Positie en taken Functionaris gegevensbescherming (FG)

Inhoudsopgave

Inleiding

Sinds 25 mei 2018 moet voldaan worden aan de bepalingen in de Algemene verordening gegevensbescherming (AVG). In de AVG is bepaald dat als de verwerkingsverantwoordelijke een overheidsinstantie/overheidsorgaan is, de verwerkingsverantwoordelijken vanaf 25 mei 2018 een Functionaris voor Gegevensbescherming (FG) aan moeten wijzen. Binnen de gemeentelijke organisatie zijn de bestuursorganen verwerkingsverantwoordelijken. Voor de meeste verwerkingen is het college de verwerkingsverantwoordelijke. In dit document wordt voor de leesbaarheid het college als verwerkingsverantwoordelijke beschouwd. Waar het college vermeldt staat, kunnen ook de andere bestuursorganen gelezen worden.

De FG ziet toe op de bescherming van persoonsgegevens en controleert de organisatie op de naleving van de privacywetgeving en het (eigen) privacybeleid, het Privacyreglement gemeente Heerenveen. De FG wordt voor de drie gemeentelijke bestuursorganen aangewezen.

Op basis van handreikingen van de VNG en de Autoriteit persoonsgegevens worden in dit document de wettelijke taken van de FG genoemd en wordt een verband gelegd met de werkzaamheden van de aanwezige Chief Information Security Officer (CISO) en Privacy Officer (PO). De werkzaamheden van de FG, CISO en PO vullen elkaar aan. Ook wordt de positie van de FG in de gemeentelijke organisatie beschreven.

1. Taken Functionaris gegevensbescherming

Het college is verantwoordelijk voor ‘alles’ wat te maken heeft met de bescherming van persoonsgegevens. De FG ziet hier op toe en adviseert. De FG heeft geen formele bevoegdheid om een bindend advies te geven, maar zijn oordeel is wel ‘zwaarwegend’. Het college neemt dit advies mee in zijn afwegingen en kan gemotiveerd afwijken van het advies van de FG.

De FG informeert en adviseert bijvoorbeeld over de verplichtingen die de gemeente op grond van de 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, ziet toe op juiste toewijzing van verantwoordelijkheden aan medewerkers binnen de gemeente en draagt zorg voor het opleiden en trainen van medewerkers die te maken hebben met gegevensverwerking. Daarnaast is de FG de contactpersoon voor de Autoriteit persoonsgegevens.

Het college dient ervoor te zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Daarnaast is in de AVG de verplichting opgenomen dat het college de FG de benodigde middelen ter beschikking stelt voor het vervullen van zijn of haar taken en het in stand houden van zijn of haar deskundigheid.

1.1 Specifieke taken

Artikel 39 AVG geeft aan welke taken de FG (minimaal) heeft:

- Het informeren en adviseren van de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen uit hoofde van de AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van de AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van het gemeentelijke beleid;
- Het toezien op de naleving van de afspraken door de verwerkers omtrent 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 gegevensbeschermingseffect-beoordeling (DPIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- Het samenwerken met de AP;
- Het optreden als contactpunt voor de AP.

De FG wordt ook aangewezen als contactpersoon voor betrokkenen.

1.2 Overige wettelijke taken

Andere verplichtingen uit de AVG zijn bijvoorbeeld:

- in samenspraak met de CISO adviseren over digitale oplossingen en de informatiebeveiliging van gegevensverwerking;
- toezien op het verwerkingsregister;
- controleren van verwerkersovereenkomsten;
- bij inbreuk persoonsgegevens (meldplicht datalekken) adviseren over de ernst en omvang ervan;
- adviseren zodat privacy klachten tot een goed einde gebracht worden;
- adviseren over de afhandeling van verzoeken van betrokkenen met betrekking tot de verwerking van hun gegevens en het uitoefenen van hun rechten (zoals o.a. recht op inzage).

2 Bevoegdheden FG

De gemeente is wettelijk verplicht om de FG controlebevoegdheden te geven, zodat hij of zij kan toezien op de naleving van de AVG. Deze controlebevoegdheden dienen overeen te komen met:

- de taakomschrijvingen van de FG in de AVG;
- de bevoegdheden die gelden voor het toezicht binnen de overheid.

Bovenstaande betekent dat:

- de FG de mogelijkheid dient te krijgen om ongevraagd alle ruimten (dus ook een serverruimte) te betreden als dit noodzakelijk is voor de uitoefening van zijn of haar taak.
- de FG de bevoegdheid dient te hebben om de benodigde inlichtingen te verkrijgen, bijvoorbeeld inlichtingen over de toegang tot systemen. Medewerking hieraan kan alleen worden geweigerd als er een geheimhoudingsplicht bestaat.
- de FG inzage kan vragen in zakelijke gegevens en documenten en hier, als hij of zij wenst, kopieën van mag maken. Dit hoeven niet persé fotokopieën te zijn, maar dat mogen ook kopieën zijn van geautomatiseerde gegevensbestanden. Hiervoor kan het nodig zijn dat de FG de beschikking krijgt over relevante inloggegevens.

Het college is verplicht aan bovenstaande zijn medewerking te verlenen aan de FG.

3 Expertise en vaardigheden FG

In de AVG staan een aantal algemene eisen waar de FG aan moet voldoen. De vereiste expertise en vaardigheden omvatten in ieder geval:

- kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming;
- begrip van de gegevensverwerkingen die de organisatie uitvoert;
- begrip van IT en informatiebeveiliging;
- kennis van de organisatie en de sector waarin die actief is;
- kennis van de administratieve regels en procedures van de organisatie;
- vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.
- integriteit;
- en een hoge mate van professionele ethiek.

4 Positie

Uitgangspunt van de FG is dat het iemand is die adviseert over de AVG. Vooral bij projecten, samenwerkingen en nieuwe ontwikkelingen. De FG kijkt of de risico's voldoende in kaart zijn gebracht en of de maatregelen die getroffen worden voldoende zijn. De FG is ook de persoon waar inwoners terecht kunnen als er een gevoel ontstaat dat er niet goed met privacy gevoelige informatie om wordt gegaan. Ook heeft de FG een controlerende taak, waarbij gelet wordt of er binnen de organisatie voldaan wordt aan de eisen die gesteld worden vanuit de AVG.

De positionering van de FG binnen de organisatie is belangrijk, want deze is bepalend voor de slagkracht van de FG. De FG wordt aangesteld als intern toezichthouder. Eén van de belangrijkste criteria is dat een FG onafhankelijk is: de FG mag geen instructies ontvangen met betrekking tot de uitvoering van zijn taken.

De FG rapporteert zo nodig rechtstreeks aan het college over de bevindingen. De FG geniet een wettelijke ontslagbescherming, zodat hij of zij niet ontslagen kan worden als gevolg van zijn of haar wettelijke rol als interne onafhankelijk toezichthouder. De FG kan een ambtenaar zijn of op grond van een dienstverleningsovereenkomst werkzaam zijn. Er dient voorkomen te worden dat de FG zich (te veel) met uitvoerende taken bezighoudt, omdat hij dan in feite ook zijn eigen uitvoerende werkzaamheden gaat adviseren of controleren. De FG kan ook andere taken en plichten vervullen. Het college zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden. Het is belangrijk dat er voldoende functiescheiding wordt aangebracht.

In Heerenveen is er voor gekozen om de FG-taken binnen het team JzenI te beleggen. Binnen het team JzenI kan er optimaal gewerkt worden doordat er korte lijnen zijn tussen de FG en de privacy officers. De privacy officers zijn juridisch adviseurs binnen het team, die samen met de FG de AVG-taken uitvoeren. Om de aanvullende taken vanuit de AVG – waaronder de FG-taken – uit te kunnen voeren, heeft in het team een uitbreiding van de formatie plaatsgevonden voor juridisch adviseurs van 0,4 fte tijdelijk in 2018 en 0,5 fte structureel in 2020. De FG-taken, dus niet de rol, worden dus uitgevoerd door en verdeeld onder de FG en de juridisch adviseurs/privacy officers samen. Daarbij geldt wel te allen tijde dat bij de FG primair het toezicht en de controle op de naleving van de AVG uitvoert. Voor de uitvoerende taken van de privacy officers, wordt verwezen naar punt 5.2.
Daarnaast is van belang dat er veel kennis van wet- en regelgeving van zowel de AVG als overige voor de organisatie relevante wet- en regelgeving aanwezig is binnen het team. Het team heeft weinig tot geen uitvoerende taken, maar houdt zich vooral bezig met het gevraagd en ongevraagd geven van onafhankelijk advies.

5 Samenwerking FG, CISO, PO en archivaris

In Heerenveen zijn zowel de functie van FG, CISO en PO onderscheiden. In de uitvoering van de functie van vooral de FG en PO bestaat een overlap, door de wijze van inrichting van de taken van de FG. Daarbij geldt echter wel dat elk van hen een eigen taak heeft, die zich onderscheidt van de andere twee. Hiermee wordt voorkomen dat er sprake zou kunnen zijn van 'de slager die zijn eigen vlees keurt' en waarborgt de geloofwaardigheid, betrouwbaarheid en komt de kwaliteit ten goede.

Voor de toepassing en naleving van de AVG is het van groot belang dat de FG nauw samen werkt met de CISO, PO en de archivaris. Dit omdat de PO de taak heeft de eigenaar te ondersteunen en te adviseren, de CISO als taak de informatieveiligheid heeft en de archivaris van groot belang is voor de naleving van de

bewaartermijnen en dataminimalisatie. De FG houdt toezicht op het geheel en de organisatie als geheel en kan daarbij steunen op de expertise van de anderen.

5.1 Chief Information Security Officer (CISO)

Persoonsgegevens maken onderdeel uit van de gegevens waarvoor een gemeente informatiebeveiligingsmaatregelen dient te treffen. Er is een duidelijke overlap in taakvelden met die van een FG te constateren. Het aspect 'vertrouwelijkheid van informatie' behoort immers ook tot het taakgebied van de CISO.

5.2 Privacy Officer PO

De PO functioneert deels op gelijke wijze als een FG. In Heerenveen hebben een aantal juridisch adviseurs tevens de rol van PO. Zoals hiervoor opgenomen onder punt 4 is in de afgelopen twee jaar hiervoor formatieruimte verkregen, zodat de PO's de FG kunnen ondersteunen in de FG-taken.

Verschillen PO en FG

Er zijn op grond van de AVG een aantal verschillen te benoemen tussen een FG en een PO, zoals:

- De FG staat vermeld in het openbaar register van de AP.
- De FG geniet wettelijke ontslagbescherming.
- De FG heeft een wettelijke geheimhoudingsplicht ten aanzien van een klacht of verzoek van een betrokkene.
- De FG neemt een melding in ontvangst van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens.
- De FG beschikt over toezichthoudende controlebevoegdheden.

Overeenkomsten PO en FG

De FG en de PO zien intern toe op de toepassing en naleving van de AVG. In Heerenveen functioneert de PO dicht op de afdelingen, praktisch adviserend en privacyvraagstukken (op casusniveau) zo nodig uitwerkend. Het formuleren van beleid is één van de taken van de PO. Deze taak kan niet bij de FG worden ondergebracht, omdat deze toeziet op het beleid.

In Heerenveen worden de volgende taken, voor zo ver deze het verwerken van persoonsgegevens raakt, ondergebracht bij de PO:

- Bevordert en adviseert de organisatie over de bescherming van persoonsgegevens (inclusief scholing);
- Stelt algemeen privacybeleid (inclusief procedures) op;
- Ondersteunt de afdeling bij het opstellen van afdelingsspecifiek privacybeleid;
- Adviseert over de juridische aspecten in de verwerkersovereenkomsten;
- Heeft een coördinerende en adviserende rol bij het verwerkingsregister;
- Adviseert bij klachtprocedures;
- Heeft een ondersteunende adviserende rol bij veiligheidsincidenten en datalekken;

- Heeft een ondersteunende en adviserende rol bij verzoeken van betrokkenen die gebruik maken van hun rechten;
- Ondersteunt en adviseert de afdelingen bij het uitvoeren van DPIA's;
- Ondersteunt en adviseert de privacy adviseurs op de afdelingen bij privacyvraagstukken.

5.3 Privacy Adviseurs

Naast de FG en de PO's zijn er privacy adviseurs op de afdelingen aangewezen. Zij hebben de rol als eerste aanspreekpunt voor de collega's op de afdelingen. Zij kunnen vragen beantwoorden die op hun afdeling leven en waar nodig/gewenst doorsturen naar de PO's. Zo wordt er doorlopend op de afdeling aandacht besteed aan wat gegevensbescherming en de privacywetgeving concreet betekenen voor de betreffende afdeling en hoe medewerkers om dienen te gaan met persoonsgegevens binnen hun taken en werkzaamheden. Ook zijn de privacy adviseurs ondersteunend aan hun afdelingshoofd om de verantwoordelijkheid voor privacy binnen de afdeling te nemen.

De privacy adviseurs worden ondersteund en geadviseerd door de PO's. De PO's voeren doorlopend gesprekken met de privacy adviseurs, om hen in staat te stellen hun rol op hun eigen afdeling te nemen. Omgekeerd ondersteunen de privacy adviseurs de PO's, onder meer bij het bijhouden en actualiseren van het verwerkingsregister. Tevens zouden de privacy adviseurs een rol kunnen krijgen in onder meer het proces van uitvoering van DPIA's en risico-inventarisatie. De uitbreiding van hun rol zal in samenspraak met de privacy adviseurs plaatsvinden.

5.4 Werkprocessen en verantwoordelijkheden

1	*Beheer van het verwerkingsregister* • De eigenaar van de betreffende persoonsgegevens binnen de organisatie is verantwoordelijk de actualiteit van de verwerkingen van zijn organisatieonderdeel in het register. • De PO is verantwoordelijk voor de coördinatie van de actualisatie van het overzicht van persoonsverwerkingen. • De PO is samen met het team Informatiemanagement verantwoordelijk voor het beheer van het organisatiebrede overzicht van alle persoonsverwerkingen. • De FG ziet toe op het invullen van de verantwoordelijkheden van de eigenaar en van de PO en ziet toe op de integriteit, vertrouwelijkheid en beschikbaarheid van het register en de (eventuele) melding van de verwerking bij de PO.				
		PO	**Eigenaar**	**CISO**	**FG**
	Actieve aanlevering van nieuwe verwerkingen bij de PO en de FG		X		
	Zorgdragen voor actualiteit van verwerkingsregister		X		
	Coördinatie van de actualisatie van register van verwerkingen	X			
	Beheer van het verwerkingsregister	X			
	Toetsing op kwaliteit, actualiteit, juistheid en volledigheid van het verwerkingsregister				X

2	*Registratie, beheer en actualisatie van verwerkersovereenkomsten* • De eigenaar van de betreffende persoonsgegevens binnen de organisatie is verantwoordelijk voor het afsluiten, beheren en actualiseren van een verwerkersovereenkomst. • De PO is verantwoordelijk voor de beschikbaarheid van een actuele model verwerkersovereenkomst die de algemene wet- en regelgeving dekt. Hij geeft daarnaast advies aan de eigenaar over het afsluiten van de verwerkersovereenkomst, over specifieke voorwaarden en onderdelen in de verwerkersovereenkomst en ondersteunt bij vraagstukken die spelen bij onderhandeling met de derde partij. • De CISO geeft advies aan de eigenaar over het afsluiten van de verwerkersovereenkomst, over specifieke voorwaarden en onderdelen in de verwerkersovereenkomst rondom informatieveiligheid en ondersteunt bij vraagstukken die spelen bij onderhandeling met de derde partij (de verwerker) specifieke beveiligingsmaatregelen. • De FG ziet toe op het invullen van de verantwoordelijkheden van de eigenaar en de PO. De FG ziet er op toe dat volgens de (Europese) privacywetgeving wordt gehandeld en ziet tevens toe op de integriteit, vertrouwelijkheid en beschikbaarheid van de centrale registratie.				
		PO	**Eigenaar**	**CISO**	**FG**
	Afsluiten van verwerkersovereenkomsten		X		

	Actualiseren en beheren van de model verwerkersovereenkomst	X		X	
	Advies aan de organisatie ten aanzien van werken met verwerkers en verwerkersovereenkomsten	X		X	X
	Archivering van verwerkersovereenkomsten		X		
	Naleving van de afspraken in de verwerkersovereenkomsten		X		
	Toezicht op registratie verwerkers en verwerkersovereenkomsten				X

---

3 *Afhandeling veiligheidsincidenten en datalekken*

- De eigenaar van de betreffende persoonsgegevens binnen de organisatie is verantwoordelijk voor de interne melding, de informatievoorziening, eventuele externe melding en de interne en eventueel externe communicatie rond het incident.
- De eigenaar is tevens verantwoordelijk voor de evaluatie van het datalek en het treffen van maatregelen om incidenten te voorkomen.
- De CISO en de PO zijn verantwoordelijk voor inhoudelijke ondersteuning van de eigenaar bij het doorlopen van de procedure die in werking treedt bij een veiligheidsincident, het registeren van het datalek en het invullen van het datalekkenregister gedurende het proces van het incident. Zij geven daarnaast advies aan de eigenaar gedurende het doorlopen van de procedure.
- De FG staat zowel de eigenaar als de CISO en de PO bij in raad en daad bij doorlopen van de incidentenprocedure, geven van inhoudelijke advies, het uitvoeren van de analyse en doen van een melding bij de AP.
- De FG is tevens verantwoordelijk voor de toetsing op implementatie van de adviezen.
- De PO en de CISO doen de externe melding onder verantwoordelijkheid van de eigenaar.

		PO	**Eigenaar**	**CISO**	**FG**
	Inventariseren van feiten en omstandigheden	X	X	X	
	Invullen datalekkenregister	X		X	
	Verstrekken advies	X		X	X
	In geval van dilemma's in analyse en / of advies afstemming verzorgen met respectievelijk PO, eigenaar, gemeentesecretaris en/of bestuurder		X	X	X
	Het doen van een externe melding	X	X	X	
	Het treffen van maatregelen om		X		

	incidenten te voorkomen				

4	*Advies en voorlichting aan organisatie* • De PO, FG en CISO geven gevraagd en ongevraagd advies aan de organisatie (medewerkers en management) en bestuur met betrekking tot informatieveiligheid en privacyvraagstukken. • De eigenaar is verantwoordelijk voor aandacht voor informatieveiligheid en privacy op de afdeling.				
		PO	**Eigenaar**	**CISO**	**FG**
	Gevraagd en ongevraagd advies verlenen aan bestuur, management en medewerkers	X		X	X
	Voorlichting en communicatie	X		X	X
	Continue aandacht voor informatieveiligheid en privacy op de afdeling		X		

5	*Uitvoeren Data Protection Impact Assessment (DPIA)* • De eigenaar is verantwoordelijk voor het initiëren van de DPIA, inbreng van inhoudelijke, functionele kennis, en uitvoer en effectueren van de resultaten van de DPIA. • De PO kan op verzoek van de eigenaar zorgen voor inhoudelijke en procedurele ondersteuning en/of juridische toetsing bij het uitvoeren van een DPIA. De PO geeft daarnaast, samen met de CISO, advies aan de eigenaar gedurende het doorlopen van de procedure. • De FG staat zowel de eigenaar als de PO bij in raad en daad bij het doorlopen van de DPIA procedure en het geven van inhoudelijk advies.				
		PO	**Eigenaar**	**CISO**	**FG**
	Initiëren DPIA		X		
	Uitvoeren DPIA		X		
	Inhoudelijke en procedurele ondersteuning en/of juridische toetsing van de eigenaar bij doorlopen van de DPIA procedure	X			
	Het adviseren van de eigenaar bij het doorlopen van de DPIA procedure	X		X	
	Opstellen DPIA inclusief aanbevelingen, verwerken en archiveren van de resultaten van de DPIA	X	X		

	Uitvoeren acties/implementeren maatregelen voortkomend uit PIA		X		
	Toetsen uitgevoerde acties / geïmplementeerde maatregelen				X
	Toetsen op de procedure, de resultaten, de effectuering en de naleving van de resultaten uit de PIA				X

6	*Klachtafhandeling* • De eigenaar is verantwoordelijk voor het initiëren, het doorlopen, het verzorgen van interne en externe communicatie en afsluiten van de klachtafhandelingsprocedure. Dit in samenwerking met de gemeentelijke klachtenfunctionaris. • De PO en de CISO zorgen op verzoek van de eigenaar voor de inbreng van kennis over privacy en informatiebeveiliging die nodig is voor het doorlopen van de klachtafhandelingsprocedure. • De FG ziet toe op de kwaliteit en de correcte afhandeling van de klacht. • In voorkomende gevallen treedt de FG op als bemiddelaar tussen de burger en de organisatie.				
		PO	**Eigenaar**	**CISO**	**FG**
	Het Initiëren, doorlopen, verzorgen van interne en externe communicatie en afsluiten van de klachtafhandelings-procedure		X		
	Inbreng van inhoudelijke kennis	X		X	
	Toetsen op kwaliteit en correcte afhandeling van klacht				X

7	*Afhandeling verzoek rechten van betrokkenen m.b.t persoonsgegevens* • De eigenaar is verantwoordelijk voor de afhandeling van verzoeken van de rechten van betrokkenen met betrekking tot de persoonsgegevens die onder zijn verantwoordelijkheid vallen. • De eigenaar wordt ondersteund door de afdeling I&I bij het inventariseren van de verwerkte persoonsgegevens en het verwerken van de uitkomsten van de verzoeken. • De PO kan de eigenaar adviseren over en ondersteunen bij de afhandeling van de verzoeken van de rechten van de betrokkenen. • De PO coördineert de afdelingsoverstijgende verzoeken van betrokkenen. • De FG ziet toe op de afhandeling van de verzoeken van betrokkenen.				
		PO	**Eigenaar**	**CISO**	**FG**
	Verantwoordelijk voor het opstellen van	X			

	procedure voor afhandeling verzoek				
	Ontvangen, uitzetten vraag binnen de organisatie, verzamelen informatie en terugkoppeling naar aanvrager bij afdelingsoverstijgend verzoek	X			
	Verzoek uitvoeren		X		
	Procedureel en inhoudelijk ondersteunen bij de procedure verzoek rechten van betrokkenen persoonsgegevens	X			
	Toezicht op doorlopen procedure verzoek rechten van betrokkenen.				X

8	*Ontwikkelen en beheer van procedures, formats en beleid* • De eigenaar is verantwoordelijk voor de uitvoering van het beleid ten aanzien van de betreffende persoonsgegevens die onder zijn verantwoordelijkheid vallen. • De PO en CISO zorgen voor de ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond procedures, formats en beleid met betrekking tot informatieveiligheid en privacy. • De FG adviseert over de ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond procedures, formats en beleid met betrekking tot privacy. • De FG is verantwoordelijk voor de toetsing op de uitvoer van het beleid.				
		PO	**Eigenaar**	**CISO**	**FG**
	De ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond procedures, formats en beleid met betrekking tot privacy	X		X	
	Advies over de ontwikkeling, het beheer, de optimalisatie en de interne en externe communicatie rond procedures, formats en beleid met betrekking tot privacy				X

	Ten uitvoer brengen van het beleid		X		
	Het beheer en de archivering van procedures, formats en beleid met betrekking tot informatiebeveiliging en privacy	X		X	
	Toezicht op de kwaliteit, archivering, communicatie en toepassing van procedures, formats en beleid				X