede samenwerking tussen de FG en de PO is essentieel.

Rechten van betrokkenen	X		X	De verwerkingsverantwoordelijke is verantwoordelijk voor de afhandeling van verzoeken, bezwaren en klachten van betrokkenen. De behandeling van deze verzoeken wordt uitgevoerd door de PO. De FG houdt toezicht op de juiste afhandeling. Daarnaast kunnen betrokkenen contact opnemen met de FG wanneer zij hun rechten willen uitoefenen.

3.3 Over welke kennis en vaardigheden dient de FG te beschikken?

De AVG stelt een aantal algemene eisen aan de FG (art. 37 lid 5 AVG):

1. Brede en toereikende kennis, zoals:

   - juridische kennis (privacyregelgeving, wetgeving in het sociaal domein , relevante gemeentelijke regelgeving);
   - inzicht in de verwerkingen die een gemeente uitvoert dan wel laat uitvoeren;
   - kennis van de omgeving waarin gemeenten opereren;
   - deskundigheid op het gebied van ICT. Kennis van wetgeving en ICT gecombineerd in één persoon is schaars. Er zal naar een praktische oplossing dienen te worden gezocht, waarbij de FG niet noodzakelijkerwijs een jurist hoeft te zijn;
   - kennis van informatiebeveiliging (Baseline Informatiebeveiliging Overheid, BIO). Om aan te tonen dat de FG over voldoende deskundigheid beschikt die noodzakelijk is om de functie te kunnen uitvoeren, kan een FG mede worden geselecteerd op grond van behaalde certificaten.[14]

2. Het vermogen om binnen de organisatie een cultuur van gegevensbescherming te bevorderen. Hier gaat het bijvoorbeeld om het strategisch opzetten en blijven onderhouden van een integraal privacy bewustwordingscampagne.

3. Soft skills en gevoel voor politiek-bestuurlijke verhoudingen.[15] De FG moet met alle lagen van de organisatie kunnen schakelen, waaronder met name het bestuur. Daarom moet degene die deze rol vervult (ook) beschikken over bestuurlijke sensitiviteit, maar ook onafhankelijk durven zijn. De gemeentelijke organisatie moet er om die reden voor waken om zomaar iemand te 'promoveren' tot FG. Hij moet stevig in zijn schoenen staan. Zo zal de FG in het algemeen behoedzaam moeten opereren, in die gevallen dat er verschil van inzicht is met of tussen vakafdelingen, de verwerkingsverantwoordelijke en/of de hoogste leidinggevende. Er mogen dus hoge eisen worden gesteld aan de diplomatieke vaardigheden van de FG.

4. Betrouwbaarheid, aangezien de FG bij de uitvoering van zijn taken geheimhouding en vertrouwelijkheid moet bewaren. Zo kan de FG de beschikking krijgen over vertrouwelijke informatie van/over betrokkenen. Daarnaast kan de FG de beschikking krijgen bedrijfsgeheimen, zoals de staat van beveiliging van computersystemen.
   Houdt er rekening mee dat de FG bepaalde rapportageverplichtingen heeft en dus in dat kader wel tot op zekere hoogte openheid van zaken moet geven. Dit is vanzelfsprekend niet in strijd met de geheimhoudingsplicht, omdat niet over alle zaken verslag hoeft te worden afgelegd. De geheimhoudingsplicht kan slechts worden doorbroken bij situaties waarin een ernstig risico voor betrokkenen ontstaat en de uitvoeringsorganisatie geen passende maatregelen treft ondanks het eerdere advies van de FG. De FG zou de verwerking zelfstandig moeten kunnen staken en eventueel de AP moeten inschakelen. In dit kader is het raadzaam om een escalatieprotocol voor de FG te hebben.

---

[11] Zie de DPIA Factsheet.
[12] Zie WP29, Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), (WP243rev.01), 13 december 2016 laatstelijk herzien 5 april 2017, p. 19.
[13] Aangegeven door de Autoriteit Persoonsgegevens in een overleg met de IBD / VNG.
[14] De meest bekende en erkende privacy certificeringen worden aangeboden door de International Association of Privacy Professionals (IAPP). De IAPP kent verschillende certificaten. Voor een FG zijn de Certified Information Privacy Professional/ Europe (CIPP/E) en Certified Information Privacy Manager (CIPM) het meest relevant. Naast deze privacy certificeringen zijn er nog de Certified Data Protection Officers (CDPO) en Privacy & Data Protection Certification (CDPO) certificeringen. De AP heeft echter nog geen certificering onderschreven.
[15] Softskills is een verzamelnaam voor onder andere de persoonlijke eigenschappen, sociale vaardigheden en communicatieve vaardigheden.

De mate waarin invulling wordt gegeven aan deze eisen van een FG bepaalt de mate van succes. Het gaat om een samenspel van bovenstaande eisen. Alleen de privacywetgeving goed kennen is niet voldoende. Aangezien de FG beschikt over zachte handhavingsmiddelen, zoals zwaarwegende adviezen en richtsnoeren – ten opzichte van de AP die over harde handhavingsmiddelen beschikt - is het extra van belang om de gemeente mee te krijgen in het volgende privacy volwassenheidsniveau door betrokken te zijn bij de organisatie (art. 39 lid 1 AVG), rekening houdend met bovenstaande vaardigheden.[16]

Dit vereist bepaalde persoonlijke kwaliteiten, zoals leiderschap en autoriteit, maar ook een flexibele meedenkende houding. Verder vergt deze rol kennis en ervaring van veel verschillende disciplines, zoals ICT, het recht (meer dan alleen de AVG), bestuur en ketensamenwerking. Het vinden van een balans tussen al deze factoren is onderdeel van de dagelijkse praktijk van de FG. Houdt daarbij altijd het doel voor ogen: de naleving van de AVG, rekening houdend met de risico's en de aard, omvang, context en doeleinden van verwerkingen.

[16] Zie het AVG borgingsproduct voor een uitgebreid overzicht van privacycontrols specifiek voor gemeenten.