ROL EN TAKEN VAN DE FG

Onder de huidige wetgeving mogen gemeenten zelf bepalen of ze een Functionaris Gegevensbescherming (FG) benoemen. In de AVG wordt de functie verplicht. Om in de toekomst verscherpt toezicht, bestuurlijke boetes of rechtszaken te voorkomen, wordt geadviseerd tijdig een FG aan te wijzen. De positionering van de FG binnen de gemeente dient juist gekozen te worden, deze is bepalend voor de slagkracht van een FG. Deze handreiking richt zich zowel tot het college van B&W als tot de FG. Het doel van deze handreiking is een handvat te bieden aan de colleges van burgemeester en wethouders (B&W) bij het aanwijzen van een FG en vormt een hulpmiddel om te komen tot concrete invulling van de FG functie. Gemeenten vinden in deze handreiking concrete beschrijvingen waarmee een gewenst functieprofiel kan worden samengesteld. De beoogde of aangestelde FG vindt aanknopingspunten om de functie in de praktijk handen en voeten te geven.

De Wet bescherming persoonsgegevens (Wbp)[1] geeft organisaties die persoonsgegevens verwerken de bevoegdheid om een interne toezichthouder aan te stellen: de Functionaris Gegevensbescherming (FG).[2,3,4] Onder de nieuwe Europese privacyverordening, de Algemene Verordening Gegevensbescherming (AVG)[5], die op 25 mei 2018 van toepassing wordt, wordt het aanstellen van een FG, een interne toezichthouder op de verwerking van persoonsgegevens, voor alle organisaties, dus ook gemeenten, verplicht. Privacy speelt een rol in de relatie tussen burger en gemeenten. Gemeenten moeten zorgvuldig en veilig, proportioneel en vertrouwelijk omgaan met het verzamelen, bewaren, beheren en gebruiken van persoonsgegevens en andere informatie die de persoonlijke levenssfeer van burgers raakt. Burgers moeten daarop kunnen vertrouwen; privacy is immers een grondrecht.[6] Als burgers dat vertrouwen niet hebben, dan kan dat er onbedoeld toe leiden dat zij geen hulp vragen of geen beroep doen op de gemeentelijke dienstverlening. Daarnaast kan de gemeente politieke en reputatieschade oplopen als bekend wordt dat er onzorgvuldig met persoonsgegevens van zijn burgers wordt omgegaan. In het ergste geval kunnen de gegevens van burgers, na een datalek, worden gebruikt bij identiteitsfraude.[7] Hierbij kan sprake zijn van aansprakelijkstelling door de burger, waarbij de gemeente verantwoordelijk wordt gehouden voor de schade. Ook loopt uw gemeente het risico om een geldboete te krijgen van de Autoriteit Persoonsgegevens (AP)[8] wanneer uw gemeente in strijd handelt met de bepalingen uit de Wbp of AVG.[9] Een FG kan uw gemeente helpen bij het vroegtijdig identificeren en adresseren van privacyrisico's.

1 http://wetten.overheid.nl/BWBR0011468/
2 Zie paragraaf 1.7 uit de Richtsnoeren beveiliging van persoonsgegevens (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf)
3 De Engelse benaming voor Functionaris Gegevensbescherming is Data Protection Officer (DPO).
4 Artikel 62, 63 en 64 Wbp.
5 http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=NL
6 http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbac43qvy#p10
7 Hierbij kan de gemeente de burger wijzen op de website www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/hoe-herken-ik-identiteitsfraude.
8 https://autoriteitpersoonsgegevens.nl/
9 Voor de AVG geldt een maximale geldboete van 20 miljoen euro of 4% van de wereldwijde jaaromzet en voor de Wbp geldt een maximale geldboete van 820.000 euro of 10% van de nationale jaaromzet.

OM ZOWEL DE BELANGEN VAN DE GEMEENTE ALS BURGERS DOELTREFFEND TE BEHARTIGEN WORDT EEN FG AANGESTELD ALS INTERNE TOEZICHTHOUDER

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN
VERENIGING VAN NEDERLANDSE GEMEENTEN

Met de komst van de AVG zijn de begrippen verantwoordelijke (controller) en bewerker (processor) gewijzigd in verwerkingsverantwoordelijke en verwerker. In deze handreiking worden de nieuwe benamingen gehanteerd.[10]

Onafhankelijkheid FG

Om zowel de belangen van de gemeente als van betrokkenen (zijnde burgers), de personen van wie informatie wordt verwerkt, doeltreffend te behartigen wordt een FG aangesteld als interne toezichthouder. De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies vanuit de gemeente en verwerkers.[11] Wel rapporteert de FG rechtstreeks aan het college van B&W over zijn werkzaamheden.[12] Er is overleg mogelijk met de AP, maar er is geen meldingsplicht bij de AP voor onregelmatigheden.[13] Tevens dient te worden voorkomen dat de FG in een spagaat terecht komt als de FG zich (teveel) met uitvoerende taken bezig houdt, de FG controleert dan in feite zijn eigen uitvoerende werkzaamheden. Deze situatie doet zich ook voor bij de adviserende rol van de FG. Dit komt de geloofwaardigheid en betrouwbaarheid niet ten goede.

Privacybeheerder BRP

De gemeenten hebben al een privacybeheerder in dienst voor de gegevensverwerkingen op grond van de Wet basisregistratie personen (BRP)[14], maar deze privacybeheerder BRP kijkt alleen naar de BRP en is (over het algemeen) alleen werkzaam binnen de afdeling burgerzaken. Gelet op de noodzaak van een onafhankelijke rolinvulling, wijst het college van B&W de privacybeheerder BRP aan. Het is te overwegen om uit praktisch oogpunt om de rol van de privacybeheerder BRP invulling te laten geven door de FG die verantwoordelijk is voor het totale privacybeheer van de gemeente. Anderzijds ligt de verantwoordelijkheid voor de juiste toepassing van de privacywetgeving in de teams. Door de privacybeheerder BRP als afzonderlijke rol te handhaven wordt deze verantwoordelijkheid benadrukt. De privacybeheerder als actiehouder en de FG als adviseur/toezichthouder zorgen zo voor de juiste naleving. Een ander aandachtspunt hierbij is of de privacybeheerder BRP wel de meest geschikte positionering heeft binnen de gemeente om de FG functie te vervullen. Het ligt het meest voor de hand om de FG een staffunctie te laten bekleden die nauw gelieerd is aan het college van B&W. Hierbij kan gedacht worden aan een positie binnen de afdeling Juridische Zaken of Concerncontrol.

Wat zijn de taken van een FG?

Het college van B&W is verantwoordelijk voor 'alles' wat te maken heeft met de bescherming van persoonsgegevens binnen uw gemeente en de FG ziet hier op toe, adviseert en stuurt. De FG heeft geen formele bevoegdheid om een bindend advies te geven, maar zijn oordeel is wel 'zwaarwegend'. De gemeente is wettelijk verplicht om de FG controlebevoegdheden te geven. Zo moet een FG bevoegd zijn om ruimten te betreden, zaken te onderzoeken en inlichtingen

en inzage te vragen.[15] Zie voor een uitgebreidere beschrijving het onderdeel 'Wat zijn de benodigde bevoegdheden voor een FG?' in deze handreiking. De FG informeert en adviseert bijvoorbeeld over de verplichtingen die uw gemeente op grond van de Wbp/AVG heeft, ziet toe op de toepassing en uitvoering van het beleid met betrekking tot de bescherming van persoonsgegevens, adviseert in de opzet van een structuur van verantwoordelijkheden en ziet toe op juiste toewijzing van verantwoordelijkheden aan medewerkers binnen uw gemeente, draagt zorg voor het opleiden en trainen van medewerkers die te maken hebben met gegevensverwerking en behandelt verzoeken[16] van betrokkenen om inzage of correctie.[17] Daarnaast is de FG de contactpersoon voor de AP.[18] De FG moet betrokken worden bij 'alle aangelegenheden die verband houden met de bescherming van persoonsgegevens'. De AVG geeft aan welke taken de FG (minimaal) heeft[19]:

- Het informeren en adviseren van de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen uit hoofde van de Wbp/AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van Wbp/AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van het gemeentelijke beleid of de verwerker met betrekking tot de bescherming van persoonsgegevens;
- Het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Het geven van advies met betrekking tot de Privacy Impact Assessment (PIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;[20,21,22]
- Het samenwerken met de AP;
- Het optreden als contactpunt voor de AP.

Bovenstaande taken van de FG worden hieronder verder uitgewerkt en toegelicht.

10 Artikel 4 lid 7 en 8 AVG
11 Artikel 38 lid 3 AVG
12 Zie ook de publicatie 'Informatieblad – Jaarverslag FG' van NGFG (http://www.ngfg.nl/download.php?id=12)
13 Zie hiervoor de Memorie van Toelichting Wbp, artikelen 63 en 64 blz. 185 (https://zoek.officielebekendmakingen.nl/kst-25892-3.html)
14 http://wetten.overheid.nl/BWBR0033715/ en de BRP betreft een lex specialis, de bepalingen in de BRP gaan boven die van de AVG.
15 http://wetten.overheid.nl/BWBR0005537/2016-07-01#Hoofdstuk5_Titeldeel5.2
16 Volgens artiekl 35 lid 1 Wbp heeft de betrokkene het recht zich vrijelijk en met redelijke tussenpozen tot de verwerkingsverantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De FG zou hierbij voorwaarden kunnen stellen zodat de verantwoordelijke op juiste manier deze verzoeken afhandeld. De FG heeft hierin dan een toezichthoudende taak.
17 Zie hiervoor de brochure 'De functionaris gegevensbescherming' van het AP.
18 Artikel 39 lid 1e AVG
19 Artikel 39 AVG
20 Artikel 35 AVG
21 Een PIA wordt in de AVG een gegevensbeschermingseffectbeoordeling of data protection impact assessment (DPIA) genoemd.
22 Zie hiervoor het operationele baseline product 'Toelichting PIA' van de IBD.

Inventariseren gegevensverwerkingen

Goed privacymanagement is de verantwoordelijkheid van het college van B&W en is gekoppeld aan de beginselen van behoorlijk bestuur. Colleges dragen zorg voor een behoorlijke, zorgvuldige gegevensverwerking in overeenstemming met de wet. Colleges dienen aan te kunnen tonen dat hun privacymanagement daaraan voldoet. Wie dat niet kan, loopt maatschappelijke, politieke en juridische afbreukrisico's. Een deskundige FG vervult hierbij een ondersteunende rol. Zicht hebben op de verwerking van persoonsgegevens is een belangrijke voorwaarde voor het uitoefenen van effectief toezicht. Een inventarisatie van de verwerkingsprocessen en de gegevensstromen binnen de gemeente is hiervoor onmisbaar. Ook kan de FG aangeven of er sprake is van een meldingsverplichting van gegevensverwerking. Deze meldingsverplichting rust overigens op het college van B&W en niet op de FG. Ook hierbij vervult de FG een adviserende rol. Zodra de AVG van toepassing is, hoeven de gegevensverwerkingen niet meer te worden gemeld bij de AP. Voor de Wbp hoeft de gegevensverwerking ook niet gemeld te worden als de verwerking valt onder het Vrijstellingsbesluit Wbp.[23,24] Er geldt vanaf dat moment wél een documentatieplicht. Dit houdt in dat het college van B&W, als zijnde de verwerkingsverantwoordelijke, een register van de verwerkingsactiviteiten bijhoudt[25] die onder hun verantwoordelijkheid plaatsvinden en dat de gemeente met documenten moet kunnen aantonen dat zij de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG te voldoen (accountability).

Adviseren over technologie en beveiliging

De FG dient alle betrokken partijen (het college van B&W en/of de verwerker) bij de gegevensverwerking te informeren en adviseren over hun verplichtingen naar aanleiding van de Wbp/AVG. Hieronder valt ook het adviseren over de PIA.[26] De verwerkingsverantwoordelijke is verplicht om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.[27] De FG kan de verwerkingsverantwoordelijke van advies voorzien voor het realiseren van een passend niveau van informatiebeveiliging, zodat de gegevens die worden verwerkt beter beschermd worden. Hierbij kan de FG nauw samenwerken met de Chief Information Security Officer (CISO).[28] Dit kan zowel betrekking hebben op de toegepaste technologie als het beveiligingsniveau, en ook over het toepassen van de principes gegevensbescherming door ontwerp (privacy by design) en door standaardinstellingen (privacy by default).[29] De FG kan het gebruik hiervan stimuleren en begeleiden. De beveiligingsmaatregelen moeten er ook op gericht zijn onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. In gevallen van twijfel kan de FG overleggen met de AP.[30]

Toezicht houden op naleving Wbp/AVG

De FG verricht stelselmatig onderzoek naar de wijze waarop persoonsgegevens worden verwerkt en beveiligd, zodat de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wbp/AVG bepaalde wordt uitgevoerd.[31] Hierbij kan de FG zich laten ondersteunen door (externe) specialisten. Het goed uitoefenen van toezicht omvat echter meer dan controleren en corrigeren. Hieronder valt ook het toezien of de uitvoering van de PIA volgens de regels wordt uitgevoerd.[32] 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. Er zijn verschillende instrumenten om te controleren of de gemeente persoonsgegevens op de juiste wijze beschermt.[33] De AP heeft hiervoor in samenwerking met koepelorganisaties en marktpartijen producten ontwikkeld. Dit betreft onder ander het Raamwerk Privacy Audit.[34] De gemeente kan zelf controleren of een product of dienst daadwerkelijk privacyproof is. Een PIA is een ander belangrijk product dat de gemeente kan helpen bij het zelf controleren of een product of dienst daadwerkelijk privacyproof is. Door een PIA krijgt de gemeente inzicht in de risico's die de gegevensverwerking met zich meebrengt voor de betrokkenen (de mensen van wie de organisatie persoonsgegevens verwerkt).

23 https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/europese-privacywetgeving#moet-ik-mijn-gegevensverwerkingen-straks-nog-melden-bij-de-ap-5579
24 https://autoriteitpersoonsgegevens.nl/nl/melden/handreiking-vrijstellingsbesluit-wbp
25 Artikel 30 lid 1 AVG
26 artikel 35 lid 1 AVG
27 Artikel 13 Wbp en Artikel 32 AVG
28 Zie hiervoor het operationele BIG product 'Handreiking IB-functieprofiel Chief Information Security Officer (CISO)' van de IBD
29 Artikel 25 AVG
30 Artikel 64 lid 4 Wbp
31 Artikel 64 lid 1 Wbp en Artikel 39 lid 1b AVG
32 artikel 35 AVG
33 Meer informatie vindt u onder Privacy Audit Proof op de website van de beroepsorganisatie van IT-auditors (NOREA). https://www.privacy-audit-proof.nl/
34 https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/raamwerk_privacyaudit.pdf en https://www.privacy-audit-proof.nl/globalassets/mijnsites/privacyauditproof/handreiking_rpa.pdf

Vragen en klachten afhandelen
De behandeling van klachten over het gebruik van persoonsgegevens kan deel uit maken van het takenpakket van een FG. Om klachten van betrokkenen doeltreffend te kunnen afhandelen, is het zaak dat de FG duidelijk herkenbaar en bereikbaar is. Dit kan bijvoorbeeld via de internetsite van de gemeente door middel van het publiceren van het privacyreglement of privacyverklaring[35]. Het is tevens denkbaar dat de FG een spreekuur houdt voor betrokkenen. Ook is het mogelijk om klachten die betrekking hebben op de verwerking van persoonsgegevens via het klantcontactcentrum (KCC) van de gemeente te laten lopen. De FG kan in dat geval als een specialist achter de schermen opereren.

Opstellen privacynormen, -beleid, -regelingen of -gedragscodes
Privacynormen kunnen de FG helpen om effectief toezicht te houden. Privacynormen zijn een praktische uitwerking van de privacyregels en afspraken, en geven de FG houvast bij het toezicht of de gemeente zich houdt aan de privacyregels en afspraken, zoals deze zijn vastgelegd met betrekking tot gegevensverwerking.[36] Het kan voor de FG en de gemeente ook praktisch zijn om een interne privacyregeling of -beleid op te stellen die specifiek is toegesneden op de gegevensverwerkingen binnen de gemeente. Dit is echter geen wettelijke verplichting. Een hieraan gerelateerde taak van de FG is het geven van voorlichting, waaronder bewustmaking en opleiding van de bij uitvoering betrokken professionals.

Samenwerken met AP
De FG zal samenwerken en overleggen met, en als contactpersoon optreden voor, de AP over zaken die met de gegevensverwerking verband houden, inclusief de voorafgaande raadpleging.[37, 38] Aanvullende informatie: Zie de website van de AP voor meer informatie over de taken en benoemingseisen van de FG.[39] Zie ook de brochure 'Privacywet en privacyfunctionaris' van het NGFG.[40] Dit document bevat een checklist voor de aanstelling van een FG. De FG kan ook lid worden van het NGFG.

Wat zijn de benodigde bevoegdheden voor een FG?
Het aanstellen van een FG brengt met zich mee dat de FG zijn plichten en taken onafhankelijk vervult en geen instructies ontvangt met betrekking tot de uitoefening van zijn functie. Daarnaast moeten aan de FG ook bevoegdheden worden toegekend. De AP heeft als externe toezichthouder een aantal instrumenten tot zijn beschikking om de naleving van de wettelijke bepalingen te bevorderen en af te dwingen. Dit betreft controlebevoegdheden en sanctiebevoegdheden. De FG beschikt niet over formele sanctiebevoegdheden, maar het college van B&W dient wel controlebevoegdheden aan de FG toe te kennen voor het uitoefenen van geloofwaardig en effectief toezicht op de naleving van de AVG. Deze controlebevoegdheden dienen overeen te komen met de taakomschrijvingen van de FG in de AVG[41] en de bevoegdheden die gelden voor het toezicht binnen de overheid.[42] 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)[43]. Hiermee heeft de FG (voldoende) instrumenten in handen voor het uitoefenen van geloofwaardig en effectief toezicht. 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.[44]

Betreden van ruimten
De interne regeling dient de FG mogelijkheden te geven om ongevraagd alle ruimten (desnoods serverruimten) te betreden, indien dit noodzakelijk is voor de uitoefening van zijn taak. De FG heeft uiteraard slechts de bevoegdheid tot het betreden van ruimten voor zover deze vallen binnen de reikwijdte van het toezicht.

Vragen van inlichtingen
De FG dient de bevoegdheid te hebben om de inlichtingen te verkrijgen die hij voor de uitoefening van zijn taak nodig heeft. 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. Indien de verwerkingsverantwoordelijke of diens ondergeschikten uit hoofde van hun ambt, beroep of wettelijk voorschrift verplicht zijn tot geheimhouding kan de medewerking worden geweigerd voor zover deze weigering uit de geheimhoudingsplicht voortvloeit.

Vragen van inzage
De FG zal, om zijn toezicht houdende rol goed uit te kunnen oefenen, bevoegd dienen te zijn om inzage te vragen van zakelijke gegevens en bescheiden. 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.

Onderzoeken van zaken
Het betreden van ruimten kan soms niet voldoende zijn om toezicht uit te oefenen. Het kan nodig zijn dat de FG toegang verkrijgt tot de (computer-)systemen waarin persoonsgegevens worden verwerkt. De FG zal desnoods de beschikking dienen te krijgen over de relevante inloggegevens. Tevens zal de FG op de hoogte dienen te zijn hoe, na het inloggen, de relevante bestanden kunnen worden bevraagd. De FG dient in staat te worden gesteld om zaken daadwerkelijk te onderzoeken.

35 Op de website Veilig internetten is een privacyverklaring (privacystatement) generator beschikbaar (https://www.veiliginternetten.nl/privacyverklaring)
36 Zie hiervoor het model 'privacyreglement' en 'privacybeleid' zoals door de VNG en KING opgesteld.
37 Artikel 36 AVG
38 Artikel 39 lid 1d en e AVG
39 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming
40 http://www.ngfg.nl/download.php?id=65
41 Artikel 39 AVG
42 Artikel 64 lid 3 Wbp en artikel 38 lid 2 AVG
43 http://wetten.overheid.nl/BWBR0005537/2016-07-01#Hoofdstuk5_Titeldeel5.2
44 Zie hiervoor de Memorie van Toelichting Wbp, Artikelen 63 en 64 blz. 185 (https://zoek.officielebekendmakingen.nl/kst-25892-3.html)

Over welke bagage dient de FG te beschikken?

De Wbp en AVG stellen een aantal algemene eisen aan de FG.[45] In de eerste plaats dient de FG aangewezen te worden op grond van zijn professionele kwaliteiten en dient de FG over toereikende kennis (op het gebied van wetgeving) te beschikken.[46,47] Ook zijn kennis van de bestuurlijke context, de gemeente, informatiebeveiliging / Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en softskills[48] ook belangrijk. In de tweede plaats dient de FG voldoende betrouwbaar te zijn. In het algemeen vereist zijn positie behoedzaam opereren. Het college van B&W dient er zorg voor te dragen dat de FG zijn controlebevoegdheden geloofwaardig en effectief kan uitoefenen. Daartoe dient de FG over voldoende faciliteiten te kunnen beschikken. Het college van B&W kan bijvoorbeeld besluiten om de FG een eigen budget te geven ten behoeve van zijn taakuitoefening

Toereikende kennis organiseren

Onder toereikende kennis wordt met name verstaan de kennis van de regels voor de bescherming van persoonsgegevens. Deze regels zijn niet beperkt tot de Wbp en AVG. Ook kennis van voor gemeenten toepasselijke wetgeving zoals de Wet maatschappelijke ondersteuning (Wmo) 2015[49] en de Jeugdwet[50], die specifieke privacyregels bevatten, alsmede gemeentelijke regelgeving, is noodzakelijk voor het goed functioneren van een FG. Het is verder aan te bevelen dat de FG deskundig is op het gebied van de informatie- en communicatietechnologie (ICT). Kennis van zowel wetgeving en ICT gecombineerd in een persoon is schaars. Er zal naar een praktische oplossing gezocht dienen te worden, waarbij de FG niet noodzakelijkerwijs een jurist hoeft te zijn. Een jurist heeft wellicht een te verkokerde blik. De niet-juridisch (getrainde) FG zal wel voldoende kennis van het specifieke vakgebied dienen te hebben. Het blijft lastig om duidelijke uitgangspunten voor de functievervulling van de FG op te stellen. De slotconclusie is dat de FG over een brede kennis, tact en diplomatie dient te beschikken en kunnen verbinden en bevragen. Tevens dient de FG over informatiseringskennis te beschikken om in processen en informatiesystemen te kunnen denken en advies kan vragen bij zowel de afdelingen die de processen uitvoeren, als automatisering en juristen. Om aan tonen dat de FG over voldoende deskundigheid beschikt die noodzakelijk is om de functie te kunnen uitvoeren, kan een FG worden geselecteerd op grond van behaalde certificaten. 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)[51] en Certified Information Privacy Manager (CIPM)[52] het meest relevant. Naast deze privacy certificeringen zijn er nog de Certified Data Protection Officers (CDPO)[53] en Privacy & Data Protection Certification (CDPO)[54] certificeringen.

Betrouwbaar

Het is goed denkbaar dat het college van B&W de voorkeur geeft aan een kandidaat met een lange staat van dienst: een medewerker die zijn betrouwbaarheid reeds bewezen heeft. Het college van B&W kan dit zelf het best beoordelen. De betrouwbaarheid van de FG is vooral in het belang van betrokkenen waar het gaat om vertrouwelijke informatie over betrokkenen. De gemeente heeft er evenzeer belang bij dat de FG op zorgvuldige en betrouwbare wijze met gevoelige informatie omgaat. Het kan dan gaan om bedrijfsgeheimen, zoals de beveiliging van computersystemen. De betrouwbaarheid uit zich met name in het vermogen alle belangen gemoeid met de verwerkingen op een onafhankelijke wijze tegen elkaar af te kunnen wegen. De FG dient in staat te zijn op een juiste en zorgvuldige wijze gebruik te maken van zijn bevoegdheden zoals beschreven in het deel ‘Wat zijn de benodigde bevoegdheden voor een FG?’ in deze handreiking.

Diplomatiek optreden

De FG dient op onafhankelijke wijze toezicht uit te oefenen. Hierbij zijn verschillen van inzicht met het college van B&W niet uit te sluiten. Bij het uitoefenen van toezicht op de naleving van de Wbp en AVG kunnen gemeentelijke belangen lijken te conflicteren met privacybelangen. Er dienen dus hoge eisen te worden gesteld aan de diplomatieke vaardigheden van de FG.

45 Artikel 63 lid 1 Wbp en Artikel 37 lid 5 AVG.
46 Artikel 37 lid 5 AVG
47 Zie hiervoor ook het functieprofiel FG van KING.
48 Softskills is een verzamelnaam voor onder andere de persoonlijke eigenschappen, sociale vaardigheden en communicatieve vaardigheden.
49 http://wetten.overheid.nl/BWBR0035362/
50 http://wetten.overheid.nl/BWBR0034925/
51 https://iapp.org/certify/cippe/
52 https://iapp.org/certify/cipm/
53 http://registercdpo.nl/
54 https://www.seco-institute.org/courses/data-protection-certification-track

MEER INFORMATIE EN VRAGEN

VIA DE WEBSITES VNG.NL EN WWW.KINGGEMEENTEN.NL HOUDEN WE U OP DE HOOGTE VAN ALLE NIEUWE PRIVACY ONTWIKKELINGEN. INDIEN U NAAR AANLEIDING VAN DEZE FACTSHEET NOG VRAGEN HEEFT, HULP NODIG HEEFT BIJ DE IMPLEMENTATIE VAN EEN PRIVACYBELEID IN UW GEMEENTE OF ADVIES WIL OVER DE WBP, AVG OF PRIVACY IN HET ALGEMEEN DAN KUNT U UW VRAGEN STELLEN VIA HET E-MAILADRES: PRIVACY@KINGGEMEENTEN.NL