Nota voor burgemeester en wethouders
Onderwerp
Benoemen Functionaris Gegevensbescherming (FG)

Team
DEV-CS

1- Notagegevens	
Notanummer	2018-000918
Datum	09-05-2018
Programma:	
01 Burger en bestuur	
Portefeuillehouder Burgemeester	

2- Bestuursorgaan	
[X]B & W	22-05-2018
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Kolkman
- Weth. Grijsen	- Weth. Rorink

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[X]Openbaar	22-05-2018	[ ]Besloten	--

Routing	d.d.
Directeur	09-05-2018
Burgemeester	14-05-2018

par.	
[ ]adj.secr.	--
[X]gem.secr.	14-05-2018
BIS Openbaar	
Status	Definitief2018-05-23

Bijlagen

B & W d.d.: 22-05-2018

Besloten wordt:
1 De heer Rien Hommes van RSM Nederland Risk Advisory Services B.V tot 1 januari 2020 te benoemen tot Functionaris Gegevensbescherming als bedoeld in artikel 37 van de Algemene Verordening Gegevensbescherming (AVG);
2 de nota en het besluit openbaar te maken, m.u.v. de bijlagen met persoonlijke gegevens.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[ ] De nota en het besluit openbaar te maken
[ ] De nota en het besluit openbaar te maken vergezeld van bijgaand persbericht
[ ] De nota en het besluit openbaar te maken nadat

[X] De nota en het besluit openbaar te maken, behalve…
de niet openbare bijlagen in verband met persoonlijke gegevens.
[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

[ ] De nota en het besluit niet openbaar te maken, gelet op artikel:

Kennisgeving/ Bekendmaking Awb

Kennisgeving (publicatie) conform Awb	Nee
Bekendmaking conform Awb	Nee

ADVIESRADEN:

Moet een van de adviesraden gehoord worden of op de hoogte gesteld? Nee

Toelichting

Inleiding

Op grond van de Algemene Verordening Gegevensbescherming (AVG) die op 25 mei a.s. volledig in werking treedt, zijn gemeenten verplicht een Functionaris Gegevensbescherming (FG) aan te wijzen. Dit is iemand die binnen de gemeente onafhankelijk toezicht houdt op de toepassing en de naleving van de AVG. Hij is tevens aanspreekpunt voor burgers, voor de verantwoordelijke (het college) en voor de Autoriteit Persoonsgegevens (AP). De FG levert daarmee een belangrijke bijdrage aan correct gebruik van persoonsgegevens door de gemeente. Een document van de VNG met meer informatie over rol en taken van de FG treft u bijgevoegd aan.

In het kader van de DOWR-samenwerking is na een onderhandse aanbesteding onder drie partijen gekozen voor een externe FG tot 1 januari 2020. Voorgesteld wordt om Rien Hommes van RSM Nederland Risk Advisory Services B.V. aan te stellen. Hij voldoet qua kennis, achtergrond en kwalificaties aan de te stellen criteria en heeft eerder IT-audtis voor de DOWR-I verzorgd. Ook Raalte en Olst-Wijhe zullen hem aanstellen als FG. Verwezen wordt naar bijgaande offerte en CV.

Voor wat betreft de voorbereidingen op de AVG zullen we als gemeente Deventer op 25 mei a.s. nog niet volledig AVG-proof zijn. De Autoriteit Persoonsgegevens (AP) heeft recent via de VNG laten weten niet meteen boetes uit te gaan delen. Wel dient er een FG aangewezen te zijn, hetgeen via dit besluit geregeld is, en een serieus begin te zijn gemaakt op basis van een duidelijk plan. Als het gaat om het plan heeft de directie onlangs het implementatieplan “Grip op privacy” vastgesteld (bijgevoegd). Dit plan bevat concrete actiepunten die inmiddels gerealiseerd c.q. in uitvoering zijn:

- op 16 januari jl. heeft uw college een beleidskader vastgesteld;
- er loopt een wervings-/selectieprocedure voor een juridisch adviseur/Privacy Officer, de interne sleutelfunctionaris op het gebied van AVG en privacy;
- er is door de directie een Privacy Impact Team (PIT) en een stuurgroep privacy ingesteld;
- veel teams binnen de organisatie hebben in het kader van de bewustwording een presentatie gehad over de AVG en de verdere aanpak;
- de werkprocessen met de grootste privacy-risico’s in het sociaal domein en bij veiligheid worden door middel van procesplannen in beeld gebracht en aangepast aan de AVG; vervolgens zullen de andere gemeentelijke werkprocessen waarbij persoonsgegevens worden verwerkt, successievelijk volgen.

Beoogd resultaat

De FG levert een belangrijke bijdrage aan correct gebruik van persoonsgegevens door de gemeente.

Kader

Artikel 37 van de Algemene Verordening Gegevensbescherming (AVG)

Argumenten voor en tegen

Wettelijke verplichting

Extern draagvlak (partners)

Afgestemd in directieberaad DOWR

Financiële consequenties

De hieraan verbonden voorzienbare kosten kunnen worden gedekt vanuit het werkbudget privacy (H6.3106.100.00). In het geval dat extra inzet van de FG nodig is (bv. onderzoek AP, bijzondere vragen van burgers, nader advies/ondersteuning van de organisatie) zal aanvullende dekking gezocht moeten worden binnen de lopende begroting.

Aanpak/uitvoering

Na besluitvorming door uw college zullen nadere afspraken worden gemaakt met de FG over diens werkprogramma.

RAADSMEDEDELING

Onderwerp	Benoemen Functionaris Gegevensbescherming (FG)		
Mededelingennr	2018-000918	**Portef.houder**	Burgemeester
Team	DEV-CS	**BenW-besluit d.d.:**	22 MEI 2018

1. Inleiding: waarom deze mededeling

Op grond van de Algemene Verordening Gegevensbescherming (AVG) die op 25 mei a.s. volledig in werking treedt, zijn gemeenten verplicht een Functionaris Gegevensbescherming (FG) aan te wijzen. Dit is iemand die binnen de gemeente onafhankelijk toezicht houdt op de toepassing en de naleving van de AVG. Hij is tevens aanspreekpunt voor burgers, voor de verantwoordelijke (het college) en voor de Autoriteit Persoonsgegevens (AP). De FG levert daarmee een belangrijke bijdrage aan correct gebruik van persoonsgegevens door de gemeente.

In het kader van de DOWR-samenwerking is na een onderhandse aanbesteding onder drie partijen gekozen voor een externe FG tot 1 januari 2020. Besloten is om Rien Hommes van RSM Nederland Risk Advisory Services B.V. aan te stellen. Hij voldoet qua kennis, achtergrond en kwalificaties aan de te stellen criteria en heeft eerder IT-audits voor de DOWR-I verzorgd. Ook Raalte en Olst-Wijhe zullen hem aanstellen als FG.

2. Kader

Artikel 37 van de Algemene Verordening Gegevensbescherming (AVG)

3. Kern van de boodschap

Informeren over het benoemen van een Functionaris Gegevensbescherming (FG)

4. Nadere toelichting

Voor wat betreft de voorbereidingen op de AVG zullen we als gemeente Deventer op 25 mei a.s. nog niet volledig AVG-proof zijn. De Autoriteit Persoonsgegevens (AP) heeft recent via de VNG laten weten niet meteen boetes uit te gaan delen. Wel dient er een FG aangewezen te zijn en een serieus begin te zijn gemaakt op basis van een duidelijk plan. Voor wat betreft dit laatste punt heeft de directie het implementatieplan “Grip op privacy” vastgesteld. Dit plan bevat concrete actiepunten die inmiddels gerealiseerd en ook in uitvoering zijn:

- Op 16 januari jl. heeft ons college een beleidskader vastgesteld (ter informatie aan de Raad gestuurd op 18 januari 2018);
- Er loopt een wervings-/selectieprocedure voor een juridisch adviseur/Privacy Officer, de interne sleutelfunctionaris op het gebied van AVG en privacy; r loopt een wervings-/selectieprocedure voor een juridisch adviseur/Privacy Officer, de interne sleutelfunctionaris op het gebied van AVG en privacy;
- Er is door de directie een Privacy Impact Team (PIT) en een stuurgroep privacy ingesteld;
- Veel teams binnen de organisatie hebben in het kader van de bewustwording een presentatie gehad over de AVG en de verdere aanpak;
- De werkprocessen met de grootste privacy-risico’s in het sociaal domein en bij veiligheid worden door middel van procesplannen in beeld gebracht en aangepast aan de AVG; vervolgens zullen de andere gemeentelijke werkprocessen waarbij persoonsgegevens worden verwerkt, successievelijk volgen.

gemeente Deventer

Grip op privacy

Implementatieplan privacy en gegevensbescherming
april 2018

Uitgave : versie 4 (ter vaststelling directie)
Naam : A.W. van Hennik
Telefoonnummer : 693908/ 06-12343437
Mail : aw.van.hennik@deventer.nl

Inhoud

1 Inleiding

Voor u ligt het implementatieplan *Grip op privacy* waarin de stappen en acties zijn opgenomen die in de komende periode nodig zijn om op een aantoonbare wijze naleving van de privacywetgeving te borgen in de organisatie van de gemeente Deventer.

De in dit plan vermelde actiepunten zijn gebaseerd op prioritering vanuit een risicoafweging wetende dat niet alle activiteiten zijn te realiseren vóór 25 mei 2018. Dat is namelijk de datum waarop de Algemene Verordening Gegevensbescherming (AVG) gehandhaafd wordt en elke organisatie in de private en publieke sector hun bedrijfsvoering in overeenstemming moet hebben gebracht met deze verordening om volledig te voldoen aan de privacywetgeving. Het niet of deels voldoen aan de AVG kan grote gevolgen hebben voor gemeenten in termen van reputatieschade, boetes en schadeclaims.

De Autoriteit Persoonsgegevens (AP) heeft recent via de VNG laten weten niet meteen boetes uit te gaan delen. Wel dient er een FG aangewezen te zijn en een serieus begin te zijn gemaakt op basis van een duidelijk plan. Dit implementatieplan "*Grip op privacy*" fungeert als zodanig.

Dat we niet alles voor deze datum realiseren heeft te maken met (1) het startmoment, (2) het gegeven dat de gemeente opereert in een omvangrijke en complexe omgeving en (3) er tijd nodig was om helder te krijgen welke consequenties de AVG ging hebben en die consequenties om te zetten in een organisatie-brede aanpak met nieuwe en aangescherpte procedures, richtlijnen en regels. Zo zullen de noodzakelijke procesplannen (zie verder $3.8) niet voor die datum zijn opgesteld maar zullen we wel de eerste stappen hebben gezet vanuit een prioritering.

De AVG is strakker geregeld dan de Wbp en een van de belangrijkste nieuwe eisen is dat de gemeente naleving van de privacyregels op aantoonbare wijze borgt en daarover rekenschap (accountability) aflegt. Dat betekent dat een gemeente onder meer met documentatie moet kunnen aantonen dat de juiste organisatorische en technische maatregelen zijn geïmplementeerd om te voldoen aan de AVG en deze documentatie ook blijvend onderhoudt. Hierop zullen we ons moeten gaan voorbereiden.

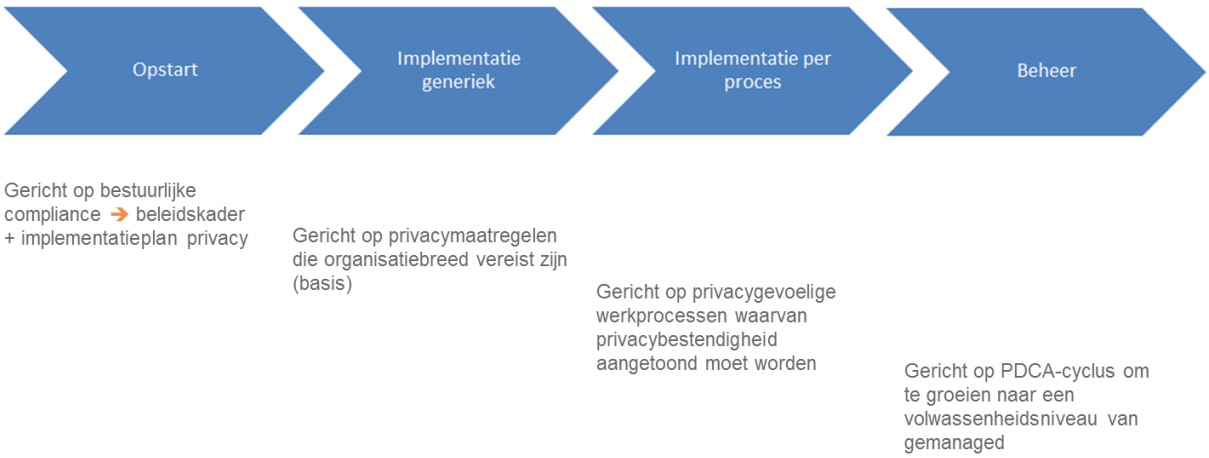
Grip op privacy haakt in op de eisen van de AVG en is mede gebaseerd op het privacy-beleidskader zoals dat in januari 2018 door het college is vastgesteld. Dit beleidskader bevat de algemene kaders en managementafspraken voor het vormgeven van privacy in de gemeentelijke organisatie.

Het implementatieplan privacy loopt tot eind 2018, met de intentie dit document in het laatste kwartaal van 2018 te actualiseren en een nieuw plan op te stellen voor 2019 met als oogmerk dat privacy uiteindelijk in de pas gaat lopen met de jaarlijks terugkerende P&C cyclus van de gemeente.

2 Aanpak

2.1 Risicogebaseerde benadering

De uitgangspunten voor de aanpak liggen vast in artikel 24 AVG[1]. Om grip te krijgen en te behouden op de AVG is een risicogebaseerde benadering nodig zonder het privacydoel uit het oog te verliezen. Dit moet worden ingekaderd in een cyclisch PDCA-proces met het devies dat het proces de inhoud borgt en waarbij samenwerking en communicatie sleutelwoorden zijn. Er is een overlap met informatieveiligheid dat eveneens via een cyclisch PDCA-proces wordt geborgd. Waar nodig komt dan ook specialistische privacykennis in beeld en handelen we met deze benadering zoveel mogelijk naar de bedoeling en niet naar de letter van de wet. Deze benadering is schematisch als volgt weergegeven:



Het implementatieplan is onderdeel van de opstartfase en primair gericht op de privacymaatregelen die organisatiebreed noodzakelijk zijn en op de privacygevoelige werkprocessen waarvan de privacybestendigheid aangetoond moet worden. Denk in dat kader onder andere aan de WMO, Jeugdzorg en Participatie maar ook aan Veiligheid. De input voor de generieke maatregelen is afkomstig uit een uitgevoerde nulmeting waarvan de resultaten zijn geprioriteerd aan de hand van een impactanalyse. Het beheerdeel nemen we ook mee en krijgt naar gelang het ‘privacyhuis’ staat meer vorm en inhoud.

Voor de implementatie per proces is vooraf inzicht nodig in de privacygevoelige werkprocessen die voor nader onderzoek (documenteren) in aanmerking komen. Van belang is dat dit geschiedt in dialoog met het management vanwege de vervolgtrajecten die hieraan zijn verbonden en die vrij arbeidsintensief zijn. In $ 3.8 gaan we hierop nader in.

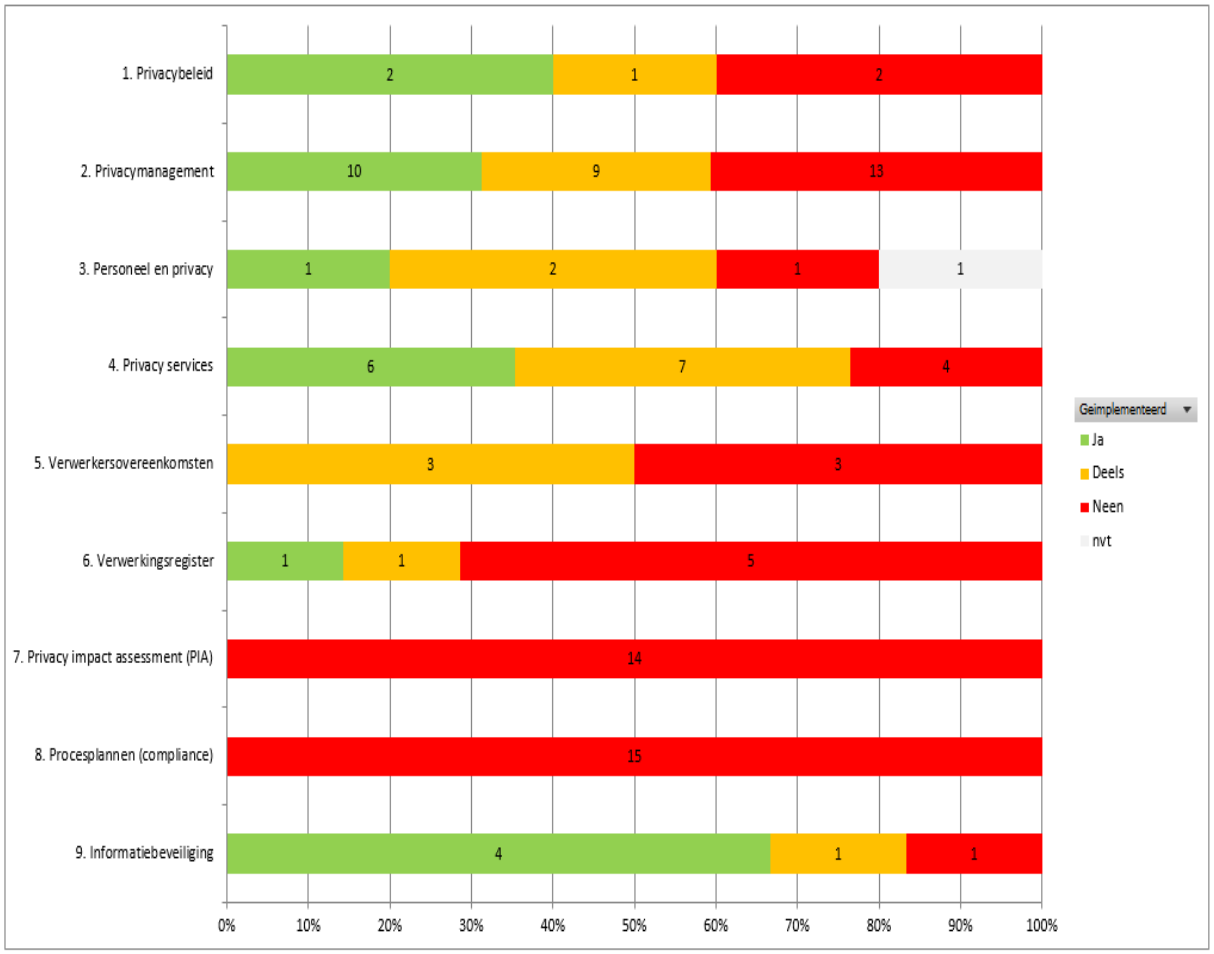
[1] Zie artikel 24 AVG: Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

2.2 Resultaten nulmeting privacy

De ambitie is om uitgaande van het privacy groeimodel toe te werken naar een niveau 4 :gemanaged, met als typering: organisatiebreed privacy-beleid gekenmerkt door hoge awareness en bijsturing van beheersmaatregelen op basis van meetbaarheid, rekenschap en periodieke evaluaties.

Daartoe worden negen thema's onderscheiden met per thema specifieke aandachtspunten. Op die basis is een nulmeting uitgevoerd in samenwerking met de directeur implementatie AVG/privacy, de teammanagers Planning & Control, I-werkorganisatie, Inkomensondersteuning en Belastingen, alsmede de CISO, de Privacy Offcer en de kwartiermaker privacy .

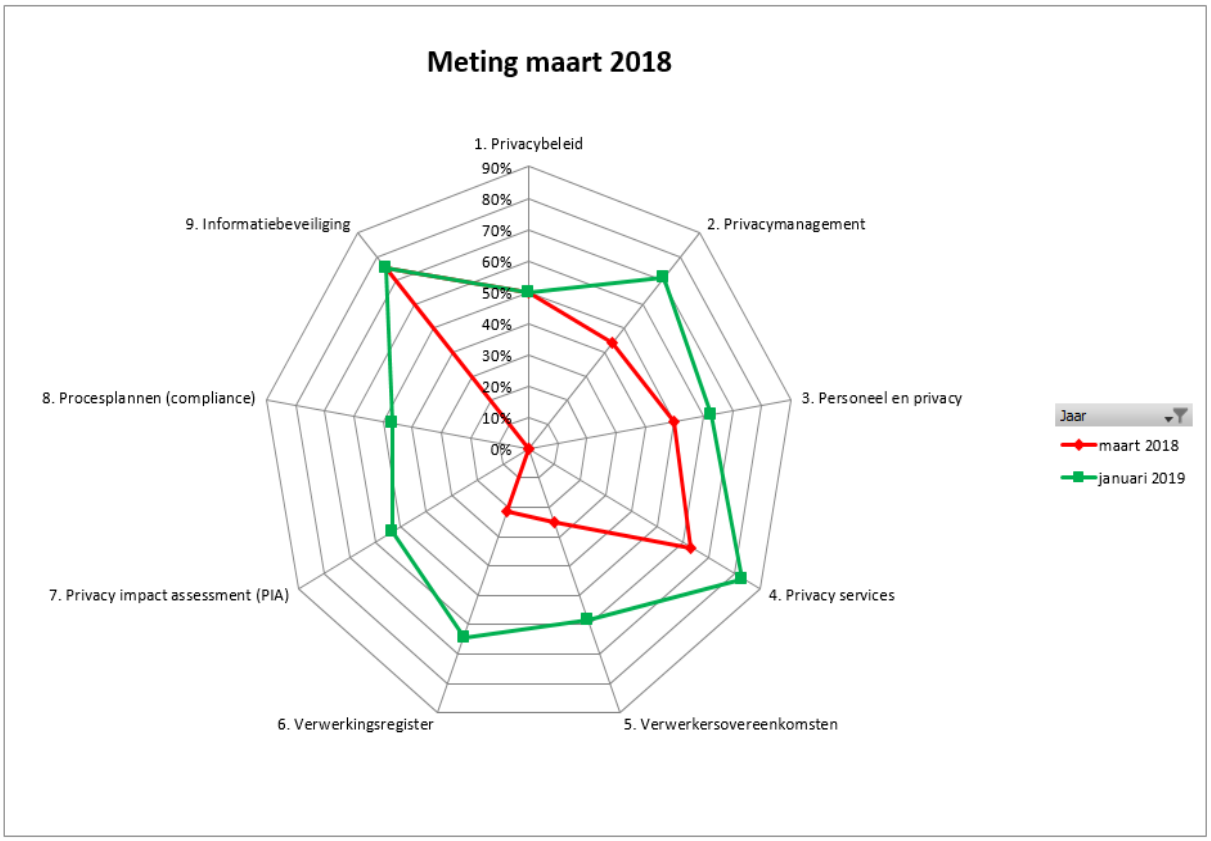
Dit geeft het volgende resultaat:



De gemiddelde score op dit moment is **32%**. Op de meeste thema's zijn stappen gezet (groen en oranje) maar er moet nog veel (rood) gebeuren waarbij prioritering van groot belang is, wetende dat er op 25 mei 2018 niet volledig voldaan gaat worden aan de privacywetgeving.

De aandachtspunten van de diverse thema's zijn vertaald in concrete actiepunten die de komende maanden uitgevoerd moeten gaan worden. Het streven is om eind 2018 uit te komen op een gemiddelde score van **80 %.**

Grafisch ziet deze verbetering voor de privacy-thema's er als volgt uit:



3 Actiepunten

3.1 Privacy-beleid

De basis voor actief sturen is een overkoepelend privacy-beleid waarin de gemeente haar visie verwoordt en aangeeft op welke wijze persoonsgegevens behoorlijk, zorgvuldig en in overeenstemming met de wet worden verwerkt.
Het beleidskader privacy en gegevensbescherming is op 16 januari jl. door B&W vastgesteld en gedeeld met de gemeenteraad.

3.2 Privacy-management

Met privacy-management wordt bedoeld alle maatregelen die ervoor zorgen dat de gemeente zich houdt aan de AVG en daarover verantwoording (accountability) aflegt. Daarbij sluiten we zoveel mogelijk op reeds bestaande (overleg)structuren en procedures in het kader van de PDCA-cyclus. Privacy-management is dus gericht op het uitvoeren van het privacy-beleidskader.

3.2.1 Inrichten

Functionaris Gegevensbescherming (FG)
Onder de Algemene Verordening Gegevensbescherming (AVG) wordt het aanstellen van een FG, een interne toezichthouder op de verwerking van persoonsgegevens, voor de gemeente verplicht.

De FG moet zonder instructies zijn werkzaamheden uit kunnen voeren en rapporteert rechtstreeks aan de algemeen directeur over zijn werkzaamheden. De FG heeft geen formele bevoegdheid om een bindend advies te geven, maar zijn oordeel is wel ‘zwaarwegend’. De FG moet zelfs controlebevoegdheden krijgen om ruimten te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen.

De AVG geeft aan welke taken de FG (minimaal) heeft:

- informeren en adviseren van de gemeente/verwerkers over hun verplichtingen uit hoofde van de AVG en andere wet- en regelgeving omtrent gegevensbescherming;
- toezien op naleving van de AVG en andere wet- en regelgeving omtrent gegevensbescherming;
- toezien op naleving van het gemeentelijke beleid met betrekking tot de bescherming van persoonsgegevens;
- toezien op toewijzing van verantwoordelijkheden, bewustwording en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- adviseren over DPIA’s en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- contactpersoon voor en samenwerken met de AP

De FG kan een eigen medewerker zijn maar kan ook extern worden ingehuurd. Het plan is om in DOWR-verband een gezamenlijke FG te benoemen die de wettelijke rol per onderscheiden gemeente uitvoert.

Privacy Officer (PO)
De Privacy Officer is het centrale aanspreek- en ankerpunt voor management, organisatie en FG op het gebied van AVG en privacy. Daarnaast adviseert en ondersteunt de PO bij het implementeren van de privacy-aanpak en –maatregelen.

Op dit moment is de Privacy Officer tijdelijk ingehuurd. Over deze functie moet op korte termijn besluiten worden genomen om een toereikende en meer structurele inzet te borgen.

Proceseigenaren
Het benoemen van proceseigenaren is nodig om de governance van de privacy tot op werkprocesniveau eenduidig te regelen. De teammanagers zijn in beginsel aangewezen als proceseigenaren en zijn verantwoordelijk voor de uitvoering van de privacybescherming. Van proceseigenaren wordt verwacht dat de verwerking van persoonsgegevens rechtmatig en zorgvuldig plaatsvindt in lijn met de AVG en dat elke proceseigenaar dit kan aantonen. Daartoe kunnen zij via de Privacy Officer een beroep doen op het concern voor ondersteuning en begeleiding.
Dit vereist een gestructureerde werkwijze waar in $3.8 nader op wordt ingegaan.

3.2.2 Organisatie

Het is van belang dat de onderlinge samenwerking tussen de directie, management en proceseigenaren, Privacy Officer, CISO en FG wordt beschreven rekening houdend met de daarbij behorende verantwoordelijkheden, taken en rollen in een PDCA-cyclus. Het doel is om grip op privacy te krijgen en te blijven houden en daarvoor toe te werken naar een effectief data protection managementsysteem (DPMS) onder beheer van de Privacy Officer. Ook het samenwerken op het gebied van informatieveiligheid is een must omdat privacy en informatieveiligheid veel met elkaar gemeen hebben en vergelijkbare doelen nastreven en middelen hanteren.

Privacy Impact Team (PIT)
Om de samenwerking, slagkracht en continuïteit op de disciplines privacy en informatieveiligheid te versterken en te voorkomen dat individuele initiatieven stranden, biedt het instellen van een Privacy Impact Team (PIT) een oplossing. Dat team is een permanent adviesorgaan voor de directie en bestaat uit de directeur implementatie AVG/privacy, de CISO, de Privacy Officer, de FG en de kwartiermaker privacy.

Het PIT behandelt alle tactische en operationele vraagstukken op het gebied van privacy en informatieveiligheid en ontzorgt daarmee de directie op inhoudelijke vraagstukken en creëert aldus meerwaarde voor de organisatie.

Stuurgroep Privacy
Daarnaast is een stuurgroep ingesteld die bestaat uit de leden van het PIT, aangevuld met de teammanagers Planning & Control, I-werkorganisatie, Inkomensondersteuning en Belastingen alsmede de regiemanager sociaal domein.

3.2.3 Risicomanagement

Het inzetten van risicomanagement is een belangrijk instrument om de doelstelling rond privacybescherming te realiseren. Immers er is een voortdurende afweging van belangen van personen over wie persoonsgegevens verwerkt worden en belangen van de gemeente die de gegevens verwerkt. De AVG biedt hiervoor ook ruimte.

Belangrijk onderdelen van risicomanagement zijn vanuit een cyclisch PDCA-proces het:

- periodiek uitvoeren van een zelfevaluatie en een daaraan gerelateerde impactanalyse;
- classificeren van elk hoofdproces naar een hoog, gemiddeld of laag privacy-risico. Deze prioritering geeft inzicht voor welke werkprocessen de privacy-bestendigheid als eerste in beeld gebracht moet worden;
- uitvoeren van Data protection impact assessments (DPIA's)[2] ingeval sprake is van een hoog risico voor rechten en vrijheden van natuurlijke personen volgens een daarvoor vastgestelde procedure en werkwijze;
- toetsen op naleving van de AVG op risicovolle onderdelen (monitoring en auditing).

Het implementatieplan kent een risico-gebaseerde aanpak. Dat betekent dat we beginnen met de verwerkingen met een hoog privacy-risico in het veiligheids- en sociale domein. Voor het uitvoeren van DPIA's verwijzen we naar $3.7.

Het toetsen op naleving werken we in dit implementatieplan nog niet uit. Dat komt later als de privacy-organisatie staat en diverse andere maatregelen zijn geïmplementeerd.

3.2.4 Middelen

Het op een aantoonbare wijze verankeren van privacybescherming in de gemeentelijke organisatie zoals bedoeld in de AVG heeft een forse impact op de organisatie en vereist voldoende beschikbare middelen. Denk in dat kader aan structurele middelen voor de Privacy Offcer en voor de FG, bewustwording en doelgerichte trainingen van medewerkers op privacybestendig werken, het vergroten van privacy-kennis en het beschikbaar stellen van middelen om werkprocessen privacy-bestendig te maken en dit ook te kunnen aantonen (documenteren).

Deze autonome ontwikkeling vergt extra incidentele en structurele middelen welke via de Voorjaarsnota 2018 bij de raad zullen worden aangevraagd. .

3.3 Personeel en privacy

Communicatie naar het personeel en het inzetten van bewustwordingsprogramma's op het gebied van privacybescherming is een actiepunt met als doel te groeien naar een privacy bewuste organisatiecultuur en het aantal datalekken vanuit menselijk handelen te minimaliseren. Daarbij is de insteek aan te sluiten bij de reeds in gang gezette bewustwordingsprogramma's rond informatieveiligheid en in een latere fase te zoeken naar een evenwichtige benadering van beide disciplines. Bewustwording is een doorlopend programma van lange adem en de inzet/effectiviteit met de benodigde middelen van dit instrument behoort jaarlijks te worden geëvalueerd.

[2] In de vertaling van de AVG is gekozen voor de term 'gegevensbeschermingseffectbeoordeling' (GEB) en in de oorspronkelijke tekst wordt gesproken van Data Protection Impact Assessment (DPIA). Dit laatste sluit beter aan op de PIA die in de Wbp wordt gehanteerd.

Voorts is een privacy-protocol nodig waarin gedragsregels staan hoe om te gaan met het verwerken van persoonsgegevens zoals het verstrekken van gevoelige gegevens aan collega's en derden. Dit protocol behoort kenbaar te worden gemaakt aan iedereen en persoonlijk te worden overhandigd bij elke nieuwe aanstelling of externe inhuur. Een belangrijk uitgangspunt voor het nog op te stellen protocol is het opnemen van een zekere terughoudendheid met het verstrekken van persoonsgegevens aan collega's en aan derden.

3.4 Privacy services

Privacy services is gericht op alle activiteiten die betrekking hebben op het waarborgen van de rechten van burgers en andere betrokkenen volgens de AVG.

3.4.1 Transparantie

Van belang is om PR- en communicatieactiviteiten rond de rechten van betrokkenen te bevorderen, enerzijds om transparant te zijn naar de burgers op welke wijze de gemeente omgaat met het beschermen van persoonsgegevens (publieksvoorlichting), anderzijds om de rechten van betrokkenen kenbaar te maken. De proceseigenaren voorzien zo nodig in bijzondere voorlichting aan specifieke doelgroepen. Hierbij kan onder andere gedacht worden aan doelgroepen in het sociaal domein.
Via de procesplannen wordt hier per verwerking aandacht aan besteed.

3.4.2 Rechten betrokkenen

De AVG besteedt uitvoerig aandacht aan de rechten van betrokkenen en stelt hiervoor hoge eisen aan organisaties. Dit onderdeel krijgt in dit plan een minder hoge prioriteit vanwege de verwachting dat een beroep op de rechten van betrokkenen in 2018 beperkt zal zijn. Het inregelen van deze rechten loopt eveneens mee in het privacy-proof maken van de verwerkingen via de procesplannen.

3.5 Verwerkersovereenkomsten

Bij het uitbesteden van de verwerking van persoonsgegevens verplicht de AVG tot het sluiten van een schriftelijke overeenkomst indien de "verantwoordelijke" (lees: B&W) persoonsgegevens laat bewerken door een "verwerker" (externe ICT-leveranciers en andere externe partijen waaraan gemeentelijke werkzaamheden zijn uitbesteed en waarbij persoonsgegevens worden verwerkt). Dit is de zgn. *verwerkersovereenkomst.*

Naast het opstellen van verwerkersovereenkomsten is ook aandacht nodig voor periodiek toezicht op naleving van deze overeenkomsten. Dit valt onder contractenbeheer dat vanuit het domein informatieveiligheid wordt opgepakt.

Als het gaat om uitwisseling van persoonsgegevens met ketenpartners in bijvoorbeeld het sociaal domein dan komt dit specifiek aan de orde bij het opstellen van procesplannen (zie $ 3.8).

3.6 Verwerkingsregister

Een van de eisen is dat de gemeente een verwerkingsregister inricht en bijhoudt conform artikel 30 AVG van alle verwerkingen van persoonsgegevens waarvoor de gemeente verantwoordelijk is. Er is immers inzicht nodig in alle verwerkingen van persoonsgegevens met vermelding voor welk doel we dit doen, waar deze gegevens vandaan komen en met wie we deze delen.

Gelet op het belang is een procedure nodig voor het beheer en gebruik van een verwerkingsregister en behoort een register te worden ingericht. Het verwerkingsregister is overigens geen openbaar document.

In tegenstelling tot veel andere maatregelen in de AVG is er voor het verwerkingsregister geen sprake van een risico-gebaseerde benadering. Formeel betekent dit dat elke verwerking van persoonsgegevens in het verwerkingsregister moet zijn vastgelegd hoe onbeduidend die ook is. Het gaat dan wel overigens om structurele verwerkingen. Op dit moment is het opleveren van een volledig verwerkingsregister niet haalbaar en onze insteek is om dit in een periode van twee jaar te realiseren. Daarbij wordt een beroep gedaan op alle proceseigenaren om elke verwerking van persoonsgegevens te melden c.q. af te stemmen met de Privacy Officer. Ook afstemming met de dataclassificatie uit het domein informatieveiligheid kan bijdragen tot een volledig beeld voor het verwerkingsregister.

Van elke vastlegging in het register wordt gebruik gemaakt van een standaard artikel 30-formulier. De bedoeling is dat elk verwerkt formulier in het register is ondertekend door de betreffende proceseigenaar en dat de Privacy Officer is belast met het beheer van het verwerkingsregister.

Het verwerkingenregister is inmiddels als licentie op een webapplicatie aangeschaft waarbij aangesloten is bij hetzelfde framework als voor informatieveiligheid wordt gebruikt.

3.7 Data Protection Impact Assessments (DPIA's)

Een van de eisen uit de AVG is dat een DPIA verplicht is als de verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Daarbij gaat het dus niet om eventuele risico's voor de organisatie zoals boetes en claims. Een DPIA is een methode om risico's voor de rechten en vrijheden van betrokkenen in beeld te krijgen en daarvoor maatregelen in te zetten waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen.

Een DPIA is aldus een risico-instrument en niet primair bedoeld om daarmee de compliance van een werkproces aan te tonen. Immers als een DPIA voor een verwerking niet nodig is dan geldt nog steeds dat moet worden voldaan aan de eisen en principes uit de AVG rond een zorgvuldige verwerking van persoonsgegevens. Denk bijvoorbeeld aan het rechtmatig verwerken van persoonsgegevens, het vaststellen van doeleinden rond de verwerking, het nemen van passende technische en organisatorische beveiligingsmaatregelen rond de verwerking, het afsluiten van verwerkersovereenkomsten, het voldoen aan de documentatieplicht, zorgen voor dataminimalisatie en het kunnen voldoen aan verzoeken van betrokkenen die hun rechten uitoefenen. Deze vereisten en daaruit voortvloeiende maatregelen zijn op zichzelf geen maatregelen die voortvloeien uit een DPIA, omdat los van de risico's voor betrokkenen, hieraan altijd voldaan moet worden.

Het gaat bij een DPIA dus om maatregelen waardoor de verwerking wordt beperkt, anders wordt ingericht en/of om goede procedures op te stellen en het helpt tot nadenken over de gevolgen van een verwerking voor betrokkenen en hoe risico's zoveel mogelijk beperkt kunnen worden. Een DPIA kan zelfs leiden tot het stopzetten van een nieuw project. In die zin is de inzet van een PIA een krachtig instrument voor het vergroten van privacy-bewustzijn onder het personeel. Uit de nulmeting blijkt dat

de gemeente geen procedure heeft voor het inzetten, uitvoeren en afwikkelen van DPIA's inclusief een daarbij behorende standaardaanpak om de kwaliteit van een DPIA te waarborgen.

De DPIA wordt dus vanaf 25 mei a.s. verplicht voor elke nieuwe gegevensverwerking met een hoog risico voor de rechten en vrijheden van natuurlijke personen. Denk bijvoorbeeld aan de aanschaf van een nieuw informatiesysteem, een koppeling met een ander systeem, inrichting van een nieuw proces/dienst of het aangaan van een samenwerkingsverband.

Er zal in eerste instantie gefocust worden op het in beeld brengen van de bestaande situaties rond gegevensverwerkingen en het op basis van die inzichten in tweede instantie gaan uitvoeren van DPIA's voor zover dat noodzakelijk is. Deze aanpak is efficiënter en sluit beter aan op een gestructureerde aanpak die begint met voorbereiding en inventarisatie en daarna met een impactanalyse (DPIA).

3.8 Rechtmatige verwerking en procesplannen

3.8.1 Zorgvuldige verwerking van persoonsgegevens

De AVG stelt de nodige eisen en principes aan een zorgvuldige verwerking van persoonsgegevens:

- het rechtmatig verwerken van persoonsgegevens,
- het vaststellen van doeleinden van de verwerking,
- het nemen van passende technische en organisatorische beveiligingsmaatregelen rond de verwerking,
- het afsluiten van verwerkersovereenkomsten,
- het voldoen aan de documentatieplicht,
- het zorgen voor dataminimalisatie
- bewaartermijnen
- het kunnen voldoen aan verzoeken van betrokkenen die hun rechten uitoefenen.

Zo stelt de AVG dus in artikel 24 dat voor elke verwerking passende technische en organisatorische maatregelen zijn getroffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Het gaat dan onder meer om aan te tonen dat voor elke verwerking de rechtmatigheid, proportionaliteit, juistheid en de wijze waarop de veiligheid is geborgd moet worden gedocumenteerd. Daarvoor hanteren wij procesplannen.

3.8.2 Procesplan

Een procesplan bevat in eerste instantie een systematische beschrijving van het werkproces inclusief ketenpartners en bijbehorende verwerkingen.

Daarnaast geeft het procesplan inzicht in:

- de van toepassing zijnde wet- en regelgeving,
- de mate waarin voldaan wordt aan de privacy-principes zoals doelbinding, rechtmatige grondslag, bewaartermijnen, enz. en
- de passende organisatorische en technische beveiligingsmaatregelen.

Op basis van deze inventarisatie kan een DPIA worden uitgevoerd indien sprake is van een waarschijnlijk hoog risico voor de rechten en vrijheden van natuurlijke personen (zie $3.7). Ook uitgevoerde DPIA's zijn onderdeel van het procesplan. Het opstellen van een procesplan geschiedt in deze opzet fasegewijs door eerst te inventariseren en daarna waar nodig DPIA's uit te voeren.

Het mag duidelijk zijn dat het opstellen van een procesplan een forse opgave is en het niet in de verwachting ligt dat alle noodzakelijke procesplannen vóór 25 mei 2018 gereed zijn. Van belang is inzicht te krijgen in het aantal op te stellen procesplannen en benodigde capaciteit.

Voor het beheer, opstellen en onderhouden van procesplannen is een procedure en een standaardaanpak nodig om ervoor te zorgen dat de daaruit voortvloeiende activiteiten beheerst worden. Het niet zorgvuldig en deugdelijk documenteren houdt immers een compliance-risico in. In $3.8.3 zoomen we hierop nader in.

Overigens kunnen procesplannen zoals bedoeld vanuit de privacywetgeving ook ingezet worden om verantwoording te kunnen afleggen in het kader van de rechtmatigheid. Er is namelijk wetgeving in de maak met de bedoeling dat het college van B&W verantwoording gaat afleggen over de rechtmatige uitvoering van de begroting met als streefjaar 2020. Een privacybestendig werkproces WMO of Jeugdzorg komt in de regel tegemoet aan de eisen van rechtmatigheid en op deze wijze ondersteunt een procesplan meerdere doelen.

3.8.3 Procedure en standaardaanpak

Voor het vastleggen van een zorgvuldige verwerking in lijn met de AVG is een procedure nodig die ingaat op de verantwoordelijkheden, taken en bevoegdheden en de onderlinge afspraken ter zake. Zo is de proceseigenaar verantwoordelijk voor zijn eigen werkprocessen en dus voor het opstellen van procesplannen maar heeft hierbij ondersteuning nodig vanuit een kernteam met kennis van zaken rond het opstellen van procesplannen.

Elk afgewikkeld procesplan bevat een 'memorandum van de proceseigenaar' waarin de belangrijkste bevindingen zijn samengevat met als doel de directie formeel te informeren over de mate waarin de privacy-bestendigheid is geregeld en over de (eventuele) verbeteringen die nodig zijn. Voorts bevat dit document een bijlage ten behoeve van het verwerkingsregister en een auditplan. Periodieke terugkoppeling via de P&C-cyclus over voortgang en bereikte resultaten wordt ook op enig moment meegenomen in de procedure. Indien DPIA's van toepassing zijn, dan zijn deze standaard opgenomen in het betreffende procesplan.

Daarnaast is een standaardaanpak nodig die de inhoudelijke kant van het onderzoek waarborgt. De bedoeling is dat elke proceseigenaar werkt volgens eenzelfde aanpak die voorziet in de nodige vragenlijsten, formulieren en sjablonen om elk onderzoek zo effectief en efficiënt mogelijk te kunnen uitvoeren en afwikkelen. De proceseigenaar gaat zelf aan de slag met het verzamelen van de benodigde documentatie ten behoeve van het procesplan, uiteraard met ondersteuning van een kernteam.

3.8.4 Opstellen procesplannen

Dit onderdeel heeft betrekking op de implementatie specifiek (zie hiervoor aanpak in $2.1).

Alvorens een procedure en een standaardaanpak voor het plannen, voorbereiden, uitvoeren, afwikkelen en monitoren van procesplannen vast te stellen, is het wenselijk deze werkmethode te testen. Daarmee doen we ervaring op en kunnen we de opgestelde procedure en aanpak evalueren en eventueel aanpassen en daarna breed uitrollen. Afgesproken is te starten met pilots in het sociaal domein en bij Veiligheid alvorens breed uit te rollen.

De proceseigenaar is verantwoordelijk en stelt medewerkers met materiekennis beschikbaar voor het onderzoek. Ondersteuning vindt plaats door een kernteam en dan kan gedacht worden aan juristen, ICT-deskundigen, de Privacy Officer, de CISO, de FG en wellicht inzet van externe deskundigen en van ondersteuning bij het vergaren van informatie voor het vullen van formats e.d.

3.9 Meldplicht datalekken

Er is een meldplicht datalekken met als belangrijkste elementen:

- een datalek is ieder beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of waarbij onrechtmatige verwerking van die gegevens niet uitgesloten kan worden. Het omvat lekken door een menselijke fout, door ontoereikende beveiliging, door fraude en/of een bewuste criminele aanval van buitenaf, dus een hack, verlies van een laptop of usb-stick, een email naar de verkeerde persoon, etc.
- een datalek moet binnen 72 uur gemeld worden aan de toezichthouder, de AP, op straffe van forse geldboetes.
- als het datalek nadelige gevolgen kan hebben voor persoonsgegevens van burgers, moeten ook zij geïnformeerd worden;

Ten behoeve van de implementatie van deze meldplicht is een procedure opgesteld waarmee snel en adequaat opgetreden kan worden indien en zodra zich een beveiligingsincident voordoet. De procedure heeft betrekking op het proces dat begint met de interne melding van een incident, de analyse, het dichten van het evt. datalek en het melden daarvan bij de AP.
Indien het noodzakelijk is om de betrokkenen te informeren, is dat een verantwoordelijkheid van de betreffende procesverantwoordelijke van de betreffende verwerking.
Een datalek wordt ook gemeld aan de gemeentesecretaris en aan de portefeuillehouder. Indien sprake is van een incident dat de continuïteit van de dienstverlening raakt, schaalt de gemeentesecretaris, in afstemming met de portefeuillehouder, verder op naar ook andere portefeuillehouder(s) c.q. naar het hele college.

Er is ook een zgn. Computer Security Incident Response Team ingesteld om bij datalekken en andere beveiligingsincidenten snel en adequaat op te kunnen treden en maatregelen te kunnen nemen.

4 Tot slot

De gemeente moet zich voorbereiden op de naleving van de privacywetgeving en daarvoor is een forse investering nodig in kwaliteit en kwantiteit. Het gaat dan niet alleen om het inzetten van een Privacy Officer en FG, maar ook om extra capaciteit voor proceseigenaren en capaciteit voor het toetsen op de naleving van de privacywetgeving dat overigens in een latere fase aan de orde komt. Dit laatste is namelijk geen rol van de FG als toezichthouder, maar een rol voor de eigen organisatie die meegenomen zal worden in het onderzoeks- en auditprogramma 2019 van het team Finance & Control.

Aandacht voor privacy en gegevensbescherming is een blijvertje en behoort een structurele plek in de organisatie te krijgen waaraan iedereen vanuit zijn eigen verantwoordelijkheid een bijdrage levert. Dat is een groeiproces van jaren, immers er is tijd nodig voor gewenning aan de privacy-eisen en daarmee vertrouwd te raken én het heeft impact op de bestaande bedrijfscultuur. De organisatie heeft aldus tijd en ruimte nodig om privacybescherming in haar DNA te absorberen. Dit implementatieplan is de kiem voor een routemap voor de komende jaren en wordt jaarlijks aangepast op basis van de laatste stand van zaken.

5 Actiepunten

Nr	Actiepunt	Verwijzingen[3]	Datum gereed[4]	Actiehouder
1.	Borg een structurele en toereikende inzet van een Privacy Officer als ankerpunt voor de implementatie van privacy en de ondersteuning en advisering van de organisatie op het gebied van AVG en privacy.	§3.2.1: vragen 2.1.4; 2.2.3	Q2 2018	DIR
2.	Benoem en positioneer een Functionaris gegevensbescherming (FG) voor 25 mei 2018 zo onafhankelijk mogelijk in de organisatie zoals bedoeld volgens de AVG en bepaal de benodigde inzet in fte.	§3.2.1: vragen 2.1.5	Q2 2018	College
3.	Stel een procedure op voor de organisatie van de privacy waarbij het onderlinge samenspel tussen key-spelers is beschreven.	§3.2.2: vragen 2.2.1; 2.2.2; 2.2.4; 2.2.8; 2.2.9	Q2 2018	PIT / DIR
4.	Zorg voor een privacy informatiebeveiligings-team (PIT) dat als permanent adviesorgaan voor de directie opereert op het gebied van operationele en tactische vraagstukken rond privacy en informatieveiligheid.	§3.2.2: vragen 2.2.1	Q3 2018	DIR
5.	Voer onderzoek uit naar de structurele middelen die jaarlijks nodig zijn om privacy blijvend te borgen in de organisatie en neem dit mee in de behandeling van de Voorjaarsnota 2018.	§3.2.4: vragen 2.4.1 t/m 2.4.7	Q2 2018	PIT / DIR
6.	Bevorder de bewustwording en kennis op het gebied van privacy onder de medewerkers.	§3.3: vragen 3.1;	Q4 2018	PIT / DIR
7.	Stel een privacy-protocol op voor de medewerkers (intern en extern) waarin gedragsregels staan voor het omgaan met privacygevoelige informatie.	§3.3: vragen 3.3; 3.4	Q3 2018	PIT / HRM
8.	Stel een privacy-statement op waarin de visie en handelwijze over de bescherming van persoonsgegevens bekend wordt gemaakt aan alle betrokkenen (op website)	§3.4; vragen 4.1.2 t/m 4.2.5	Q3 2018	DIR/ College
9.	Stel een kader en een procedure op over het contracteren van verwerkers zodat de verantwoordelijkheid voor een zorgvuldige omgang met persoonsgegevens conform de AVG geborgd is.	§3.5; vragen 5.1	Q3 2018	DIR
10.	Stel een procedure op voor het beheer en gebruik van het verwerkingsregister.	§3.6: vragen 6.2; 6.3; 6.4	Q3 2018	PIT / DIR
11.	Richt een verwerkingsregister in conform artikel 30 AVG	§3.6: vragen 6.1; 6.3; 6.4	Q1 2018	PO
12.	Stel een artikel 30-formulier op waarin verzoek tot wijzigingen in het verwerkingsregister opgenomen kunnen worden.	§3.6: vragen 6.5	Q4 2018	PIT / DIR

[3] Verwijst naar de paragraaf in het implementatieplan en naar de nulmeting (vragen).
[4] De vermelde datum gereed is in deze tabel indicatief.

Nr	Actiepunt	Verwijzingen[3]	Datum gereed[4]	Actiehouder
13.	Inventariseer zoveel mogelijk alle structurele verwerkingen van persoonsgegevens en leg dit vast in het verwerkingsregister gebruikmakend van het artikel 30-formulier.	$3.6: vragen 6.4; 6.7	Q2-Q4 2018	Proceseigenaren
14.	Stel een procedure op voor het uitvoeren en beheren van DPIA's.	$3.7: vragen 2.3.4; 7.1.1; 7.1.3; 7.1.4	Q3 2018	PIT/ DIR
15.	Stel een standaardaanpak op om de kwaliteit van elke DPIA te waarborgen.	$3.7: vragen 2.3.4; 7.1.2	Q4 2018	PIT / DIR
16.	Stel procesplannen op voor de werkprocessen met een hoog privacy-risico in het sociaal domein en bij veiligheid om de procedure en aanpak te testen.	$3.8.3: vragen 8.2.1; 8.3.2; 8.3.3; 8.3.4	Q2-Q3 2018	PIT / proceseigenaar
17.	Stel een procedure op om het proces rond het opstellen en onderhouden van procesplannen (compliance) te waarborgen.	$3.8.2: vragen 8.1.1; 8.1.2; 8.1.3; 8.1.4	Q3 2018	PIT / DIR
18.	Stel een standaardaanpak op om de kwaliteit van procesplannen te waarborgen voorzien van de nodige formulieren en sjablonen.	$3.8.2: vragen 8.1.5; 8.1.6; 8.1.7	Q3 2018	PIT / DIR
19.	Richt een evaluatieproces op basis van de PDCA-cyclus in dat directie en B&W via rapportages voorziet van tijdige stuur- en verantwoordingsinformatie om de privacybescherming te kunnen beheersen.	$3.1, 3.2.3, 4; vragen 1.4; 1.5; 2.2.5; 2.2.6; 2.2.8	Q4 2018	DIR / College

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