Nieuw aan te wijzen: de Functionaris voor de gegevensbescherming

Een nieuwe privacywet

Op het gebied van privacy staat er veel te veranderen per 25 mei van dit jaar. Op dat moment wordt de Algemene Verordening Gegevensbescherming (AVG) van kracht, die de huidige Wet bescherming persoonsgegevens vervangt. Inhoudelijk verandert er niet enorm veel aan het beschermingsregime maar wel zijn er nieuwe regels over de manier waarop organisaties zich moeten verantwoorden dat en hoe zij zich aan de regels houden. Die verantwoording vraagt nogal wat.
Gemeenten hebben heel veel data over hun burgers, voor de uitvoering van allerlei verschillende taken. Om een betrouwbare overheid te zijn, moet de gemeente zorgen en aantonen dat zij daar zorgvuldig en veilig mee omgaat. Burgers moeten daarop kunnen vertrouwen. Hetzelfde geldt overigens voor ambtenaren en bestuurders, ook van hen heeft de gemeente persoonsgegevens in huis.

Functionaris voor de gegevensbescherming

Een van de veranderingen die volgen uit de AVG is dat alle overheden (en andere organisaties die veel met persoonsgegevens werken) verplicht zijn een functionaris voor de gegevensbescherming aan te stellen. Deze FG heeft zowel een informerende en adviserende als een toezichthoudende taak en is de contactpersoon voor de Autoriteit Persoonsgegevens (de nationale toezichthouder) en voor burgers die hun privacyrechten willen uitoefenen.
Het gaat dan om toezicht op de naleving van de AVG. Allen overheden en andere grote organisaties die met persoonsgegevens werken zijn verplicht een FG aan te stellen. Het is in de gemeenten Haarlem en Zandvoort een nieuwe functie. De FG moet deze taken onafhankelijk kunnen uitvoeren. Deze notitie gaat in op de rol en taken van de FG en leidt tot het voorstel de huidige strategisch privacyadviseur als FG te benoemen. Er wordt een aparte, bredere notitie gemaakt over de algehele voorbereiding op de AVG.

Taken

Uit de AVG volgen de taken van de FG:

- *Informeren en adviseren* van de eigen organisatie over de wettelijke regels op het gebied van privacy, m.n. de AVG.
- *Toezien* op de naleving van die regels en het eigen privacybeleid
- Adviseren over en toezien op het doen van *DPIA's* (data protection impact assessment of gegevensbeschermingseffectbeoordeling)
- Optreden als *contactpersoon voor de nationale toezichthouder* (de Autoriteit Persoonsgegevens).
- Optreden als contactpersoon voor burgers die hun privacyrechten op basis van de AVG willen uitoefenen.

Governancestructuur

In feite is het vooral de taak van de FG te zorgen voor een goede governance op het gebied van privacy. Dat betekent met name versterken van de bewustwording en kennis in de organisatie, compliant worden en blijven op processen waarin persoonsgegevens worden verwerkt, , wat de risico's zijn voor de betrokkenen en hoe kan worden gewaarborgd. Het doel is de gemeente in de loop van de tijd te begeleiden naar een hoger niveau van volwassenheid op het gebied van privacy.

Toezicht houden
Tegelijk is er de toezichthoudende rol. Als er nieuwe werkprocessen of systemen worden ingericht waarin met persoonsgegevens wordt gewerkt, bestaande werkprocessen zullen worden beoordeeld zal de FG daarin betrokken worden. Via bijvoorbeeld risico-beoordeling, advisering en audits. Het eerste doel zal steeds zijn om de organisatie te helpen het werk zo te organiseren dat de privacy gewaarborgd is. Als het nodig is, zal de FG een duidelijk negatief advies geven. In het uiterste geval moet de FG ook op tijd en op het juiste niveau aan de bel trekken als het een keer echt niet goed dreigt te gaan. NB: de FG blijft wel uiteindelijk een adviseur. Directie en bestuur zijn degenen die beslissen en zijn eindverantwoordelijk.

Verantwoording afleggen
Om als organisatie aan alle verplichtingen te kunnen doen, verplicht de AVG onder andere tot het aanleggen van een 'register van verwerkingen' (een overzicht van alle processen waarin de gemeente persoonsgegevens verwerkt) en het doen van zogeheten DPIA's. In een DPIA wordt een proces doorgenomen om te bezien of dat privacyproof is. Beoordeeld wordt of en waar er risico's zijn voor de mensen om wier gegevens het gaat, hoe die zoveel mogelijk weg te nemen of terug te brengen tot een aanvaardbaar, proportioneel niveau. Als een risico niet kan worden weggenomen, zal moeten worden bekeken of de impact die het heeft op de privacy van de betrokkenen (degenen van wie er gegevens worden verwerkt) opweegt tegen het doel waarvoor de persoonsgegevens worden verwerkt. De gemeente heeft wel wat maar nog niet veel ervaring met het doen van DPIA's. Dit zal de komende periode veel meer en systematischer moeten gebeuren. De FG zal de DPIA's niet noodzakelijk allemaal zelf begeleiden, daar speelt in elk geval ook de privacyadviseur een rol in. De FG beoordeelt in elk geval wel de rapportages van de DPIA's. Het genoemde register wordt op dit moment gevuld. Dat vraagt een grote inspanning. Er wordt een aparte notitie gemaakt over hoe de organisatie voor te bereiden op de eisen die AVG stelt, waarin hierover meer wordt gezegd.

De slager die zijn eigen vlees keurt?
Dat de FG zowel moet adviseren als controleren levert een zekere spanning op. Dit is overigens geen onbekend verschijnsel in onze organisatie: ook controllers kennen die dubbele pet in hun rol. Voor de FG betekent dit dat de advisering zich meer zal richten op het overkoepelend, strategisch niveau en op de governance. De privacyadviseur adviseert meer op tactisch niveau en deels ook op operationeel niveau. Gezien de toename van eisen en risico's zijn waarschijnlijk meer privacyadviseurs nodig, dichter bij of in de vakafdelingen zelf.

Externe rol
De FG heeft ook een externe rol. Enerzijds richting de Autoriteit Persoonsgegevens, de nationale toezichthouder. De FG is de eerste contactpersoon voor de AP. Meldingen van eventuele datalekken worden gedaan bij de AP, onder verantwoordelijkheid van de FG. Als de AP aanleiding ziet vragen te stellen of een onderzoek in te stellen, zal zij contact opnemen met de FG. Een andere externe rol is die richting de burgers. Als burgers vragen hebben of een klacht, kunnen zij zich tot de FG richten.

Kennis en vaardigheden
Met alle taken die bij een FG zijn belegd, wordt eigenlijk een schaap met vijf poten gevraagd. De FG moet onder andere kennis hebben van de wet, van ethiek, techniek, beveiliging, het houden van audits en van de organisatie. Om bewustwording van de organisatie te versterken moet de FG ook presentaties of workshops kunnen verzorgen. De gevraagde kennis is zo breed dat het in de praktijk

niet te vinden is in één persoon. Dat betekent dat het nodig is goed samen te werken met de privacyadviseur, de strategisch adviseur informatiebeveiliging/CISO, de strategisch adviseur informatiebeheer/CDO en de IT-auditor en andere collega's met kennis van de verschillende vakgebieden. Op dit moment is er al veel samenwerking tussen collega's uit die vakgebieden, onder andere in een team Compliancy onder leiding van de CIO en een team Informatiesamenleving, dat zich meer richt op de strategische vraagstukken. Daarnaast wordt in de advisering rond bijvoorbeeld aanbestedingen samengewerkt. Op dit moment is in de eerste plaats iemand nodig die kennis heeft van de AVG, die daarbij versterking van de bewustwording van de organisatie verzorgt en die organiseert dat er een governancestructuur van de grond komt.

Om effectief te zijn is een starre juridische benadering niet wat nodig is. De eerste taak van de FG is om de organisatie te ondersteunen om compliant te zijn. Daarvoor is wel duidelijkheid nodig over wat wel en niet mag binnen de wet en om de risico's te benoemen. Vervolgens gaat het er echter om te ondersteunen om binnen de regels tot een aanpak of besluit te komen waarmee wel het beoogde doel wordt bereikt.

Communicatieve vaardigheden zijn dus vereist. Onder andere om zoals hiervoor gezegd op de juiste toon te kunnen adviseren en mensen te overtuigen. Een FG moet zowel streng kunnen zijn als diplomatiek optreden. Communicatieve vaardigheden zijn ook van belang omdat – zeker de eerste tijd - veel aandacht nodig is om de organisatie bewust te maken. Dat betekent onder andere presentaties houden en workshops geven, mensen laten zien wat het belang is van privacy en dat het ook hun werk raakt. Ook in het contact met burgers moet een FG de juiste toon treffen en in goed verstaanbare taal vragen kunnen beantwoorden.

In privacyvraagstukken kunnen de belangen van betrokkenen op gespannen voet staan met bestuurlijke doelen. Dat vraagt begrip voor beide kanten, bestuurlijke sensitiviteit en een goed gevoel voor verhoudingen.

Onafhankelijkheid

De FG mag geen instructies krijgen over de uitvoering van zijn taken. Ook mag hij niet worden ontslagen of gestraft voor de uitvoering van zijn taken. Dat staat expliciet in de AVG, om de FG in alle vrijheid zijn adviezen te laten geven en zo nodig rechtstreeks verslag uit te brengen aan directie of college. Dit is een bescherming die vergelijkbaar is met die van de concerncontroller en van OR-leden.

Plek in de organisatie

Dit alles overziend is de vraag waar en bij wie de rol van FG te beleggen. Vanwege de gevraagde kennis en vaardigheden is het advies de taak bij de strategisch privacyadviseur te leggen.

Vanwege de toezichthoudende rol moet een FG niet zelf verantwoordelijk zijn voor beslissingen waarin persoonsgegevens kunnen worden geraakt. Dat betekent dat de taak niet bij een leidinggevende moet worden gelegd. Omdat de FG met alle vakafdelingen te maken heeft, is een centrale plek gewenst. Vanwege de onafhankelijkheid en het spanningsveld tussen advies en toezicht, is er een duidelijke parallel met de taken van de controllers. Als het een keer nodig is te waarschuwen dat ergens echt onaanvaardbare risico's worden genomen, is het slim om gebruik te kunnen maken van de lijn die de concerncontroller in dat opzicht al heeft. In de afdeling Concerncontrol zijn bovendien verschillende kennisgebieden vertegenwoordigd die deels overlappen met of raken aan privacy: via de strategisch adviseurs op het gebied van

informatiebeveiliging, informatiebeheer en privacy. Daarnaast vallen ook de IT-auditor en de interne accountant onder Concerncontrol. Dat vergemakkelijkt de samenwerking om een goede governance te organiseren. Daarbij zijn overigens ook de privacyadviseur en de adviseur informatiebeveiliging van de afdeling Interne Dienstverlening en de adviseur Informatiebeheer van de afdeling Informatievoorziening belangrijke partners. Zij zijn samen verantwoordelijk voor de advisering – in samenhang – op tactisch niveau.

Conclusie

Het advies is de strategisch privacyadviseur in de afdeling Concerncontol aan te wijzen als FG. Deze zal om de rol waar te maken moeten samenwerken met collega's uit aanpalende vakgebieden en met de tactisch adviseurs op het gebied van privacy, informatiebeveiliging en informatiebeheer.
NB: Om aan alle eisen van de AVG te kunnen voldoen, is naar verwachting versterking nodig. Dit komt aan de orde in de notitie over de AVG.