De functionaris gegevensbescherming in het ritme van de stad

Een model voor de middelgrote gemeente.

mr. Angelique Schepers

9 mei 2021

De functionaris gegevensbescherming in het ritme van de stad

Een model voor de middelgrote gemeente.

MASTERTHESIS
MASTER PUBLIC MANAGEMENT

door
mr. Angelique Schepers
S2263041

begeleider
Dr. J.A.M. De Kruijf

tweede lezer
Dr. ir. J. de Leede

Universiteit Twente
Drienerlolaan 5, 7522 NB Enschede

Zoetermeer 9 mei 2021

SAMENVATTING

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Deze verordening gaat over het rechtmatig omgaan met persoonsgegevens. In deze verordening is opgenomen dat bepaalde organisaties, zoals gemeenten, een functionaris voor gegevensbescherming moeten aanstellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.

Het doel van dit onderzoek is om de middelgrote gemeente te voorzien van een model dat gebruikt kan worden om de functionaris voor gegevensbescherming in de organisatie te positioneren op een wijze dat wordt voldaan aan de uitgangspunten van de regelgeving. Daarnaast is het een hulpmiddel voor de functionaris voor gegevensbescherming bij de uitoefening van zijn functie.

Om dit model op te stellen is literatuuronderzoek en kwalitatief onderzoek gedaan. Bij het literatuuronderzoek is de gemeentelijke organisatie en het begrip toezichthouder onderzocht. Vervolgens is de relevante wet- en regelgeving en de toelichting hierop nader bekeken. Op basis van dit literatuuronderzoek is een driedeling gemaakt. Deze driedeling bestaat uit de taken van de functionaris voor gegevensbescherming, de eisen die aan de organisatie worden gesteld en de eisen die aan de functionaris voor gegevensbescherming worden gesteld. Alle eisen die uit het onderzoek van de regelgeving naar voren zijn gekomen zijn opgenomen in een model dat als basis heeft gediend voor de tweede fase van het onderzoek, het kwalitatief onderzoek. Hiervoor is veldonderzoek gedaan in de vorm van interviews. Een twaalftal functionarissen voor gegevensbescherming, die werkzaam zijn bij een middelgrote gemeente zijn geïnterviewd. De interviews zijn geanalyseerd en op basis van de analyse zijn aanvullingen op het model gemaakt. Alle aanvullingen die uit het veldonderzoek voortkomen betreffen geen wettelijke vereisten maar zijn hulpmiddelen die ter ondersteuning zijn aan de middelgrote gemeente en de functionaris voor gegevensbescherming.

Uit het onderzoek blijkt dat functionaris voor gegevensbescherming naast toezichthouden ook een hele expliciete adviestaak heeft. Uit het kwalitatieve onderzoek is naar voren gekomen dat deze adviestaak verschillend wordt ingevuld. Dit heeft met name te maken met de fase waarin de gemeentelijke organisatie zich bevindt. Hoe minder kennis op het gebied van gegevensbescherming in de organisatie hoe meer de functionaris voor gegevensbescherming aan de voorkant van processen betrokken is en adviseert. Indien er meer bewustzijn in de organisatie zelf aanwezig is, of als er een duidelijke keuze is gemaakt dat de functionaris zich met voornamelijk met toezicht zal bezighouden dan wordt de adviesrol voornamelijk vanuit een toezichthoudend kader uitgevoerd.

Kijkend naar de opgestelde driedeling kan over het onderdeel taken van de functionaris voor gegevensbescherming uit de regelgeving worden opgemaakt dat dit gaat over het informeren en adviseren, toezien op de naleving van regelgeving, toezien op de naleving van gemeentelijk beleid, zichtbaar zijn naar het personeel, toetsen van data protection impact assessments, contactpersoon van de Autoriteit Persoonsgegevens zijn en hier ook mee samenwerken. Ook moet er gerapporteerd worden aan de hoogste leidinggevende. Uit het kwalitatieve onderzoek zijn aanvullingen op de taken van de functionaris voor gegevensbescherming gemaakt. Het gaat hierbij om het duidelijk uitspreken waar de verantwoordelijkheid voor gegevensbescherming in de organisatie ligt, gebruik van het borgingsdocument VNG, gebruik van audits, het aangaan van samenwerkingen binnen en buiten de organisatie, werken aan

zichtbaarheid, zorgen dat bekend is in de organisatie dat de FG de contactpersoon van de Autoriteit Persoonsgegevens is en de wijze van verantwoording afleggen.

Het tweede punt uit het drieluik betreft de eisen aan de organisatie. Uit de regelgeving is op te maken dat de gemeente de functionaris voor gegevensbescherming naar behoren en tijdig moet betrekken. De functionaris moet toegang hebben tot alle persoonsgegevens en verwerkingsactiviteiten. Daarnaast moet de functionaris over voldoende middelen beschikken. De functionaris mag geen instructies ontvangen of benadeeld worden. De functionaris moet toegang hebben tot hoogste leidinggevende. Hij moet goed bereikbaar zijn voor betrokkenen, is gehouden aan geheimhouding en vertrouwelijkheid en er mag geen belangenverstrengeling ontstaan. Uit voorgaande blijkt dat deze eisen aan de organisatie vooral betrekking hebben op de onafhankelijke taakuitoefening van de functionaris voor gegevensbescherming. De aanvullingen uit het kwalitatieve onderzoek betreffen aanwijzingen aan de organisatie om hier meer invulling aan te geven zoals betrokkenheid van de functionaris voor gegevensbescherming bij projecten een aanbestedingen, het beschikbaar stellen van scholing en zorgen voor een regelmatige overlegstructuur.

Het laatste punt van het drieluik betreft de eisen die aan de functionaris zelf worden gesteld. Dit is van belang voor de gemeentelijke organisatie bij de werving van een functionaris voor gegevensbescherming of kan behulpzaam zijn voor de persoonlijke ontwikkeling van de functionaris zelf. Uit de regelgeving komt naar voren dat het hier gaat over niveau van deskundigheid, professionele kwaliteit, ervaring met wetgeving, kennis van de bedrijfstak/organisatie, inzicht in verwerkingsactiviteiten, kennis van administratieve regels en procedures, het vermogen om de taken te vervullen en ook zaken zoals persoonlijke vaardigheden en kennis en de positie in de organisatie. Uit het kwalitatieve onderzoek komt naar voren dat het van belang is dat er gezocht wordt naar een functionaris die past bij de organisatie en het niveau van volwassenheid op het gebied van gegevensbescherming. Vooral vaardigheden zijn van belang en competenties waarbij als belangrijkste worden genoemd de wijze waarop de functionaris communiceert, op verschillende niveaus kan schakelen, analytisch inzicht heeft, goede adviesvaardigheden moet hebben en stevig in zijn schoenen moet staan. Daarnaast is het van belang dat de functionaris voor gegevensbescherming geïnteresseerd is wetgeving en juridische affiniteit heeft. Vanuit een positie bij een staf/control afdeling kan de functie het beste worden uitgevoerd. Ook is het van belang dat de functionaris voor gegevensbescherming een vervanger heeft die zijn taken kan overnemen indien die zelf teveel inhoudelijk advies heeft gegeven of afwezig is.

Dit geheel is opgenomen in een praktisch bruikbaar model dat is voorzien van een toelichting.

INHOUDSOPGAVE

VOORWOORD

Met veel plezier heb ik de masteropleiding Public Management aan de universiteit Twente gevolgd. Deze thesis is de afsluiting van een leerzame periode. Naast kennis heb ik ook leuke contacten heb opgedaan. Deze thesis schreef ik in de winter en voorjaar 2020/2021. Een winter waarin vanwege de uitbraak van de Covid-19 pandemie een lockdown was. Vermaak moest binnenshuis gevonden worden. Ik heb die gevonden in het schrijven van deze thesis.

Werken en mijzelf ontwikkelen zijn zaken die in mijn werkzame leven samen optrekken. Na een lange middelbare schoolperiode van mavo naar havo en vervolgens vwo besloot ik te gaan werken. Hier ontdekte ik toch al vrij snel dat je zonder opleiding niet veel verder komt. Om zo snel mogelijk een functie van enig niveau te kunnen bekleden deed ik in de avonduren de hbo-opleiding sociaal juridische dienstverlening. Een leuke opleiding maar ik miste diepgang. Ik deed vervolgens de studie Nederlands Recht aan de universiteit Leiden. Daarna deed ik nog een aantal postacademische opleidingen. Steeds lukte het mij om ook stappen in mijn carrière te maken. Zes jaar geleden heb ik de overstap gemaakt naar management ben ik vooral bezig met daar verder in te ontwikkeling. Deze Master Public Management past dan ook goed in deze lijn.

Ik heb gekozen voor dit onderwerp omdat ik zelf naast manager juridische aangelegenheden & bestuursondersteuning bij de gemeente Zoetermeer ook functionaris voor gegevensbescherming ben. Ten tijde van de implementatie van de Algemene Verordening Gegevensbescherming leek dit een logische keuze. Nu na een aantal jaar kan je de vraag stellen of dit nog steeds een goede keuze is en leek het mij een goed idee om hier onderzoek naar te doen.

In dit voorwoord wil ik van de gelegenheid gebruik maken om de diverse mensen te bedanken. Zij hebben het mogelijk gemaakt dat ik de opleiding nu kan afronden.

Voor deze thesis heb ik twaalf functionarissen voor gegevensbescherming geïnterviewd. Ik wil ze bedanken voor de medewerking. Iedereen is anonimiteit toegezegd. Een respondent heeft afstand gedaan van zijn anonieme deelname en via hem, te weten Frank van Vonderen, wil ik alle geïnterviewden bedanken voor de tijdsbesteding en input. Ik heb genoten van de interviews.

Daarnaast mijn werkgever de gemeente Zoetermeer. Een prettige organisatie die altijd veel heeft geïnvesteerd in haar medewerkers, een gemeente waar het mogelijk is om jezelf te ontwikkelen.

Ook wil ik bedanken mijn begeleider Johan de Kruijf, zeker voor zijn scherpe blik.

En als laatste bedank ik mijn echtgenoot Gerben. De eerste onofficiële beoordelaar.

1. INLEIDING

1.1. Aanleiding

Privacy en gegevensbescherming, een onderwerp dat de afgelopen jaren flink in de aandacht staat. Ook een onderwerp waar inmiddels iedereen een mening over heeft. Zo roept de een heel hard ‘ik heb niets te verbergen’ tegenover de ander die niets deelt.

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) van kracht. Een Europese verordening met rechtstreekse werking in de lidstaten van de Europese Unie. Deze verordening gaat over het rechtmatig omgaan met persoonsgegevens. Om deze rechtmatige omgang met persoonsgegevens binnen organisaties goed te regelen is ook in deze verordening opgenomen dat bepaalde organisaties een functionaris voor gegevensbescherming moeten aanstellen. Een functionaris die kan adviseren en toezien op de juiste naleving van de verordening. In dit onderzoek wordt de functionaris voor gegevensbescherming bij een middelgrote gemeentelijke organisatie nader bekeken. Voor de definitie van middelgrote gemeente is aangesloten bij de definitie van het stedennetwerk G40. Op de website van de G40 (https://www.g40stedennetwerk.nl/) is te lezen dan het G40-stedennetwerk het netwerk is van 40 middelgrote steden, die elkaar vinden in de stedelijke vraagstukken waar de leden van het netwerk voor staan Het betreft een groep die met dezelfde stedelijke vraagstukken te maken hebben en hierdoor op elkaar lijken.

Binnen een gemeentelijke organisatie zijn de belangrijkste taken van de functionaris voor gegevensbescherming het informeren en adviseren van de gemeente over haar verplichtingen op het gebied van gegevensbescherming. Het gaat om verplichtingen die voortvloeien uit de AVG en de overige wetgeving omtrent gegevensverwerking en gegevensbescherming. Daarnaast moet de functionaris toezien op naleving van de AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming. Ook moet de functionaris voor gegevensbescherming toezien op het naleven van gemeentelijke beleid dat betrekking heeft op de bescherming van persoonsgegevens. De functionaris is ook belast met het opleiden van personeel en het uitvoeren of toezien op Data Privacy Impact Assessments (DPIA). Het landelijke toezichthoudende orgaan is de Autoriteit Persoonsgegevens (AP). De functionaris zal met de AP moeten samenwerken en is ook het eerste aanspreekpunt bij de gemeente. De functionaris zelf brengt verslag uit aan het hoogte leidinggevende niveau.

Dit alles zal de functionaris vanuit een onafhankelijke positie moeten uitvoeren. Het belang dat de functionaris in het oog moet houden is de juiste naleving van de regelgeving omtrent gegevensbescherming en niet het belang van de gemeente. Door deze verschillende belangen kan de functionaris mogelijk in een spagaat komen. Hoe behoud je als functionaris voor gegevensbescherming deze onafhankelijke positie binnen een hiërarchische structuur. Wat het nog extra complex maakt is dat de taak van functionaris voor gegevensbescherming mogelijk wordt gecombineerd met een andere functie. Dit kan de uitoefening van de onafhankelijke taak complexer maken. En dit alles in een omgeving van een publieke organisatie die steeds meer wordt geconfronteerd met complexe vraagtukken en snel veranderende technologie, de zogenoemde wicked problems (Boersma-De Jong et al., 2017). Of zoals Turnbull & Hoppe (2018) het noemen complexe problemen. Het gaat over beleidsproblemen die in verschillende gradaties en complexiteit voorkomen.

De wetgever heeft wel een aantal uitgangpunten meegegeven. Een duidelijke taakomschrijving en daarnaast eisen die aan de organisatie en de functionaris worden gesteld.

1.2. Probleemanalyse

De functionaris gegevensbescherming is met de implementatie van de AVG niet geheel nieuw. In de reeds ingetrokken Wet Bescherming Persoonsgegevens uit 2001 werd al gesproken over de functionaris voor gegevensbescherming. Het was onder die wet geen verplichting om er een aan te stellen. Wel waren er organisaties die er een aanstelden en is er sinds 2003 in Nederland een beroepsvereniging aanwezig, het Nederlands Genootschap voor Functionarissen voor Gegevensbescherming. Met de implementatie van de AVG is het aanstellen van een functionaris voor gegevensbescherming voor bepaalde organisaties een wettelijke verplichting geworden. De gemeentelijke organisatie is een van de organisaties waarvoor de wettelijke plicht om een functionaris voor gegevensbescherming aan te stellen geldt. De vraag die gesteld kan worden is of gemeenten uit de voeten kunnen met de door de wetgever geformuleerde uitgangspunten. En op welke wijze kan de functionaris voor gegevensbescherming zijn taak echt onafhankelijk uitoefenen.

1.2.1. Doelstelling

Het doel van dit onderzoek is om de middelgrote gemeente te voorzien van een model dat gebruikt kan worden om de functionaris voor gegevensbescherming in de organisatie te positioneren op een wijze dat wordt voldaan aan de uitgangspunten van de regelgeving. Daarnaast is het een hulpmiddel voor de functionaris voor gegevensbescherming bij de uitvoering van de functie.

Dit model bevat een overzicht van de in de regelgeving opgenomen uitgangspunten waar middelgrote gemeenten rekening mee moeten houden bij de aanstelling en positionering van deze functionaris. Deze uitgangspunten zijn nader aangevuld met uitgangspunten die vanuit veldonderzoek (interviews) naar voren zijn komen. Daarnaast is deze thesis ook een zoektocht of bepaalde begrippen uit de regelgeving eenduidig worden uitgelegd. Verstaan verschillende gemeenten hetzelfde onder de wettelijk geformuleerde uitgangspunten.

In het theoretische kader worden de uitgangpunten uit de regelgeving gedistilleerd. In het veldonderzoek zal dit normenkader met uitgangspunten naast de werkelijkheid worden neergelegd om zo te zien of er discrepantie ontstaat en of er aanvullingen zijn.

Aangesloten wordt bij de driedeling zoals ook in de regelgeving wordt gebruikt:

- Taken functionaris voor gegevensbescherming;
- eisen aan de organisatie;
- eisen aan de functionaris voor gegevensbescherming.

1.2.2. Onderzoeksvraag

Om de doelstelling van dit onderzoek te halen is de volgende onderzoeksvraag ontwerpend geformuleerd:

Ontwerp een model met hierin opgenomen de uitgangspunten voor de middelgrote gemeente en de daar aangestelde functionaris voor gegevensbescherming. Voor de gemeentelijke organisatie is dit model een hulpmiddel om de functionaris voor gegevensbescherming te positioneren en tot een juiste taakuitoefening te laten komen. Voor de functionaris gegevensbescherming biedt dit model een handvat voor een juiste uitoefening van zijn taken.

1.2.3. Deelvragen

Theoretische deelvragen:

1. Wat zijn de uitgangspunten (vanuit de regelgeving) waaraan voldaan moet worden zodat de functionaris gegevensbescherming zijn functie kan uitoefenen.
2. Zijn al deze uitgangspunten van gelijkwaardig belang.
3. Hoe kan de organisatie waarborgen dat aan deze uitgangspunten voldaan worden.
4. Hoe kan de functionaris gegevensbescherming in de organisatie gepositioneerd worden.

Zodra deze deelvragen vanuit de literatuur beantwoord zijn wordt een model opgesteld. In dit model wordt opgenomen de taken van de Functionaris voor Gegevensbescherming, de eisen die gesteld worden aan de organisatie en de eisen die gesteld worden aan de functionaris voor gegevensbescherming. Vervolgens zal de volgende fase van het onderzoek ingaan en zal dit opgestelde model in het veldonderzoek als basis voor de interviews dienen en om de volgende vraag te beantwoorden.

Empirische deelvraag:

5. Levert het veldonderzoek nieuwe uitgangspunten op die aan het model, dat op basis van de theorie is opgesteld, toegevoegd moeten worden.

1.3. Relevantie onderzoek

Het uitvoeren van onderzoek aan de universiteit moet relevant zijn voor de maatschappij en wetenschap.

1.3.1. Maatschappelijke relevantie

Dit onderzoek is maatschappelijk relevant omdat een juiste uitvoering van de regelgeving omtrent gegevensverwerking en gegevensbescherming kan bijdragen aan het vertrouwen van de burger in de overheid. Een wettelijk verplichte functionaris voor gegevensbescherming is geïntroduceerd met de implementatie van de AVG. Er is nog niet eerder onderzoek gedaan naar hoe middelgrote gemeenten op

een juiste wijze uitvoering kunnen geven aan de door de wetgever benoemende uitgangspunten, of deze eenduidig worden uitgelegd en of deze uitgangspunten voldoende zijn voor een juiste taakuitoefening. Dit onderzoek zal gemeenten en functionaris voor gegevensbeschermingen helpen bij een juiste wijze van taakuitoefening en positionering van deze functionaris.

1.3.2. Wetenschappelijke relevantie

Dit onderzoek is wetenschappelijk relevant omdat bestaande kennis en wettelijke uitgangspunten nader ingevuld zullen worden. Ook zullen ze worden uitgebreid met uitgangspunten die uit het veldonderzoek naar voren komen. Slechts een, niet wetenschappelijk onderzoek is eerder uitgevoerd (Centrum voor Informatiebeveiliging en Privacybescherming, 2018). Dit onderzoek is breder van opzet, qua onderzoeksvraag en qua deelnemers. Deze thesis vult een leegte op. Een goed uitgewerkt theoretisch kader over de functionaris voor gegevensbescherming binnen de gemeentelijke organisatie en dit nader ingevuld door kwalitatief onderzoek.

1.3.2. Leeswijzer

In deze inleiding is de doelstelling van het onderzoek en de relevantie weergegeven. Hierna zal eerst het theoretisch kader uiteengezet worden. Dit is op basis van literatuuronderzoek uitgevoerd. Vervolgens zal het onderzoeksontwerp en dataverzameling van het kwalitatieve onderzoek nader worden uitgewerkt. Daarna is de analyse van de verzamelde data weergegeven met resultaten en aanbevelingen. Het geheel komt samen in het hoofdstuk conclusies en model. Hier worden de in hoofdstuk 1 geformuleerde onderzoeksvragen beantwoord en een model gepresenteerd. Als laatste is de reflectie toegevoegd. In de bijlagen zijn de documenten opgenomen, het gaat hier om de aan de respondenten toegezonden informatie (bijlagen A en B) en het gebruikte interviewschema (bijlage C).

2. THEORETISCH KADER

2.1. Inleiding

In het inleidende hoofdstuk is te lezen dat de functionaris voor gegevensbescherming binnen een gemeentelijke organisatie als adviseur optreedt maar ook toezicht moet houden op de gemeente. Toezicht op de werkzaamheden die de gemeente uitvoert. Hierbij is het van belang of deze werkzaamheden in overeenstemming worden uitgevoerd met de geldende regelgeving omtrent gegevensbescherming. Dit toezicht moet de functionaris voor gegevensbescherming onafhankelijk kunnen uitvoeren.

Het verwerken van gegevens is niet nieuw voor gemeenten. Sinds het bestaan van gemeenten worden er persoonsgegevens verwerkt en moet dit zorgvuldig gebeuren. Berkvens en Prins (2014) schreven al dat de verantwoordelijke zich niet alleen aan zijn wettelijke verplichtingen dient te houden maar dat hij bovendien binnen zijn organisatie toezicht moet organiseren op de naleving. Het verplicht aanstellen van een functionaris die moet adviseren en toezicht houden op de gegevensbescherming is sinds 2018 nieuw. Voor 2018 bestond de functie functionaris voor gegevensbescherming al, deze werd zelfs genoemd in de toen geldende Wet Bescherming Persoonsgegevens, echter was het geen verplichting om er een aan te stellen. Met de AVG is het aanstellen van de functionaris voor gegevensbescherming een verplichting geworden en door de opname in de AVG is de wettelijke verankering op het toezicht op de naleving in de regelgeving geborgd.

2.2. Gemeentelijke organisatie

Gemeenten zijn er in diverse soorten en maten. Zo heeft de grootste gemeente van Nederland Amsterdam volgens het CBS per 1 januari 2020 872.757 inwoners en de kleinste gemeente Schiermonnikoog per dezelfde datum slechts 947 inwoners. Voor deze thesis wordt als uitgangspunt genomen de middelgrote gemeente. Voor de definitie van middelgroot wordt aangesloten bij die van de G40-stedennetwerk. Dit betreft een stedennetwerk van de 40 (middel)grote gemeenten in Nederland, die elkaar vinden in de stedelijke vraagstukken waar de leden van het netwerk voor staan.

Een gemeente is een lichaam van het openbaar bestuur. Een gemeente is hiermee, in tegenstelling tot een private partij, naast de geldende regelgeving die betrekking heeft op dataverwerking ook altijd gebonden aan de algemene beginselen van behoorlijk bestuur. Dit betreft een stelsel van geschreven en ongeschreven regels waar overheden zich aan dienen te houden. Een burger kan namelijk niet kiezen met welke overheid hij zaken gaat doen, of als het niet bevalt bij de ene overheid naar een andere gaan. De machtsverhouding tussen de burger en de overheid is altijd ongelijk, daarom zijn deze extra beginselen noodzakelijk om de burger te beschermen. Het gaat om geschreven regels uit wetgeving, met name de Algemene wet bestuursrecht, zoals onder andere het zorgvuldigheidsbeginsel (art. 3:2 Awb), het motiveringsbeginsel (art. 3:46 Awb), onpartijdigheid (art. 2:4 Awb) en het Verbod op détournement de pouvoir (art. 3:3 Awb). Maar ook het gelijkheidsbeginsel uit de Grondwet (art. 1 GW). Daarnaast zijn er ook

ongeschreven beginselen van behoorlijk bestuur die niet in de wet zijn vastgelegd maar voortkomen uit de jurisprudentie zoals het vertrouwensbeginsel.

Deze algemene beginselen van behoorlijk bestuur zijn ook van belang voor de functionaris van gegevensbescherming die bij de overheid werkt. Het is niet altijd mogelijk om op wetgeving terug te vallen omdat niet alles in wetgeving is gereguleerd. Zo is bijvoorbeeld op dit moment datagebruik alleen nog maar gereguleerd door de algemene beginselen van openbaar bestuur (Drahmann, 2019).

2.2.1 Organisatieinrichting

Gemeenten van middelgroot formaat hebben de afgelopen drie decennia verschillende organisatiemodellen gebruikt. Het secretariemodel, het sectorenmodel/(concern)dienstenmodel en in de laatste jaren het directiemodel/afdelingenmodel (Aardema en Korsten, 2009). Aardema en Korsten (2009) merken op dat veel gemeenten van 100.000 + inwoners in 2009 nog gebruik maakten van het (concern) dienstenmodel. Op dit moment maken steeds meer gemeente de omslag naar opgavegericht werken.

Aardema en Kosten (2009) omschrijven het sectorenmodel- of (concern) dienstenmodel als een organisatie waarbij de verschillende beleidsterreinen zijn geclusterd naar een dienst of sector b.v. ruimte of inwoners. Zo is het beleidsmatige werk steeds gecombineerd met het uitvoerende werk op het desbetreffende beleidsterrein. De invoering hiervan ging bij veel gemeenten gepaard met het idee dat er ‘bedrijfsmatiger’ gewerkt zou moeten worden (Aardema, 2002). Echter had dit weer tot nadeel dat er veel verkokering ontstond. Deze verkokering is het meest genoemde nadeel van dit model (Aardema en Koster, 2009).

Bij het directie/afdelingenmodel wordt gebruik wordt gemaakt van een indeling volgens ‘burgerlogica’ met een beleidsafdeling, een buitenafdeling, een frontoffice en een backoffice (Aardema en Koster, 2009).

Zitten de controllers en toezichthouders in het sectorenmodel binnen de eigen sector, in het directiemodel zullen deze meer gezamenlijk werken van uit een ondersteunende bedrijfsvoeringsafdeling.

Een andere ontwikkeling die binnen gemeenten heeft gespeelt is de opkomst van New Public Management (NPM) (Hood, 1991). Waarbij overheden meer zijn gaan samenwerken met private partijen en zichzelf ook zo zijn gedragen om te komen tot goedkopere, betere en meer publieke diensten en producten. De basis van New Public Management ligt in het verminderen of verwijderen van verschillen tussen de publieke en private sector en het verleggen van het accent op input- en procesverantwoording naar verantwoording over resultaten (Van Helden en Jansen, 2002, Hood, 1995).

Volgens Vosselman (2011) heeft de ontwikkeling van New Public Management geleid tot een sterke control mentaliteit in de publieke sector. Vosselman (2011) schetst dat door de toename van besturings- en controlconcepten binnen publieke organisaties de rationele mens, die hij Homo Economics 2.0 noemt heeft voortgebracht. Hij pleit voor een ontwikkeling in de richting van een steward, zoals een steward die tijdens een voetbalwedstrijd vriendelijk toezicht houdt. Overtollig wantrouwen moet plaats maken voor vertrouwen, afrekening moet plaats maken voor de ontwikkeling van leervermogen. Vosselman (2011) pleit voor vernieuwing via het discours Public Value. Een concept van Mark Moore van de Harvard University waar het meer gaat over de waardering die de burger heeft voor het optreden van de overheid en haar organisatie (Moore, 1995).

Bij een middelgrote gemeente wordt er op het gebied van risicobeheersing en controle vaak gewerkt via het model van three lines of defence. Een model dat is ontwikkeld door The Institute of Internal Auditors (2013). In een gemeentelijke organisatie komt dit neer op de volgende indeling. Er is een eerste lijn, de vakafdeling, die is zelf verantwoordelijk voor haar activiteiten. In het geval van gegevensbescherming binnen een gemeente is de vakafdeling zelf verantwoordelijk voor het product dat de afdeling aflevert, inclusief een goede gegevensbescherming. De manager is integraal verantwoordelijk. Hierbij kan de afdeling ondersteuning, van een meer gespecialiseerd iemand krijgen, dit is de tweede lijn. Op het gebied van gegevensbescherming zijn dit vaak privacy officers (PO-ers) die inhoudelijk meer kennis hebben. Vervolgens is er de derde lijn, dit betreft de controle functie zoals de concerncontroller, de Chief Information Officer (CIO) en op het gebied van gegevensbescherming zou de Functionaris voor Gegevensbescherming als derde lijn gezien kunnen worden.

2.2.2. Toezichthouders binnen een gemeentelijke organisatie

Binnen een gemeentelijke organisatie werken diverse toezichthouders. Gemeentebesturen zijn verantwoordelijk voor het toezicht en handhaving van veel wet- en regelgeving, het aantal ligt rond de 190 wetten en daarop gebaseerde regelgeving (Winter en Mein, 2017). In deze thesis zijn de toezichthouders van belang die toezicht houden op de eigen organisatie. Hiervan zijn er binnen de gemeentelijke organisatie diverse te vinden. Zo is er bij veel gemeenten een concerncontroller. Maar er zijn ook commissies, zoals de klachtencommissie of bezwarencommissie, die in opdracht van het bestuursorgaan de oorspronkelijke besluiten beoordelen en adviseren over de afhandeling. Ook zijn er gemeenten die met een juridische controller werken. Schuiling en Winter (1997) pleitten hier al voor bij de invoering van het dienstenmodel. Zij omschreven de juridisch controller als ‘iemand die binnen een organisatie verantwoordelijkheid draagt voor respectievelijk de advisering, het beheer, de uitvoering en rapportage ten aanzien van één of meerdere voor deze organisatie essentiële voorwaardenscheppende functies’ (Schuiling en Winter, 1997).

De opkomst van New Public Management en de meer zakelijke benadering van een gemeentelijke organisatie loopt gelijk op de opkomst van de controller. Zo deden controllers begin jaren 80 hun intrede in gemeentelijke organisaties. In de publieke sector werd de controller al direct breder dan alleen financieel gepositioneerd. In overheidsorganisaties is de beoordeling van doelmatigheid immers niet alleen gericht op het behalen van financiële resultaten maar op het al dan niet behalen van maatschappelijke doelstellingen en effecten (Anderson, 2006). De controller onderzoekt, adviseert, ondersteunt, speelt een rol in de planning & control cyclus, verstrekt informatie, bepaalt mede de strategie, voorziet het management van kritische reflectie en speelt in overheidsorganisaties ongetwijfeld nog zeer veel andere rollen (Anderson, 2006). Niet elke gemeente heeft een controller en de uitoefening van de functie kan ook per gemeente verschillen.

Ten aanzien van de positionering van de controller binnen de gemeentelijke organisatie, kan gesteld worden dat concerncontrollers doorgaans zijn gepositioneerd binnen een stafafdeling die direct verbonden is aan de functie van een gemeentesecretaris (Van der Velden, 2002). De ideale positionering kan niet eenduidig worden aangegeven (Anderson, 2006).

Een andere interessante functionaris die binnen de gemeente onafhankelijk opereert is de Chief Information Security Officer (CISO). Doordat de Baseline Informatiebeveiliging Overheid (BIO) als

normenkader verbindend is verklaard, hanteert de overheid een basisniveau voor informatiebeveiliging. Dit is nog maar van recente datum te weten 1 januari 2020. Per die datum is de aanstelling van een CISO ook voor gemeenten verplicht geworden. De CISO heeft een controlerende en adviserende rol op het gebied van informatiebeveiling. Informatiebeveiliging en de gegevens die in de systemen worden opgenomen en verwerkt gaan hand in hand. De CISO is dan ook een belangrijke partner voor de functionaris voor gegevensbescherming binnen de gemeente.

Goed om bij dit onderwerp in het oog te houden is dat gegevensverwerking, waarop toegezien moet worden door de functionaris voor gegevensbescherming, voornamelijk digitaal plaatsvindt. Binnen de eigen gemeentelijke organisatie maar ook grotendeels bij externe partijen. Dit doordat systemen van gemeenten steeds mee in handen zijn van private partijen. Veel ICT-oplossingen hangen in de cloud of draaien op servers van private partijen. Partijen die door middel van (Europese) aanbestedingen zijn geselecteerd. Dit geeft een extra dimensie aan dit onderwerp. Meijer et al. (2019) geven aan dat deze snelle technologische veranderingen het lokaal bestuur voor grote uitdagingen plaatst. In het rapport van het Rathenau Instituut (2017) worden een vijftal actiepunten voorgesteld om het governancelandschap te kunnen opwaarderen. Het tweede actiepunt betreft: 2. “Versterk de rol en positie van toezichthouders”. In dit rapport wordt de overheid opgeroepen om normerende kaders op te stellen waaraan de aanschaf, ontwerp en inrichting van systemen moeten voldoen, en waar toezichthouders en handhavers op kunnen toetsen. Bijvoorbeeld door vast te stellen hoe een software-ontwikkelaar verantwoording kan afleggen over de werkwijze van complexe algoritmen, zodat softwareontwikkelaars dat in het ontwerp van het systeem inbouwen (Rathenau Instituut, 2017).

De borging van data-opslag, beheer en hoe om te gaan met leveranciers die in gemeentelijke systemen kunnen wordt in de BIO nader uitgewerkt. Onderdeel van de BIO is ook het afsluiten van een verwerkersovereenkomst met leveranciers die persoonsgegevens voor gemeenten gaan verwerken (BIO, p. 59). Bij de gemeentelijke accountantscontrole wordt hier steekproefsgewijs op gecontroleerd. Op het gebied van de opslag van data worden afspraken gemaakt over het niveau van beveiliging, de benodigde certificaten of het overleggen van gedane penetratietests. Op het gebied van privacy is de ISO 27001-norm voor informatiebeveiliging uitgebreid met een privacyparagraaf.

Uit onderzoek (Dijck et al., 2016) is geconstateerd dat de opkomst van onlineplatformen een grote impact heeft op de inrichting van onze samenleving en met name op de wijze waarop publieke belangen en waarden daarin verankerd zijn. Overheden kunnen zelf initiatiefnemer zijn van een platform of deelnemer. Dijck et al. (2016) stelt dat overheden bij het beslissen van het gebruiken of toelaten van apps, eisen moeten stellen aan de voorwaarden waaronder dat gebruik kan plaatsvinden. Door toegang te eisen kan de toezichthouder controleren.

De omgeving waarbinnen het lokaal bestuur functioneert verandert snel door processen van informatisering en dataficatie (Meijer et al., 2019). In de uitvoering treden er voortdurend onvoorziene, maar belangrijke veranderingen op (Robertson, 2015). Het gaat om fundamentele keuzen over de positionering van lokaal bestuur en de noodzakelijke transitie van de overheidsorganisatie (Meijer et al., 2019). Hierin is de positionering van de functionaris voor gegevensbescherming van belang.

2.3. Toezichthouder

Zoals in de inleiding is te lezen is de functionaris voor gegevensbescherming een medewerker die moet toezichthouden op de naleving van regelgeving omtrent de verwerking van persoonsgegevens. Kijkend naar de internet versie van de Van Dale wordt toezicht gedefinieerd als*: hoede, zorg, controle: toezicht houden; onder toezicht staan*. Dit is heel ruim en algemeen.

Een definitie uit de literatuur over toezicht van Ruimschotel (2014, p. 12) is: "*Toezicht is kijken of het goed gaat, maar ook zorgen dat het goed gaat'.* Ruimschotel (2014, pp. 5-6) heeft het bij toezicht over een actief waakzame houding vanuit een plicht dat bestaat uit de volgende vier kenmerken:

1. Bemoeienis met de activiteiten van anderen. Bij toezicht sta je aan de zijlijn en kijk je toe, bij niet-toezicht sta je op het veld en speel je mee.
2. Het gaat steeds om een cluster van activiteiten met als componenten beschermen, waken en zorgen. Actieve waakzaamheid ten aanzien van iets buiten zichzelf, het liefst ook early warning, bijtijds ingrijpen en preventie.
3. Toezicht is conserverend en creëert niet. Bij toezicht worden geen nieuwe belangen of waarden gecreëerd, wordt geen beleid gemaakt los van toezichtsbeleid en er worden geen nieuwe dingen gemaakt, slechts bewaakt.
4. Toezicht is altijd meer of iets anders dan blinde uitvoering. Toezicht houdt altijd iets normerends in, het met enige objectiviteit en distantie beoordelen van iets of iemand anders. Bij uitvoering is men erop gericht het zelf te doen, bij toezicht kijkt men of anderen het goed doen.

Een ruime definitie van toezicht bevat de volgende drie elementen:

- Het verzamelen van de informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen;
- het vormen van een oordeel daarover;
- het eventueel naar aanleiding daarvan interveniëren (Ruimschotel, 2014, pp. 10-11).

Deze definitie is volgens Ruimschotel (2014, pp. 10-11) te ruim. Een conceptuele analyse van het woord toezicht laat verschillende aspecten zien: een activiteit (inspanningsverplichting) en een resultaat (resultaatsverplichting). De volgende elementen zijn van belang zoals verantwoordelijkheid, taak, plicht, zorgen, waken en belangeloosheid. Er moet verschil zijn met de situatie dat er geen toezicht is.

De Algemene Rekenkamer (2008, p. 16) schrijft over de onafhankelijkheid van goed toezicht het volgende. Toezicht moet als een afzonderlijke, onafhankelijke functie onderscheiden kunnen worden. Dat houdt in dat de toezichtfunctie gescheiden moet blijven van andere functies zoals beleid, regelgeving, uitvoering en advies. Dit betekent niet dat de toezichtfunctie altijd organisatorisch moet zijn afgezonderd maar van voldoende waarborgen zijn voorzien (Algemene Rekenkamer, 2008, p. 16).

2.4. Handhaving

Nauw verwant met toezicht is handhaving. Nadat informatie is verzameld en beoordeeld zou een volgende stap handhaving zijn. Het is goed om te kijken naar het verschil tussen toezicht en handhaving.

In de eerste kaderstellende visie op toezicht (2001) heeft het kabinet een onderscheid tussen toezicht en handhaving opgenomen. Bij toezicht gaat het om het verzamelen van informatie of een handeling of zaak voldoet aan de daaraan gestelde eisen, het oordelen daarover en het eventueel naar aanleiding daarvan interveniëren. Handhaving richt zich op de vraag of burgers, bedrijven en overheden zich aan de gestelde regels houden. Het is daarbij gericht op repressief optreden. Deze repressie is de bevoegdheid om dwang uit te oefenen en vrijheden te beperken. Ruimschotel (2014, p. 13) verwoordt het als volgt: 'het oog is symbool van toezien en de hand van handhaven'.

Toezichthouden kan op verschillende manieren. Het kabinet heeft in de tweede kaderstellende visie op toezicht (2005, pp. 14-18) een driedeling in soorten toezicht gemaakt. Als eerste is er nalevingstoezicht, hierbij wordt toegezien op handelingen van burgers en bedrijven. Dit is gericht op naleving van wet- en regelgeving. Een voorbeeld hiervan zijn de rijksinspecties zoals de Voedsel en Warenautoriteit. De tweede vorm van toezicht is uitvoeringstoezicht. Hierbij is er toezicht op de uitvoering van publieke taken door zelfstandige organisaties, een voorbeeld hiervan is de controle van het ministerie van Infrastructuur en Waterstaat op de RDW (een zelfstandig bestuursorgaan) op de juiste afgifte van kentekenbewijzen. Als derde is er interbestuurlijk toezicht, gericht op de uitvoering van publieke taken door medeoverheden. Zo houden provincies toezicht op de gemeentefinanciën.

De functionaris voor gegevensbescherming is adviseur en toezichthouder. Een toezichthouder die toezicht houdt op de juiste wijze van uitvoering van wet- en regelgeving. Hij houdt toezicht op het proces en vertoont hiermee de meeste overeenkomsten met een nalevingstoezichthouder. Echter is de nalevingstoezichthouder nauw verwant met handhaving en de functionaris voor gegevensbescherming houdt toezicht maar kan bij de constatering van onrechtmatigheden niet handhaven. De handhaver van de AVG is de nationale toezichthouder, in Nederland de Autoriteit Persoonsgegevens. De functionaris voor gegevensbescherming kan alleen de verwerkingsverantwoordelijke op de hoogte stellen van zijn bevindingen en/of het aan de AP melden. Als de verwerkingsverantwoordelijke dit advies naast zich neerlegt kan de functionaris voor gegevensbescherming zelf geen handhavingsactiviteiten ondernemen. Drewer en Miladinova (2018) noemen de functionaris voor gegevensbescherming dan ook de kanarie in de datamijn, hij kan alleen maar gaan roepen als hij gevaar ziet.

Daarnaast geeft de AVG ook rechten aan de betrokkenen gegeven om zelf toezicht te houden. In de artikelen 15-18 AVG zijn rechten opgenomen die door betrokkenen actief ingezet kunnen worden. Het gaat hier om het recht op inzage, rectificatie en aanvulling, vergetelheid en beperking van de verwerking. Deze rechten zijn bedoeld om betrokkenen in staat te stellen meer controle uit te oefenen en hierdoor hun achterstandspositie ten opzichte van de verwerkingsverantwoordelijke te verbeteren (Wolters, 2018). Binnen de gemeente is de functionaris voor gegevensbescherming het aanspreekpunt voor de betrokkenen.

2.5. Samenwerking Autoriteit Persoonsgegevens

Elk land in Europa dat uitvoering moet geven aan de AVG heeft een eigen toezichthoudende autoriteit. In Nederland is dat de Autoriteit Persoonsgegevens. In de AVG is opgenomen dat de functionaris voor gegevensbescherming de contactpersoon is van de organisatie waar die werkzaam is of waarmee een dienstverleningsovereenkomst is. Zodra er een onderzoek door de autoriteit wordt ingesteld dan zal de functionaris voor gegevensbescherming samenwerken met de Autoriteit Persoonsgegevens. Door het

gebruik van het woord ‘samenwerken’ zou de functionaris van gegevensbescherming gezien kunnen worden als een verlengde van de Autoriteit Persoonsgegevens.
De autoriteit heeft voordeel bij organisaties waar het toezicht goed is geregeld. Bij organisaties die zichzelf goed reguleren daar hoeft de toezichthouder minder capaciteit aan te wijden (De Bruijne et al., 2015).

Op de website van de Autoriteit Persoonsgegevens staat vermeld dat een belangrijke taak van de FG is intern toezicht houden op het naleven van de AVG. Om dit te kunnen doen, kan de functionaris voor gegevensbescherming:

- Informatie verzamelen over gegevensverwerkingen binnen de organisatie;
- deze verwerkingen analyseren en beoordelen of ze aan de wet voldoen;
- informatie, adviezen en aanbevelingen geven aan de organisatie.

Daarnaast heeft de Autoriteit Persoonsgegevens een e-mailadres ingesteld waar de aangemelde functionaris voor gegevensbescherming vragen kan stellen.

2.6. Juridisch kader

Het aanstellen van een functionaris voor gegevensbescherming is in de wetgeving, de AVG, verankerd. Niet elke organisatie die gegevens verwerkt moet een functionaris voor gegevensbescherming aanstellen. De verordening geeft hier duidelijke richtlijnen voor. In de verordening is opgenomen dat een functionaris voor gegevensbescherming verplicht is wanneer de verwerking door een overheidsorgaan wordt verricht (art. 37 lid 1 sub a AVG). Deze functionaris voor gegevensbescherming moet vervolgens ook worden aangemeld bij de bij de Autoriteit Persoonsgegevens, die hier ook op controleert. Is er geen functionaris voor gegevensbescherming aangemeld waar dit wel verplicht is kan er door de AP een sanctie worden opgelegd.

2.7. Functionaris Gegevensbescherming

De functionaris gegevensbescherming is met de implementatie van de AVG niet geheel nieuw. In de reeds ingetrokken Wet Bescherming Persoonsgegevens uit 2001 die de implementatie van Richtlijn 95/46/EG uit 1995 betrof stond opgenomen dat: ‘*verantwoordelijke of een organisatie waarbij verantwoordelijken zijn aangesloten kan een eigen functionaris voor de gegevensbescherming benoemen, onverminderd de bevoegdheden van het College ingevolge hoofdstuk 9 en 10 van deze wet’* (artikel 62 WBP).
De groep voor gegevensbescherming artikel 29 (hierna: WP29) is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer. De Groep schrijft dat het in de voorbije jaren in verschillende lidstaten toch een gewoonte is geworden om een functionaris voor gegevensbescherming aan te stellen (Groep gegevensbescherming artikel 29, 2017). WP29 beargumenteerde al voor de invoering van de AVG dat de functionaris voor gegevensbescherming de hoeksteen is van de verantwoording en dat het aanstellen van een functionaris gegevensbescherming de naleving kan vereenvoudigen. De naleving wordt vereenvoudigd door de implementatie van verantwoordingsinstrumenten en de functionarissen voor gegevensbescherming fungeren als tussenpersoon tussen relevante belanghebbenden (zoals

toezichthoudende autoriteiten, betrokkenen en bedrijfseenheden binnen een organisatie (Groep gegevensbescherming artikel 29, 2017)). De functionaris gegevensbescherming als 'de hoeksteen van de verantwoording' (Kadir, 2018 p. 25).

2.7.1 Taken van de functionaris voor gegevensbescherming

In artikel 39 AVG is uitgewerkt wat de taken van een functionaris voor gegevensbescherming zijn. Voor een functionaris gegevensbescherming die bij een gemeente werkt komt dit neer op de volgende taken:

- 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 (art. 39 lid 1 sub a AVG).
- Toezien op naleving van de AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming (art. 39 lid 1 sub b AVG).
- Toezien op naleving van het gemeentelijke beleid (art. 39 lid 1 sub b AVG).
- Het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de audits te weten de Data Protection Impact Assessments (DPIA) (art. 39 lid 1 sub b juncto art. 39 lid 1 sub c AVG).
- Het samenwerken met de Autoriteit Persoonsgegevens (art. 39 lid 1 sub d AVG).
- Het optreden als contactpunt voor de Autoriteit Persoonsgegevens (art. 39 lid 1 sub e AVG).
- De functionaris voor gegevensbescherming rapporteert aan het hoogste leidinggevende niveau (art. 38 lid 3 AVG). Binnen een gemeente is dit ambtelijk de secretaris (art. 102 Gemeentewet). Bestuurlijk kan dit verschillen per verwerkingsactiviteit, de Gemeentewet noemt de burgemeester, college van burgemeester en wethouders en de gemeenteraad als bestuursorganen (art. 6 Gemw.).

In de taken van de functionaris voor gegevensbescherming is een tweedeling te maken. Hij is adviseur en toezichthouder. Zo kan het dus ook voorkomen dat de functionaris bij bepaalde onderwerpen advies geeft en op de uiteindelijke uitkomst zelf toezicht moet houden. Hier kan een rollenconflict ontstaan.

Over het toezichthouden wordt verschillend gedacht. Zo schrijven Engelfriet en Chew-Meij (2017, p. 157) dat de functionaris voor gegevensbescherming geen toezichthouder is en geen corrigerende rol heeft. Wel wegen zijn aanbevelingen zwaar bij bepaling of een verwerking rechtmatig is. Vervolgens schrijven ze ook dat de functionaris een zorgplicht heeft om op een professionele en deskundige manier zijn taken te kunnen vervullen. In het bijzonder moet hij op gepaste wijze kunnen informeren en adviseren, toezien op naleving en contact onderhouden met de toezichthouder (Engelfriet en Chew-Meij, 2017, p. 160).

Drewer en Miladinova (2018, p. 812) noemen de functionaris voor gegevensbescherming een 'canary in the data mine'. Iemand die roept als er iets fout gaat. Volgens Drewer en Miladinova (2018, p 812) kan de functionaris voor gegevensbescherming de functie van 'canary in the data mine' alleen goed uitoefenen als die volledig functioneel onafhankelijk is. Dit is ook opgenomen in overweging 97 van de AVG daar staat dat de functionarissen voor gegevensbescherming in staat dienen te zijn hun taken en verplichtingen onafhankelijk te vervullen, ongeacht of ze in dienst zijn van de verwerkingsverantwoordelijke.

2.7.2. Organisatie

Om als functionaris voor gegevensbescherming de taken zoals in voorgaande paragraaf opgenomen goed te kunnen uitoefenen zal de verwerkingsverantwoordelijke, in deze thesis een gemeente van middelgroot formaat, een aantal maatregelen moeten nemen om de functionaris te ondersteunen.

In artikel 38 AVG staan duidelijke instructies opgenomen waar de gemeente zich aan moet houden:

- De functionaris voor gegevensbescherming zal naar behoren en tijdig worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens (art. 38 lid 1 AVG).
- De functionaris voor gegevensbescherming krijgt bij de vervulling van zijn taken toegang tot persoonsgegevens en verwerkingsactiviteiten (art. 38 lid 2 AVG).
- De benodigde middelen voor het vervullen van deze taken en het in standhouden van zijn deskundigheid worden ter beschikking gesteld (art. 38 lid 2 AVG) .
- Er worden geen instructies gegeven met betrekking tot de uitvoering van de taken (art. 38 lid 3 AVG).
- De functionaris voor gegevensbescherming mag door de gemeente niet worden ontslagen of gestraft voor de uitvoering van zijn taken (art. 38 lid 3 AVG).
- Er wordt rechtstreeks verslag uitgebracht aan de hoogste leidinggevende niveau (art. 38 lid 3 AVG).
- Betrokkenen moeten rechtstreeks contact kunnen opnemen met de functionaris voor gegevensbescherming over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van de AVG (art. 38 lid 4 AVG).
- De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken overeenkomstig tot geheimhouding of vertrouwelijkheid gehouden (art. 38 lid 5 AVG).
- Indien de functionaris voor gegevensbescherming andere taken en plichten vervult dan mogen deze niet tot een belangenconflict leiden (art. 38 lid 6 AVG). Dit artikel in de AVG is al nader vormgegeven in jurisprudentie. Er is een uitspraak van de geschillenkamer van de gegevensbeschermingsautoriteit uit België. In casu was de functionaris voor gegevensbescherming ook director audit, risk en compliance. In deze uitspraak is bepaald dat indien de functionaris voor gegevensbescherming het beleid moet controleren dat hij zelf heeft opgesteld, dan wel zelf verantwoordelijk voor is, er onvoldoende mogelijkheid is om onafhankelijk te adviseren (Geschillenkamer Gegevensautoriteit 28 april 2020, AH-2019-0013).

2.7.3. Eisen aan de functionaris voor gegevensbescherming

Aan de functionaris gegevensbescherming worden ook eisen gesteld.

- De functionaris voor gegevensbescherming moet een niveau van deskundigheid hebben. Deskundigheid op het gebied van wet en regelgeving en de praktijk inzake gegevensbescherming (art. 37 lid 5 AVG). WP29 zegt hierover dat het niveau van deskundigheid niet strikt is gedefinieerd maar dit moet in verhouding zijn met de gevoeligheid en complexiteit van de gegevens (Groep gegevensbescherming artikel 29, 2017).
- Een functionaris voor gegevensverwerking wordt aangewezen op grond van zijn professionele kwaliteit (art. 37 lid 5 AVG).
  WP29 heeft deze eisen nader uitgewerkt en schrijft hierover het volgende:
  - De functionarissen voor gegevensbescherming moeten enige ervaring hebben met nationale en Europese wetten en praktijken op het gebied van gegevensbescherming. De WP29 wijst er ook op dat het interessant is als de toezichthoudende autoriteit een gepaste en regelmatige opleiding voor functionarissen voor gegevensbescherming stimuleren (Groep gegevensbescherming artikel 29, 2017).
  - Kennis van de bedrijfstak en organisatie (Groep gegevensbescherming artikel 29, 2017).
  - Voldoende inzicht hebben in de uitgevoerde verwerkingsactiviteiten, de informatiesystemen en de behoeften van de verwerkingsverantwoordelijke op het vlak van gegevensbeveiliging en gegevensbescherming (Groep gegevensbescherming artikel 29, 2017). Engelfriet en Chew-Meij (2017) merken op dat het onduidelijk is hoe hoog deze lat behoort te liggen. Ze achten het wel waarschijnlijk dat deze hoger ligt dan de gewone zorgplicht van de opdrachtnemer (artikel 7:401 BW).
  - Bij een overheidsinstantie, ook gedegen kennis van de administratieve regels en procedures van de organisatie (Groep gegevensbescherming artikel 29, 2017).
- De functionaris voor gegevensbescherming moet het vermogen hebben om zijn taken te vervullen (art. 37 lid 5 AVG).
  - Het gaat hier om persoonlijke vaardigheden en kennis (Groep gegevensbescherming artikel 29, 2017).
  - Ook van belang is de positie binnen de organisatie (Groep gegevensbescherming artikel 29, 2017).

Ondanks dat de functionaris voor gegevensbescherming reeds voor de implementatie van de AVG al bestond, is het toch een relatief nieuwe discipline en de weinige privacycertificeringen die er momenteel zijn, zijn vrij onvolwassen (Ross, 2018).

WP29 vermeldt nog nadrukkelijk dat indien er sprake is van een externe functionaris voor gegevensbescherming, op basis van een dienstverleningsovereenkomst het van essentieel belang is dat aan alle eisen van afdeling 4 van de AVG voldaan moet worden. Zo is het van essentieel belang dat er geen belangenconflicten zijn. Ook mag er geen sprake zijn van oneerlijke beëindiging van de

dienstverleningsovereenkomst voor activiteiten als functionaris gegevensbescherming (Groep gegevensbescherming artikel 29, 2017).

Naast de wet en de nadere invulling door WP29 is er geen nadere (academische) literatuur aanwezig over de functionaris voor gegevensbescherming, zijn positie in de organisatie en zijn taakuitoefening.

2.8. Model

Uit de regelgeving en nadere uitwerking door Groep gegevensbescherming artikel 29 is een overzicht met uitgangspunten opgesteld. Dit model, figuur 1, is opgesteld volgens het in paragraaf 1.2.1. geformuleerde drieluik. Het vormt de basis voor het kwalitatieve onderzoek en zal nader worden aangevuld vanuit het veldonderzoek. De blauwe blokken zijn uitgangspunten afkomstig zijn uit de regelgeving. De lichter gekleurde blokken zijn nadere aanvullingen van de Groep gegevensbescherming artikel 29.

Figuur 1. Conceptueel model op basis van regelgeving.

3. ONDERZOEKSONTWERP EN DATAVERZAMELING

3.1. Inleiding

De methode van onderzoek en de wijze waarop de dataverzameling heeft plaatsgevonden zal in dit hoofdstuk worden toegelicht.

3.2. Onderzoeksdesign

Voor de aanpak van het onderzoek is gekozen voor een deductieve onderzoeksaanpak. Bij deductief onderzoek formuleert de onderzoeker verwachtingen aan de hand van (bestaande) theorieën en modellen. Er worden gegevens verzamelt en geanalyseerd om na te gaan of deze theorieën standhouden (Verhoeven, 2018). In deze thesis is eerst het theoretisch kader vormgegeven. Vanuit deze theorie is een model gevormd, figuur 1. Dit model is de basis voor de vormgeving van de interviews. Met de gegevens die vanuit het veldonderzoek zijn opgehaald is bekeken of het model aanpassing nodig had en is het model aangevuld. De vraag of dit model juist was opgesteld, juist op basis van de regelgeving, is in de interviews niet nagegaan. Na de eerste interviews bleek dit een te diepgaande vraag. Dit zou veel voorbereiding van respondenten verlangen. De interviews zijn vervolgens zo ingericht om informatie op te halen om het opgestelde model aan te vullen. Omdat het model de basis was voor de interviews en uit de interviews niet naar voren kwam dat de onderwerpen die ter sprake kwamen onjuist of niet van toepassing zijn op de functievervulling van de functionaris voor gegevensbescherming kan impliciet gesproken worden over toetsing van het model.

Omdat er al theorie en wetgeving over dit onderwerp aanwezig is past deze wijze van deductief onderzoek bij de in deze thesis geformuleerde doelstelling en onderzoeksvraag waarbij getoetst wordt of de theorie in de praktijk standhoudt.

Het in dit hoofdstuk omschreven onderzoek en werkwijze is goedgekeurd door de ethische commissie van de universiteit Twente.

3.2.1. Kwalitatief onderzoek

De opzet van het veldonderzoek betreft dataverzameling op basis van kwalitatief onderzoek.

Boeije (2016) geeft de volgende definitie van kwalitatief onderzoek: ’In kwalitatief onderzoek richt de vraagstelling zich op onderwerpen die te maken hebben met de wijze waarop mensen betekenis geven aan hun sociale omgeving en hoe ze zich op basis daarvan gedragen. Er worden onderzoeksmethoden gebruikt die het mogelijk maken om het onderwerp vanuit het perspectief van de onderzochte mensen te leren kennen met het doel om het te beschrijven en waar mogelijk te verklaren’.

De onderzoeksactiviteiten betreffen het houden van interviews. Er is gekozen voor deze wijze van kwalitatief onderzoek om zo de persoonlijke mening, persoonlijke beleving, en achterliggende meningen van mensen te achterhalen. Een onderzoeksmethode die valide is bij de gestelde onderzoeksvraag.

Om goed het model te kunnen aanvullen vanuit de praktijk is gekozen voor een gestructureerd interview waarbij gewerkt is met een vooraf opgestelde vragenlijst (bijlage C).
De geïnterviewde is voorafgaand aan het interview een document toegezonden (bijlage B) met hierin aangegeven het soort vragen en het model. Het vragenschema is door de onderzoeker tijdens het interview als leidraad gebruikt.

3.2.2. Selectie respondenten

Per 1 januari 2020 telde Nederland 355 gemeenten. Voor dit onderzoek is gekozen voor de middelgrote gemeente. Voor de definitie van een middelgrote gemeente is aangesloten bij de definitie van het stedennetwerk G40. Het G40-stedennetwerk is het netwerk van 40 middelgrote steden in ons land, die elkaar vinden in de stedelijke vraagstukken waar de leden van het netwerk voor staan. Het betreft een groep die met dezelfde stedelijke vraagstukken te maken hebben en hierdoor op elkaar lijken. De inwonersaantallen van deze gemeente variëren van 67.760 inwoners van de gemeente Assen tot 234.394 inwoners in Eindhoven.

Als respondenten is gekozen voor de functionaris voor gegevensbescherming van de G40 gemeenten. Dit omdat het te toetsen model de functionaris voor gegevensbescherming zelf betreft is deze functionaris de aangewezen persoon om het interview op af te nemen.

Om niet de gehele populatie van 40 gemeenten te interviewen is er een steekproef getrokken. Er is gekozen om van deze 40 gemeenten er 12 te selecteren voor een interview. Er is een enkelvoudige aselecte steekproef getrokken. Zo heeft elke gemeente evenveel kans om in de onderzoeksgroep terecht te komen. Dit is gedaan door alle gemeenten in een Excel-lijst op te nemen in volgorde van inwoneraantal. Aan die lijst is een tabel toegevoegd waarbij gebruik is gemaakt van de random generator die de gemeenten nummert. Er is een kolom met de Syntax: *ASELECT()* aan de lijst met gemeenten toegevoegd waardoor de gemeenten willekeurig geordend zijn. Deze nieuwe lijst, waarbij de gemeenten in een random volgorde staan, is gebruikt voor de benadering. Van de bovenkant van de lijst is gestart met het benaderen van de betreffende functionaris van gegevensbescherming.

Met deze steekproef die 30% van de gehele populatie omvat kan een uitspraak gedaan worden over de gehele populatie. Een valide aantal dat past bij deze totale groep. Dit werd ook bevestigd doordat er in de interviews op een gegeven moment verzadiging ontstond. Bij de afname van de laatste interviews werd er nog maar weinig nieuwe informatie meer verkregen over het onderwerp.

Volgens de AVG moet elke gemeente op zijn website de gegevens bekendmaken over hoe de functionaris voor gegevensbescherming te benaderen is. Dit is bij elke gemeente nagegaan en dit betrof een e-mailadres of een webformulier. Naar dit adres is het verzoek tot deelname, bijlage A, verzonden.

Er zijn in totaal 20 gemeenten benaderd. Hiervan hebben er twaalf volledige medewerking verleend, deze zijn opgenomen in tabel 1. Het interview is twee keer per telefoon afgenomen en tien keer middels Microsoft teams. Van de niet-deelnemende gemeente hebben een aantal niet gereageerd op het verzoek tot deelname, een aantal gaven aan dat ze niet wilden meewerken vanwege verschillende redenen en een deelnemer heeft zich na afname van het interview teruggetrokken.

Tabel 1:

Deelnemende gemeenten	
Almelo	Haarlemmermeer
Apeldoorn	Hoorn
Breda	Leiden
Delft	Schiedam
Dordrecht	Zaanstad
Groningen	Zwolle

3.2.3. Verwerking data & anonimiteit

Van het interview is een bandopname gemaakt. Deze opname is gebruikt om het interview te transcriberen. Er is zoveel mogelijk woordelijk getranscribeerd, waarbij zoveel mogelijk is opgeschreven wat er door de respondent is gezegd maar stopwoorden, aarzelingen zijn genegeerd. Ook is er interpunctie voor de leesbaarheid toegevoegd. Dit transcript is aan de respondenten toegezonden ter goedkeuring en instemming voor gebruik. Na de ontvangen goedkeuring is de bandopname gewist.

Van alle correspondentie met respondenten is een audit trail bijgehouden.

Voor het onderzoek is het niet relevant om te weten welke respondent bij welke gemeente werkzaam is. In het audit trail zijn de geïnterviewde gemeenten genummerd. Een nummering van 1 tot en met 12 is gebruikt om de gemeenten te anonimiseren. Deze nummering is gebruikt bij de citaten in hoofdstuk 4. De nummering komt niet overeen met de volgorde zoals de deelnemende gemeenten zijn opgenomen in tabel 1.

De registratie van de verzamelde gegevens betreft in eerste instantie de transcripten van de interviews. In deze transcripten is al een structuur aangebracht door de onderwerpen te groeperen, er is aangesloten bij de onderwerpen uit de literatuur en figuur 1.

3.2.4. Coderen

Doordat er gebruik is gemaakt van een gestructureerd interview met een leidraad, zijn de transcripten al per onderwerp ingedeeld. Voor de vervolgverwerking is gebruik gemaakt van het softwareprogramma Excel. Hierin is een tabel opgesteld die is gebruikt voor de statistische analyse. Er is gestart met het uiteenrafelen van de gegevens. Als eerste een aantal algemene gegevens over de geïnterviewde, zoals achtergrond en werkervaring. Vervolgens is de indeling van figuur 1 is gehanteerd en per, ‘taken’, ‘organisatie’ en ‘eisen aan functionaris’ gestructureerd. Als code zijn er vanuit de transcripten korte tekstuele omschrijvingen in het Excel document opgenomen zodat het mogelijk is om de analyse uit te voeren en relaties, structuren en verbanden te leggen.

Zoals Boeije (2012) het omschrijft is er sprake van open coderen. Alle verzamelde gegevens zijn zeer zorgvuldig gelezen en in fragmenten gelabeld en onderling vergeleken. Het resultaat van deze wijze van coderen is een groot geordend bestand. De structuur van de interviews is hierbij aangehouden.

Uit de codering en de transcripties is te achterhalen welke uitspraken door welke respondent zijn gedaan. Dit komt mede doordat bij de meeste gemeenten slechts één functionaris voor gegevensbescherming werkzaam is. Om anonimiteit van de deelnemers te garanderen zijn de codering en transcripten niet als bijlagen bij deze thesis gevoegd.

3.2.5. Beperkingen van het onderzoek

De beperking van woordelijk transcriberen is dat bij deze wijze van verslaglegging er informatie verloren kan gaan over de wijze waarop iemand iets zegt, lichaamstaal en intonatie verdwijnt. Voor dit onderwerp worden deze emoties niet als heel belangrijk gevonden.

De interviewer moet tijdens de afname van het interview objectiviteit nastreven. Om deze objectiviteit zoveel mogelijk te waarborgen is gebruik gemaakt van standaardisatie door gebruik te maken van de opgestelde vragenlijst en de bandopname. Door gebruik te maken van de vragenlijst wordt ook voorkomen dat het interview wordt overgenomen door de geïnterviewde. Omdat de onderzoeker een collega functionaris voor gegevensbescherming is bleek de bereidheid om mee te werken groot. Je helpt een collega. Hier zit ook een beperking in. De onderzoeker kan de geïnterviewde dus ook iets brengen. De geïnterviewde is mogelijk zelf ook op zoek naar informatie. Het gedrag van de geïnterviewde zou hiervoor beïnvloed kunnen worden. Een risico waar Schindler (2019) ook voor waarschuwt. Tijdens de afname van de interviews heeft dit zich ook een aantal keer voortgedaan. Hierop is geacteerd door voorafgaand heel duidelijk te maken wat het doel van het interview was en dat dit volgens een bepaalde structuur zou verlopen. Daar waar er wel door de onderzoeker informatie is gegeven, was dit soms voor het gesprek nodig en ook mogelijk, is dit altijd gedaan nadat de geïnterviewde zijn antwoord al had gegeven of na afsluiting van het interview. Dit zodat de antwoorden van geïnterviewde zo min mogelijk beïnvloed zouden worden.

De geïnterviewden zelf vormen een mogelijke beperking van het onderzoek. Volgens Schindler (2019) zijn er zeven risico's waar gewaakt voor moet worden bij de respondenten namelijk, gebrek aan kennis, verkeerde interpretatie van de informatie, verkeerde interpretatie, incomplete deelname, weigering van deelname, vooringenomenheid en dat er sociaal wenselijke antwoorden worden gegeven. Er is niet gebleken dat een van de punten zich heeft voortgedaan. Alle geïnterviewde hadden voldoende kennis en er is geen blijk gegeven dat er informatie verkeerd is geïnterpreteerd. De deelnamen waren volledig.

Bij de selectie van partijen is het voorgekomen dat benaderde functionarissen voor gegevensbescherming niet wilden meewerken, of niet reageerden op het verzoek. Omdat het een steekproef betrof is vervolgens de eerst volgende op aselecte lijst benaderd. Dit totdat er voldoende respons was en data om een analyse te starten. Vooringenomenheid of het geven van sociaal wenselijke antwoorden is door de onderzoeker niet geconstateerd.

4. ANALYSE, RESULTATEN EN AANVULLINGEN MODEL

4.1. Inleiding

In dit hoofdstuk worden de resultaten van de interviews weergegeven. Om een beeld van het gehele spectrum te scheppen zal als eerste in worden gegaan op de respondenten, de organisatie waar ze werken, de werkzaamheden die ze uitvoeren en de positionering in de organisatie.

Vervolgens zal aan de hand van de indeling van figuur 1 worden ingegaan op de taken van de functionaris voor gegevensbescherming, de organisatie en de eisen die gesteld worden aan de functionaris. Daar waar er relaties zijn te leggen met de onderzochte literatuur, zoals opgenomen in hoofdstuk 2, zal dit direct worden weergegeven.

Tijdens de interviews zijn er door respondenten diverse aanbevelingen gedaan. De analyse is dan ook niet los te zien van de aanbevelingen. Boeije (2012) schrijft dat bij kwalitatief onderzoek een strikte scheiding tussen analyse en aanbevelingen moeilijk te maken is. Daar waar de aanbevelingen een nadere aanvulling zijn op het theoretische model, figuur 1, zijn deze direct opgenomen onder het kopje 'aanvulling model'. De betreffende aanbeveling is voorzien van een onderbouwing waarom het een aanvulling op het model is. Alle aanvullingen die uit de analyse voortkomen betreffen geen wettelijke vereisten maar hulpmiddelen die ter ondersteuning zijn aan de middelgrote gemeente en de functionaris voor gegevensbescherming. Het gaat om aanvullingen die een middelgrote gemeente helpen bij de positionering van de functionaris voor gegevensbescherming in de organisatie of de functionaris zelf van hulp kan zijn bij de uitvoering van zijn taken.

Om een compleet beeld van de interviews weer te geven wordt gebruik gemaakt van citaten. Het gaat hier om de preservationist-benadering, waarbij de oorspronkelijke weergave van de opname zo letterlijk mogelijk wordt weergegeven. Citaten kunnen volgens Boeije (2012) voor meerdere redenen gebruikt worden. In deze thesis zijn de citaten ter onderbouwing van het verhaal, om de lezer meer invulling te geven zodat die het idee heeft hoe de interviews zijn verlopen en om de tekst te verlevendigen.

In de analyse wordt meer dan voorafgaand gebruik gemaakt van afkortingen. Met name de functionaris voor gegevensbescherming wordt afgekort als FG. Dit is gedaan om meer aan te sluiten bij het taalgebruik van de interviews waarin veelal de afkortingen zijn gebruikt.

4.2. De respondenten

Bijna alle geïnterviewden zijn tussen de één en drie jaar actief in de functie van functionaris voor gegevensbescherming. Dit is niet zo vreemd aangezien gemeenten de AVG, met hierin de verplichte FG-functie uiterlijk per 25 mei 2018 geïmplementeerd moesten hebben. Een geïnterviewde werkte bij de gemeente in de functie van FG al ruim voor de implementatie van de AVG. De meeste respondenten hebben voorafgaand aan de functie van functionaris voor gegevensbescherming een lange staat van dienst binnen de gemeentelijke organisatie. Een aantal hadden voorafgaand aan de functie al veel met privacy te maken of met een onderwerp zoals informatietechnologie waarbij privacy een grote rol speelt. Een respondent heeft met de opkomst van het onderwerp privacy en de AVG juist een keuze gemaakt om vanuit het consultancyvak naar een gemeente over te stappen.

Van de twaalf respondenten zijn er tien in dienst van de gemeente. Twee zijn extern en worden ingehuurd. Zij hebben naast de werkzaamheden als functionaris voor gegevensbescherming andere werkzaamheden maar niet bij de gemeente waar ze worden ingehuurd als FG. Van de interne functionarissen is het merendeel voor al zijn arbeidsuren werkzaam als FG. Er is één gemeente die bewust de keuze heeft gemaakt om twee FG's te benoemen, beide voor 50% van de werkzame uren. Zoals verder in deze analyse zal blijken kan dit een goede oplossing zijn bij de waarborging van de onafhankelijke rol van de FG in gevallen waar de FG's veel inhoudelijk advies heeft gegeven. Er is ook één gemeente die de vervanging van de FG bij de CISO heeft neergelegd. Vervanging van de FG, ook ten tijde van vakantie van de FG, is nog niet bij elke gemeente goed ingeregeld.

De achtergrond van de functionarissen voor gegevensbescherming is divers. Zij studeerden onder andere rechten, ICT, bedrijfskunde, bedrijfseconomie, communicatie, bestuurskunde etc. In het werkzame leven zijn de respondenten in aanraken met het vakgebied privacy en gegevensbescherming gekomen en er zo ingerold. Alle respondenten zijn al langer actief op de arbeidsmarkt.

Aanvulling model

Het niet hebben van een vervanger kan problemen opleveren. Zeker in gevallen dat een FG al veel aan de voorkant van een proces als adviseur betrokken is geweest. Het vervolgens toezichthouden op het eigen advies wordt dan lastig. Uit het veldonderzoek is naar voren gekomen dat dit met name bij DPIA's nog wel eens gebeurd. De FG's treden bij de DPIA op als procesbegeleider en moeten vervolgens een onafhankelijk oordeel geven. Als er binnen de organisatie een vervanger aanwezig is kan er een taakverdeling gemaakt worden. De vervanger kan dan de rol van toezichthouder op zich nemen. Daarnaast is uit het veldonderzoek gebleken dat niet elke FG een vervanger heeft ten tijde van afwezigheid. Vragen van burgers, het eigen personeel en de AP blijven dan liggen. Voorgaande is een reden om als aanvulling op het model '*Vervanging*' op te nemen in het onderdeel '*Eisen aan functionaris/positie in organisatie*'. Dit is een aanvulling die de organisatie helpt zijn FG te positioneren.

4.3. Organisatie en privacylandschap

Alle deelnemende gemeenten hebben een platte organisatiestructuur waarbij de verantwoordelijkheden daar liggen waar het werk wordt uitgevoerd. Er is veelal sprake van een diensten/directiemodel waarbij er een directie is, vervolgens een laag met afdelingen en in een aantal gevallen daaronder nog een laag met teams. Een aantal gemeenten werken met programmamanagers voor de aansturing van grote gemeentelijke ontwikkelingen, het in paragraaf 2.2.1. benoemde opgavegericht werken. Bij elke deelnemende gemeente ligt de verantwoordelijkheid voor de juiste uitvoering van het verwerken van persoonsgegevens op basis van de AVG op afdelingsniveau. In laag 1 van de three lines of defence zoals omschreven in paragraaf 2.2.1. Respondenten hebben het over 'verantwoordelijkheden liggen laag in de organisatie' of een 'platte structuur'.

Alle deelnemende gemeenten zijn op het gebied van privacy en gegevensbescherming nog aan het bouwen. Veelal is de basisinrichting aanwezig en zit de gemeente in de fase van het verder vormgeven. Op accenten, die voor dit onderzoek niet relevant zijn, zijn er verschillen. Doordat er nog veel gebouwd wordt

op het gebied van gegevensbescherming zijn veel FG's voornamelijk met hun adviestaak bezig. Er zijn gemeenten die bij de werving van de FG gekeken hebben naar de competenties van de FG en de fase waarin de gemeente zich op het gebied van gegevensbescherming bevindt en hier een passende FG bij hebben gezocht. Zo is er een respondent die is aangetrokken omdat het een echte verbinder is. De betreffende gemeente heeft daar op dit moment behoefte aan.

De meeste organisaties hebben een privacy officer (PO-er) die eerste of tweedelijns advies geeft. Daarnaast hebben veel gemeenten ook op de afdelingen zelf medewerkers geschoold die een eerste inschatting/beoordeling op het gebied van privacy en gegevensbescherming kunnen maken.

Een aantal FG's zijn helemaal alleen. Zij hebben geen privacy officer of privacy geschoolde medewerkers op de afdelingen. Bij deze functionarissen zie je dat ze veel aan de voorkant van het proces in de adviesrol zitten. Deze FG's die er alleen voor staan, en deze werken in 100.000 plus gemeenten, zijn actief op het gebied van risico gedreven toezicht.

> *Een FG is natuurlijk ook adviseur. Je helpt de organisatie meer door actief gebruik te maken van de adviesrol, dit is toezicht aan de voorkant. Als je aan de voorkant meedenkt of meegeeft waaraan gedacht moet worden dat voorkomt aan de achterkant dat je met je vinger moet wijzen. (Respondent 10, p. 2)*

Een aantal gemeenten dragen actief de tree lines of defence uit. Waarbij de eerste lijn de verantwoordelijke afdeling is. De afdeling zelf is soms in staat om bij privacyvraagstukken een eerste afweging te maken. De tweede lijn is de privacy officer, en bij een aantal gemeenten de FG, die advies geeft en inhoudelijk meewerkt en meedenkt. Vervolgens is er de derde lijn, de FG. Deze lijn opereert meer op strategisch niveau, hier wordt de adviestaak op strategisch niveau ingevuld en toezicht gehouden. Er zijn een aantal gemeenten die ook op deze wijze werken maar dit niet heel duidelijk kenbaar maken. Bij deze gemeenten komt het nog wel eens voor dat de verantwoordelijke afdeling/integraal manager zich niet verantwoordelijk voelt voor het gehele product dat hij moet afleveren. Een product dat moet voldoen aan de AVG en een goede gegevensbescherming aan de burger biedt. Zij kijken voor die verantwoordelijkheid naar de privacy officer of functionaris voor gegevensbescherming, die zijn van privacy en moeten zorgen voor een goede gegevensbescherming.

<u>Aanvulling model</u>

Misverstanden over de (eigen)verantwoordelijkheid ontstaan bij een onduidelijke taakverdeling en onbekendheid over de eigen verantwoordelijkheid. Duidelijkheid omtrent verantwoordelijkheden van de ambtenaar, afdelingsmanager en de FG kan zorgen voor betere samenwerking en heeft tot gevolg een betere wijze van gegevensbescherming. Het vastleggen en uitdragen van deze verantwoordelijkheden helpt hierbij. Een mogelijke plek hiervoor is de organisatieregeling/verordening of het privacybeleid. Als aanvulling op het model in het onderdeel '*Taken/Informeren & Adviseren'* wordt opgenomen '*Verantwoordelijkheid*'. Dit is een aanvulling die de organisatie helpt zijn FG te positioneren.

4.3.1. Positionering

De respondenten zijn binnen de gemeentelijke organisaties op verschillende afdelingen gehuisvest. Het merendeel is op een afdeling gepositioneerd waaruit hun onafhankelijke positie goed blijkt, zoals een afdeling control, audit & onderzoek of bij de (directie)staf. Er zijn ook functionarissen die bij de afdeling juridische zaken of ICT zijn ondergebracht. Hoewel de respondenten hier geen problemen in de uitvoering van de werkzaamheden ervaren, is het wel eens voorgekomen dat de onafhankelijke positie van de functionaris niet werd herkend. Ook is door een respondent aangegeven dat een afdeling juridische zaken vaak aan het einde van het proces zit. Hierdoor wordt ook het onderwerp gegevensbescherming pas laat opgemerkt. Net als bij andere adviseurs zitten binnen gemeenten de eerstelijns juristen vaak op de vakafdeling zelf. De juridische afdeling vervult een tweedelijns adviesfunctie, die niet direct bij de opstart van projecten en werkzaamheden wordt betrokken. Dit geldt ook voor de afdeling ICT, die wordt ook niet direct bij vakafdelingsprojecten betrokken, pas als er een ICT component aan zit. Door plaatsing FG op deze afdelingen wordt ervaren dat betrokkenheid pas laat in het proces plaatsvindt.

> *Er is me wel eens gevraagd om mijn advies aan te passen omdat je integraal adviseert aan het college. Toen heb ik uitgelegd dat dit niet werkt voor de FG. Dit betrof meer onwetendheid en onbekendheid met mijn onafhankelijke rol. Ze stapte naar mijn manager, met het verzoek om het advies aan te passen. Toen zijn we wel in gesprek gegaan. Mogelijk dat een andere positionering hierbij zou kunnen helpen. (Respondent 10, p. 6)*

<u>Aanvulling model</u>

Geconcludeerd kan worden dat plaatsing van een functionaris voor gegevensbescherming bij een control of stafafdeling er voor zorgt dat het onderwerp gegevensbescherming meer als een gemeentebrede verantwoordelijkheid wordt gezien dan van een afdeling (zoals juridische zaken of ICT). Onder *'Eisen aan functionaris/Positie in de organisatie'* wordt als aanvulling op het model gemaakt de plaatsing bij '*Staf/control'.* Dit is een aanvulling die de organisatie helpt zijn FG te positioneren.

4.3.2. Werkzaamheden

> *Privacy is niet sexy noem ik het wel eens. Het is leuker om te zeggen dat we gaan verbouwen, we gaan vernieuwen, we hebben een mooi stadspark en verzin het allemaal maar, als dat we zeggen 'heb je er wel eens over nagedacht dat we veilig, vertrouwd en verantwoord moeten werken met de persoonsgegevens die we hebben', dat is lastig, dat is niet leuk. (Respondent 1, p. 2)*

De werkzaamheden van de respondenten in de rol van FG is heel divers. Een aantal functionarissen voeren veel werkzaamheden zelf uit zoals het afhandelen van klachten, afhandelen van datalekken en het bijhouden van het verwerkingsregister. Anderen hebben dit soort werkzaamheden binnen de organisatie belegd en pakken de afdelingen het zelf op of voert de privacy officer ze uit (eerste of tweede lijn). De FG is dan echt de derde lijn die toezicht houdt en vanuit een toezichthoudend kader adviseur is.

Een groot gedeelte van de werkzaamheden van de FG vindt plaats door de gehele organisatie en op alle niveaus. Van het geven van trainingen aan (nieuwe) medewerkers, gevraagd en ongevraagd advies geven, reageren op actualiteiten en het uitvoeren of toetsen van Data Protection Impact Assessments (DPIA's).

> *Heel veel in gesprek zijn met de organisatie, de afdelingen, de vraagstukken die daar liggen. Ik ben niet de politieman die als toezichthouder door de organisatie gaat. Af en toe moet ik streng zijn, maar eigenlijk ben ik voortdurend bezig met mee te denken om oplossingen te vinden voor een privacyvraagstuk. (Respondent 12, p. 1)*

Veel genoemde samenwerkingspartners zijn de privacy officers, de Chief Information Security Officer (CISO) en de concerncontroller. Vaak wordt er samen met de CISO opgetrokken, dit omdat informatiebeveiligingsvraagstukken en privacyvraagstukken vaak gelijktijdig spelen. Een aantal respondenten geven aan dat de CISO binnen hun gemeente niet op dezelfde afdeling als de FG is geplaatst maar dat dit wel wenselijk zou zijn.

Een respondent maakt heel actief gebruik van de 'plan-do-check-act-cyclus' om te zorgen dat privacy continue op de afdelingen bij de primair verantwoordelijke aanwezig is.

Een andere respondent zoekt voor de uitvoering van de toezichthoudende en controlerende taken aansluiting bij het in de gemeente aanwezige team Verbijzonderde Interne Controle (VIC). Een cyclus waaraan de gemeente al gewend is.

Aanvulling model:

Uit de analyse blijkt dat samenwerking de FG helpt in de uitvoering van zijn taken. Een aanvulling op het model in het onderdeel *'Taken/Toezien op de naleving van Regelgeving'* is om *'Samenwerkingen'* vorm te geven. Dit is een aanvulling op het model dat de FG van hulp kan zijn bij de uitvoering van zijn taken.

4.3.3. Toezicht en advies

Een aantal functionarissen voor gegevensbescherming richten zich met name op de toezichthoudende taak. Dit is een bewuste keuze van de betreffende gemeente. De betreffende organisatie is er ook op ingericht dat dit mogelijk is. De werkzaamheden van deze toezichthoudende FG's bestaan uit het stellen van kritische vragen, beoordelen van DPIA's, ze hebben contacten met directeuren en geven advies vanuit een toezichthoudend kader. De organisatie zelf wordt inhoudelijk bijgestaan door privacy officers of privacycoördinatoren. Die houden zich bezig met het inhoudelijke advies op het gebied van privacy, zij spelen mee in het veld. De adviestaak van deze toezichthoudende functionarissen omvat het uitbrengen van verslagen aan het bestuur en organisatie met verbeterpunten. Die verbeterpunten moet de organisatie dan zelf oppakken.

Deze toezichthoudende FG's voldoen aan alle vier de kenmerken van een toezichthouder zoals door Ruimschotel (2014) is geformuleerd en in paragraaf 2.3. is opgenomen. Zij staan aan de zijlijn en spelen

niet mee in het veld (1). Ze hebben een cluster activiteiten met componenten als beschermen, waken en zorgen (2). Hun toezicht is conserverend en creëert niet (3) en het houdt altijd iets normerends is (4).

Daarnaast zijn er functionarissen voor gegevensbescherming die, zoals Ruimschotel (2014) het noemt, meespelen in het veld. Soms is dat ingegeven doordat ze het zonder ondersteuning moeten doen. Maar in de meeste gevallen is er wel ondersteuning in de vorm van een privacy officer en gaat het meer om een andere taakinvulling. Zij wijzen erop dat in de regelgeving de adviestaak, aan de voorkant/in het veld, ook is opgenomen.

Een van de FG's die alles zelf moet doen heeft hier wel moeite mee. Doordat deze FG helemaal alleen is wordt die in de operationele rol getrokken. Deze FG is zelf actief in het begeleiden van DPIA's en opstellen van verwerkersovereenkomsten. Wel vindt deze FG aanwezig zijn aan de voorkant belangrijk. Wat het nog complexer maakt is dat er geen vervanger in de betreffende gemeente aanwezig is die bij grote betrokkenheid van de FG op de inhoud de toetsende en controlerende pet kan oppakken.

> *Ik vind dat ik meer aan toezicht moet doen. Maar ik kan alleen goed toezicht houden als ik ook de adviserende rol oppak. Ik vind het heel belangrijk dat mensen mij weten te vinden en benaderen en het gevoel hebben 'ik heb iets aan die FG'. En niet iemand die je achteraf alleen maar op je vingers tikt. En dat bereik je juist door mee te denken en adviezen te geven. (Respondent 8, p.2)*

Een andere gemeente waar de FG ook meespeelt op het veld en erg aan de voorkant van het proces betrokken is heeft dit heel praktisch opgelost. Bij deze gemeenten werken twee FG's. Daar waar de ene FG inhoudelijk betrokken is neemt de andere FG de toetsende rol op zich. Zeker in processen als DPIA's kan dit heel handig zijn. Het proces wordt dat zorgvuldig doorlopen doordat tijdens het opstellen van de DPIA er privacyadvies wordt gegeven. En vervolgens kan de andere FG een toetsend advies op de DPIA geven.

4.3.4. Rollenconflict

Geen enkele FG ervaart een conflict in rollen bij de uitvoering van de advies- en toezichtstaken. De rol van FG met beide taken wordt wel verschillend ingevuld. Eén FG spreekt heel nadrukkelijk over de adviestaak en dat het advies stopt daar waar de uitvoering begint. Daar wordt duidelijk uitgesproken dat de verantwoordelijkheid ligt bij de proceseigenaren. Een van de respondenten noemt zichzelf in de basis een toezichthouder maar wel eentje met een advies en hulprol. Een andere respondent spreekt over het geven van advies vanuit een toezichthoudend kader. Er is bij de FG's een groot bewustzijn van beide rollen en hoe hier invulling aan te geven.

> *Ik ben aan de voorkant betrokken. Ik weet wat er speelt, al aan de voorkant. Waar ik dan ook gevraagd of ongevraagd ga adviseren. Dit kan zich ontwikkelen tot een punt, dat je er over het grote geheel iets van moet vinden en dan heb je in het proces je bouwstenen al gelegd. Is dat erg, is de vraag. Je komt altijd tegen dat je je invloed uitoefent op wat je moet beoordelen. Ik voel op dit moment niet zoveel conflict. Dit is een werkbare vorm. (Respondent 7, p. 7)*

Een aantal FG's geven aan dat de organisatie nog erg aan het bouwen is op het gebied van privacy. Hierdoor is het nog niet mogelijk om de toezichthoudende rol volledig uit te voeren. Zij willen wel naast het veld staan maar worden nog vaak gevraagd om op het veld mee te spelen. Dit wordt niet als een probleem ervaren maar als een ontwikkeling die de gemeente doorgaat. Zij werken en bouwen mee aan de organisatie om in een later stadium wel die meer toezichthoudende rol op zich te nemen. De AVG is nog niet lang van kracht en verbeteringen binnen de organisatie worden uitgevoerd. Het is meer in de trant van Rome is ook niet in een dag gebouwd, zo is het ook bij het opzetten van een geheel privacyhuis binnen een gemeentelijke organisatie.

> *Ik heb daar nog nooit een conflict mee gehad. Ik vind het buitengewoon passen dat je een stok achter de deur hebt. Dat zit in twee dingen, als eerste heb je de taak, er wordt van jou verwacht dat je toezicht houdt. Af en toe moet je bij een afdeling vragen, als je je zorgen maakt, van hoe zit dit? En als je geen bevredigend antwoord krijgt, dat is dan het tweede ding, de positie die je hebt. Dus als het mij niet bevalt dan kan ik naar de gemeentesecretaris, als het moet zelfs de burgemeester (als portefeuillehouder) maar dat zal bijna nooit gebeuren. Maar wel naar de secretaris en daar dan aandacht vragen. En dan kan je zien wat er vanuit de verantwoordelijkheid die iedereen zelf heeft gaat gebeuren. Dat betekent niet dat je altijd je zin krijgt, maar wel dat je een vraagstuk heel helder maakt vanuit de risicoblik. Of er op die manier voor kunt zorgen dat het probleem op een goede manier wordt opgelost, dat men zich meer voegt naar wat de wetgever heeft beoogd of anderszins dat er gewerkt wordt met risico-acceptatie, dat is ook mogelijk. Uiteindelijk ben ik niet verantwoordelijk en zijn een directeur en gemeentesecretaris verantwoordelijk. Als die zeggen 'we horen jou en zien dat dit problematisch kan zijn gezien de wetgeving maar we accepteren het risico', dan is het ook goed. (Respondent 12, p.2)*

Een van de FG's gebruikt het borgingsdocument van de Vereniging van Nederlandse Gemeenten (VNG) als toezichtskader. Dit is een door VNG opgesteld instrument met handvatten om een goede omgang met persoonsgegevens binnen de gehele gemeente te waarborgen. De gemeente kan met behulp van dit document een ambitieniveau bepalen en laten vaststellen. Dit document helpt de FG in zijn rol en (ongevraagde) advisering. Andere FG's hebben dit document niet genoemd, of dit onbekendheid is of het hun niet behulpzaam is is niet achterhaald. Wel zijn veel FG's nog zoekend naar de invulling van de toezichthoudende taak.

<u>Aanvulling model:</u>
Uit de interviews komt naar voren dat het uitvoeren van de toezichthoudende taak nog niet overal volledig is vorm gegeven en dat FG's nog zoeken naar nadere invulling hiervan. Een hulpmiddel dat uit de interviews naar voren kwam en andere FG's kan helpen bij de invulling van het toezichtskader is het borgingsdocument AVG van de VNG.
Een aanvulling op het model in het onderdeel *'Taken/Toezien op naleving van regelgeving'* is dan ook om het *'Borgingsmodel VNG'* op te nemen. Dit is een aanvulling op het model dat de FG van hulp kan zijn bij de uitvoering van zijn taken.

4.4. Taken van de functionaris voor gegevensbescherming

4.4.1. Informeren en adviseren

Voorgaande paragraaf leidt tot de vraag of de respondenten zich meer adviseur of toezichthouder voelen. Het antwoord is verdeeld. Ongeveer de helft van de respondenten vindt zichzelf echt een adviseur. Een aantal adviseur en toezichthouder, maar met een nadruk op adviseur. Dit is vaak ingegeven door de fase waarin de betreffende gemeente zich momenteel bevindt. Zo geeft een van de respondenten aan dat die zich echt een toezichthouder voelt maar in de praktijk meer een adviseur is. De adviesrol aan de voorkant wordt ook wel omschreven als 'toezicht aan de voorkant'.

Er zijn drie respondenten die zichzelf echt als toezichthouder zien. Een hiervan geeft aan dat er in de praktijk ook veel inhoudelijk advies wordt gegeven en niet vanuit een toezichthoudend kader. De andere twee zijn de FG's waarbij de organisatie ook nadrukkelijk zo is ingericht dat ze toezichthouder zijn.

> *Ik kom te weinig aan toezichthouden toe. Ik ben een toezichthouder maar daar kom ik te sporadisch aan toe. Ik ben te veel adviseur. Een FG is natuurlijk ook adviseur. Je helpt de organisatie meer door actief gebruik te maken van de adviesrol, dit is toezicht aan de voorkant. Als je aan de voorkant meedenkt of meegeeft waaraan gedacht moet worden dat voorkomt aan de achterkant dat je met je vinger moet wijzen. Ik vind dat een FG ook zeker een adviseur moet zijn, maar wel ruimte moet hebben voor toezicht. (Respondent 10, p. 2)*

Adviseren op diverse niveaus is bij de meeste FG's sterk aanwezig. Een van de FG's geeft ook aan dat de rol van adviseur ook van nature in hem zit. Zoals in de quote van respondent 12 in paragraaf 4.3.2 is weergegeven kunnen de verschillende rollen gezien worden als twee lagen. Eerst advies en als dat niet werkt kan de toezichthoudende rol worden opgepakt.

4.4.2. Toezien op naleving van de regelgeving

Een belangrijk onderdeel van de taken van de FG is dat die moet toezien op de naleving van de regelgeving.

In paragraaf 2.2.2. van het theoretisch kader is ingegaan op het feit dat de gemeente niet al haar werkzaamheden zelf uitvoert. Veel werkzaamheden, met name ICT-oplossingen, worden door private ondernemingen uitgevoerd. Deze bedrijven zullen zich waar het gaat om de verwerking van persoonsgegevens zelfstandig aan de AVG moeten houden. Daar waar de externe partij de gegevens verwerkt voor de gemeente zal een verwerkersovereenkomst afgesloten moeten worden.

De geïnterviewde FG's is gevraagd of ze ook toezicht houden bij externe partijen. Het merendeel van de respondenten gaf aan geen toezicht bij externe partijen uit te oefenen. De focus ligt op intern. Wel staat het hoog op de lijst van de FG's om dit te gaan oppakken. Omdat vooral de informatiebeveiliging bij deze derde partijen van belang is wordt er nagedacht om samen met de CISO steekproeven te gaan uitvoeren bij externen en dan met name op het gebied van jeugdzorg en ICT. Een tweetal respondenten willen zich

gaan verdiepen in samenwerkingsverbanden, ook daar worden vaak veel gegevens verzameld en onderling met elkaar gedeeld. Een FG wijst op de verwerkersovereenkomsten die worden afgesloten. Hierin is ook opgenomen aan welk normenkader de externe partijen moeten voldoen. Een andere respondent geeft aan dat de derde partijen nog niet toe zijn aan controles uitgevoerd door een gemeentelijke FG. Het is al moeilijk om met ze een verwerkersovereenkomst af te sluiten. Deze FG heeft geconstateerd dat datalekken bij derden wel worden opgelost maar niet worden gemeld bij de gemeente, dit zou wel moeten.

Of derde partijen zelf weer zaken uitbesteden is in de interviews niet ter sprake gekomen.

> *De afhankelijkheid van grote verwerkers en het toezicht dat je daar als FG nog op kunt uitoefenen, ervaar ik als heel beperkt. Het is complex, dit zit in twee dingen. Ik ben de enige FG, dat kan eigenlijk al niet. En mijn aandachtgebied is veel meer gericht op de interne eigen organisatie. Die moeten echt leren omgaan met privacyvraagstukken, zo een verwerker niet. Het tweede is dat een zo'n verwerker een heel groot contract heeft met diverse aspecten/mensen van de gemeente te maken heeft dat zo'n privacy aspect niet de meeste prioriteit heeft. (Respondent 12, p.2)*

Twee respondenten geven aan wel eens toezicht te houden bij externen. Waarvan een aangeeft dat hij vaak het antwoord krijgt dat andere gemeenten geen vragen stellen. Een andere FG wil dit in regioverband oppakken. Dit omdat leveranciers vaak voor meerdere gemeenten werken en de partners zo niet onnodig belast worden.

Zoals in het theoretisch kader is aangegeven heeft het Rathenau instituut aangegeven dat de rol en positie van toezichthouders versterkt moet worden en dat de overheid wordt opgeroepen om normerende kaders op te stellen waar de aanschaf, ontwerp en inrichting van een systeem aan moet voldoen zodat de toezichthouder kan toetsen.

In paragraaf 4.5.1. zal nader ingegaan worden op de rol die de FG bij de selectie van partijen, in aanbestedingsprocedures, zou kunnen innemen.

Het uitvoeren van ICT-systeemchecks vinden de meeste FG's een taak van de CISO en informatiebeveiliging.

Ook is gevraagd of de FG's audits op de dienstverlening door ICT-bedrijven (bijvoorbeeld ISAE 3402, EDP) uitvoeren. Dit deed geen enkele FG. Geen een FG was bekend met dit soort audits, hier is in de interviews dan ook niet verder op doorgegaan.

Eén FG had wel een duidelijke mening over audits, namelijk dat de FG die niet zelf moet uitvoeren maar erop moet toezien. Er wordt verwezen naar gemeentelijke auditeurs en het team verbijzonderde interne controle.

> *Als deze al zouden moeten gebeuren dan zou de FG niet die audits moeten doen. De verhouding tussen de gemeente en de verwerker is de verantwoordelijkheid van de gemeente. Dat is het grootste verschil, de FG vertegenwoordigd niet de organisatie. De FG is toezichthouder van de organisatie en de organisatie moet die dingen regelen. (Respondent 6, p.3)*

Andere respondenten wijzen op de reeds aanwezige audits die binnen gemeenten worden uitgevoerd en de FG van veel informatie voorzien zoals de ENSIA-audits, audits op de Digi-D, Suwi-net, rekenkamer onderzoeken en de audit op de Wet gebruik politiegegevens. Ze zijn een bron van informatie voor de FG.

Bijna elke FG voert zijn werkzaamheden risico gedreven uit, risico gedreven toezicht. Vanwege de vele werkzaamheden die ze moeten uitvoeren zijn ze hier genoodzaakt toe. Veel respondenten zijn goed bekend met de gemeentelijke processen en weten waar de meeste risico's liggen, denk hierbij aan het sociaal domein, burgerzaken, openbare orde & veiligheid. Er worden verschillende hulpmiddelen voor gebruikt zoals het verwerkingsregister en de BIO. Ook is er een respondent die gebruik maakt van een GAP-analyse. Een andere respondent maakt gebruik van een dataclassificatie op 10 risicovolle systemen. Ook het toezichtskader van de AP wordt genoemd.

Aanvulling model

Uit de analyse blijkt dat diverse FG's de in de gemeente aanwezige audits gebruiken bij het toezien op de regelgeving. Ze zijn voor de FG een bron van informatie. Een aanvulling op het model in het onderdeel *'Taken/Toezien op naleving van regelgeving'* is dan ook om *'Audits'* op te nemen. Dit is een aanvulling op het model dat de FG van hulp kan zijn bij de uitvoering van zijn taken.

4.4.3. Beleid

In paragraaf 2.7.1. is aangegeven dat een van de taken van de FG is het toezien op naleving van het gemeentelijke beleid. Het gaat dan om beleid dat betrekking heeft op gegevensverwerking. Het beleid waar zeker op toegezien moet worden is de naleving van het gemeentelijke privacybeleid. De meeste respondenten geven aan toe te zien op de naleving van dit privacybeleid. Zij zijn ook niet betrokken bij het schrijven van het gemeentelijke privacybeleid en vinden dit ook een taak van de organisatie of de PO-er. Een aantal respondenten zijn wel betrokken geweest bij het opstellen van het privacybeleid, zij hebben dit vanuit een adviserende rol gedaan.

In paragraaf 2.7.2. is de uitspraak van de Belgische toezichthouder besproken en uit deze uitspraak komt naar voren dat indien de FG het beleid moet controleren dat hij zelf heeft opgesteld, dan wel zelf verantwoordelijk voor is, er onvoldoende mogelijkheid is om onafhankelijk te adviseren (Geschillenkamer Gegevensautoriteit 28 april 2020, AH-2019-0013).

Van de vier kenmerken van toezicht geformuleerd door Ruimschotel (2014) in paragraaf 2.3. is kenmerk nummer 3 van een toezichthouder dat een toezichthouder geen beleid maakt los van toezichtsbeleid, er worden geen nieuwe dingen gemaakt, slechts bewaakt. Uit de interviews kwam naar voren dat geen enkele FG afzonderlijk toezichtsbeleid dan wel een visie op toezicht heeft opgesteld. Wel is er een gemeente die dit in het privacybeleid heeft opgenomen. Een respondent geeft aan dat er hier wordt samengewerkt met de Verbijzonderde Interne Controle (VIC) op het gebied van het nakomen van interne afspraken.

Wat wel veel respondenten aangeven is dat ze met een jaarplan werken. Dit jaarplan wordt op verschillende manieren ingevuld. Zo is er een respondent die een rapportage met aanbevelingen maakt en

direct de aandachtspunten voor het komende jaar opneemt. Een combinatie van rapportage en jaarplan. Een respondent maakt een A4 waar die zich het komende jaar op gaat richten. Een andere respondent stelt het jaarplan halfjaarlijks bij. Zo zijn er verschillende manieren waarin toch de plannen en aandachtspunten van de FG worden vastgelegd en kenbaar gemaakt aan de organisatie.

Een respondent noemt hier nadrukkelijk de in paragraaf 2.2.1. omschreven three lines of defence.

> *Hierin staat opgenomen wat er allemaal moet gebeuren. Dit heeft te maken met de plan-do-check-act cyclus die moeten worden opgezet. De DPIA's die moeten plaatsvinden en hoe gaan we om met datalekken. Bewustwordingsacties zitten hierin.*
>
> *Wij hebben de filosofie van three lines of defence omarmd. De 3 lijnen van verdediging. De eerste lijn is de uitvoerende afdeling, die zijn primair verantwoordelijk voor de goede uitvoering van privacy-aspecten. De tweede lijn dat zijn de privacyofficers, rechten van betrokkenen, begeleiden van DPIA's. De derde lijn is dan de FG. Meer een toezichthoudende rol, adviserende rol in de derde lijn. Ik zeg ook heel duidelijk tegen de proceseigenaren, het reguliere management, jullie zijn verantwoordelijk voor de uitvoering van privacy. Als er een datalek is en het gaat heel goed mis en er staat een regionale tv-zender op de stoep dan ben jij degene die naar buiten gaat en niet ik. Dat besef moeten ze heel goed hebben. Er is nog een 4e en 5e lijn, denk aan de gemeenteraad en toezicht van de provincie, maar 3 lines is voor ons meer dan voldoende. (Respondent 11, p. 3)*

In paragraaf 2.3. is ook opgenomen dat Ruimschotel (2014) heeft aangegeven dat er bij toezicht verschil moet zijn met de situatie dat er geen toezicht is. Aan de respondenten is gevraagd wat er binnen de gemeentelijke organisatie zou gebeuren als er geen FG aanwezig zou zijn. Dit leverde verschillende inzichten op.

> *Zonder FG draaien de zaken gewoon door. Het is wel zo dat als de FG af en toe zijn tanden laat zien of mensen vriendelijk corrigerend toespreekt, de medewerkers scherper op het onderwerp zullen zijn. En nemen ze meer eigen verantwoordelijkheid want ze willen geen gedoe op dit gebied. Dat is de bijdrage als FG, dat mensen denken, laat ik het maar netjes doen, want ik heb geen zin in moeilijke vragen van de FG. Het is net als de politieauto die voorbij rijdt, mensen passen hun gedrag aan. (Respondent 2, p. 3).*

Respondenten geven aan dat als er een goede PO-er is het mogelijk niet veel verschil zal maken. Anderen geven aan dat er dan dingen fout zullen gaan. Hieruit is op te maken dat veel gemeenten behoefte hebben aan advies bij de uitvoering van de werkzaamheden. Een respondent geeft aan heel bewust een verbindende, zichtbare en toegankelijke rol aan te nemen en deze FG helpt de organisatie met handleidingen en actualiteiten die spelen. Een respondent geeft aan dat de implementatie van de AVG langzamer zou gaan als er geen FG zou zijn dit omdat privacyvraagstukken soms vertragend werken in de dienstverlening. Een ander geeft aan dat het belang van de burger, dat de FG vertegenwoordigd, uit beeld zou raken. Ook wordt erop gewezen dat waarborgen dan wegvallen. Ook stelt een FG dat dan niet meer aan het wettelijk vereiste wordt voldaan, het vereiste om een FG aan te stellen. Geconcludeerd kan worden dat het instellen van een FG in de korte verplichte periode ten goede komt aan de kwaliteit van de gemeentelijke organisatie en de behartiging van de belangen van de burger.

Aanvulling model:

Uit de analyse blijkt dat er geen enkele FG afzonderlijk toezichtsbeleid maakt. Wel zijn er diverse FG's die een jaarplan maken en hierin de aandachtspunten voor het komende jaar weergeven. Een aantal FG's hebben wel actief bijgedragen aan het gemeentelijke privacybeleid. Het is aan de FG om toezicht te houden op het privacybeleid en dit niet zelf op te stellen. Het is dan ook een aanvulling op het model in het onderdeel '*Taken/Toezien op naleving gemeentelijke beleid'* om '*Toezichtsbeleid*' op te nemen. Dit zodat er door de FG toezichtsbeleid wordt gemaakt. Dit is een aanvulling op het model dat de FG van hulp kan zijn bij de uitvoering van zijn taken.

4.4.4. Personeel & DPIA's

De geïnterviewde FG's stellen zich verschillend op richting het personeel van de gemeente.

De FG's waarbij de gemeente zo is ingericht dat ze zich voornamelijk met toezicht bezig houden ondernemen niet veel actie richting het personeel. PO-ers en anderen hebben hier het meeste contact met het personeel. Zij zijn voor de werknemers en ook de burgers goed te bereiken. Andere FG's houden zich veel bezig met bewustwordingscampagnes en geven voorlichting aan nieuwe medewerkers. Ook richten ze zich op afdelingen, waar per afdeling verschillende vraagstukken spelen. Een respondent geeft aan dat vooral de PO-ers gevonden moeten worden en dat die op de voorgrond treden. Veel respondenten gebruiken acties richting het personeel, zoals voorlichting en het actief opstellen van hulpmiddelen als een manier om gegevensbescherming op de kaart te zetten en zo aan de voorkant van de gemeentelijke processen betrokken te worden.

Een aantal respondenten geven aan dat in het jaar 2020 door de uitbraak van Covid-19, met het gevolg dat bijna alle ambtenaren vanuit huis werken, het lastiger is om zichtbaar voor het personeel te zijn.

De bijdrage van respondenten op het gebied van DPIA's is verschillend. Waar de meer toezichthoudende FG's ze als laatste toetsen en een advies geven zijn er ook respondenten die DPIA's zelf begeleiden of tussendoor al advies geven.

Aanvulling model:

Kenbaarheid en bekendheid in de organisatie helpt de FG in de uitvoering van zijn functie. De FG is dan gemakkelijker door het eigen personeel te vinden bij vragen of meldingen. Uit de analyse is naar voren gekomen dat FG's die dit actief doen ervaren dat ze binnen de organisatie goed gevonden worden. Het is dan ook een aanvulling op het model in het onderdeel '*Taken/Personeel/DPIA's'* om als FG te werken aan '*Zichtbaarheid*' en acties richting het personeel te ondernemen, zoals bewustwordingsacties of scholing. Dit is een aanvulling op het model dat de FG van hulp kan zijn bij de uitvoering van zijn taken.

4.4.5. Autoriteit Persoonsgegevens

Een van de taken van de functionaris voor gegevensbescherming is dat die moet samenwerken met de Autoriteit Persoonsgegevens. Ook is de FG contactpersoon van de AP.

De AP ziet de FG als verlengstuk. Een aantal respondenten geven aan dat zij zich daadwerkelijk als verlengstuk van de AP zien. Een aantal respondenten hebben ook goed contact met de AP. De meeste FG's zien zichzelf niet als verlengstuk van de AP, dit omdat hun rol anders is. De FG is echt onderdeel van de gemeentelijke organisatie. Vaak is de FG als adviseur betrokken bij de oplossing binnen de organisatie. Een respondent geeft ook aan beperktere bevoegdheden te hebben dan de AP, zo kan een FG bijvoorbeeld geen boetes opleggen. Een respondent geeft aan dat de AP meer op de toezichthoudende kant zit en de FG meer op de advieskant. Dit komt ook overeen met hoe de FG zijn eigen rol binnen de organisatie ziet, zoals omschreven in paragraaf 4.4.1. zien zij zichzelf veelal als adviseur.

Contact met de AP is er niet veel. Dit beperkt zich tot een aantal keer per jaar. De meeste contacten gaan over de afhandeling van datalekken of klachten. Slechts een enkeling heeft inhoudelijk contact met medewerkers bij de AP, deze contacten komen voort uit het netwerk dat deze FG onderhoudt. Voor het sparren of stellen van inhoudelijke vragen maken de FG's gebruik van hun eigen netwerk of vragen het een jurist die werkzaam is bij de gemeente.

Een respondent geeft aan dat als de AP contact opneemt met de gemeentelijke organisatie, niet altijd de FG wordt benaderd. Het zou een aanbeveling voor de AP zijn om altijd de FG te benaderen. Omdat deze thesis gericht is op de gemeentelijke organisatie en niet op de AP zal de aanbeveling dan ook zijn om dit intern binnen de gemeente goed te regelen. Mocht iemand in de organisatie door de AP benaderd worden dan moet de organisatie zo alert zijn om ook de FG te attenderen.

> *Alleen de organisatie heeft echt behoefte aan iemand die helpt. Als ik alleen maar ga roepen dat ze dingen niet goed doen dan geloof ik niet dat mensen graag bij mij aankloppen. Ik heb als doel om de organisatie vooruit te helpen naar een volwassenheidsniveau waar we tevreden over zijn. Daar moeten we op dit moment de balans in vinden. In de toekomst kan ik mogelijk iets strenger optreden. Als de boel eenmaal staat dan is daar meer tijd voor. Als ik alleen maar met de rode pen ga schrijven dan blijven mensen weg. (Respondent 4, p. 4)*

> *Ik zit er nu nog veel meer in als onderdeel van de oplossing als er wat schoort, als opspoorder van het defect. Die defecten zijn er en die komen vanuit de organisatie voldoende naar boven, daar hebben we onze handen al vol aan. Ik zou wat meer aan de opsporende kant en toezichthoudende kant moeten doen, maar daar kom ik op dit moment niet aan toe. Mijn rol is meer, wat draagt bij aan de oplossing, wat is een verantwoorde manier voor de gemeente om te gaan doen. (Respondent 7, p. 5)*

Aan respondenten is gevraagd wie ze als samenwerkingspartners zien. Intern wordt hier de CISO, PO-ers, en functionarissen gegevensbescherming genoemd. De samenwerking met de CISO wordt echt gezien als aanvullend, de FG en CISO lopen hand in hand. Het zal helpen om deze samen binnen één afdeling te

positioneren. Voor de gehele organisatie is dan duidelijk dat deze beide functionarissen onafhankelijk werken. Extern werken veel FG'ers samen in de regio. Hier wordt samengewerkt en er zijn ook een aantal respondenten die regionaal aan intervisie doen. Niet elke respondent ziet de FG's in de regio echt als samenwerkingspartner maar noemt ze wel in de zin van onderdeel van het netwerk.

Aanvulling model:

De FG is bij de gemeente het aanspreekpunt de Autoriteit Persoonsgegevens. Omdat de AP niet zelf altijd als eerste de FG benadert bij kwesties verdiend het de aanbeveling om dit binnen de gemeente te organiseren. Het is dan ook een aanvulling op het model in het onderdeel *'Taken/Samenwerken Autoriteit Persoonsgegevens'* om *'Kenbaarheid'* van de FG te organiseren. Dit is een aanvulling op het model dat de FG van hulp kan zijn bij de uitvoering van zijn taken.

4.4.6. Hoogste leidinggevende niveau

Een van de taken van de FG is dat die rapporteert aan het hoogste leidinggevende niveau. Voor alle respondenten is ambtelijk het hoogste leidinggevende niveau binnen de gemeente de gemeentesecretaris. Bestuurlijk wordt het college van burgemeester & wethouders, de gemeenteraad en de burgemeester genoemd. De meeste respondenten hebben regelmatig contact met de gemeentesecretaris en bestuurlijk met de portefeuillehouder, dit kan een wethouder of de burgemeester zijn. Regelmatig overleg, sommigen per kwartaal, wordt als prettig ervaren. Zo landt het onderwerp gegevensbescherming en privacy op tafel van het hoogste niveau.

Bij een respondent is uit praktische overwegingen de directeur bedrijfsvoering aangewezen om dit onderwerp als onderdeel van het takenpakket op te pakken. Hier wordt regelmatig overleg mee gevoerd.

Een beperking in de toegang tot het hoogste leidinggevende niveau wordt door geen enkele FG ervaren. Ook de FG's die onder een afdelingshoofd werken ervaren geen beperkingen. Soms wordt er wel eens uit praktische overweging gekozen om een onderwerp via een businesscontroller te laten lopen.

Aan wie gerapporteerd wordt verschild. Zo zijn er FG's die aan de gemeentesecretaris rapporteren die het vervolgens richting de politiek brengt. Bij veel gemeenten wordt, indien er een jaarrapportage wordt opgesteld dit aan de bestuurders voorgelegd. Een aantal respondenten geven aan de rapportage in het reguliere jaarverslag op te nemen. Met de jaarstukken wordt verantwoording afgelegd over het gevoerde beleid. Zo gaat de rapportage en verantwoording van de FG mee in het ritme van de gemeente. Voor de politiek ook heel handig om alles bij elkaar te hebben.

Aanvulling model

Om niet zelf een afzonderlijke rapportage op te stellen doen een aantal FG's de aanbeveling om als FG verantwoording af te leggen in het gemeentelijke jaarverslag. Omdat dit FG's kan helpen in het afleggen van verantwoording wordt *'Jaarverslag'* als aanvulling op het model in het onderdeel '*Taken/Rapporteer aan hoogste leidinggevende niveau'* als aanvulling opgenomen. Dit is een aanvulling op het model dat de FG van hulp kan zijn bij de uitvoering van zijn taken.

Daarnaast wordt regelmatig overleg met de gemeentesecretaris door de respondenten die dit hebben als prettig ervaren. Het landt hiermee op tafel bij de hoogste ambtelijke verantwoordelijke. Hierom wordt het voeren van *'Overleg'* toegevoegd aan het model onder het onderdeel *'Organisatie/Toegang tot hoogst leidinggevende'*. Dit is een aanvulling die de organisatie helpt zijn FG te positioneren.

4.5. De organisatie

4.5.1. Tijdig betrekken

De FG moet tijdig betrokken worden bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Gemeenten van middelgroot formaat zijn vrij groot in omvang. Vaak is er een ambtelijk apparaat van rond de 1.000 werknemers. Een van de respondenten geeft aan dat een gemeente meer producten heeft dan Philips, dit geeft de complexiteit van de organisatie aan. Aan de voorkant betrokken worden is dan nog wel eens een uitdaging. Respondenten geven aan dat ze wel steeds beter gevonden worden. Bij gemeenten waar gestructureerd projectmatig wordt gewerkt, en de start van een project begint met een inventarisatie of zoals een van de respondenten het noemt een initiatiefkaart, is gegevensverwerking en het betrekken van de FG een vast onderdeel van het proces. Andere respondenten zijn goed bekend met de organisatie en weten zelf wat waar speelt. Deze FG's wachten niet af tot ze betrokken worden maar reageren op signalen en vinden zo hun weg. Ook de samenwerking met de CISO levert hier voordelen op. Die weet ook wat er speelt.

De respondenten willen vooral betrokken worden aan de voorkant van het proces en bij onderwerpen zoals Smart cities, wisseling van ICT-systemen, data-analysen en aanbestedingen.

Bij Europese aanbestedingen, waar de gemeente een derde partij selecteert om werkzaamheden uit te voeren is betrokkenheid van de FG van belang. Zoals in paragraaf 4.3.2. besproken worden veel gemeentelijke processen door derden uitgevoerd. Dit omvat ook veel processen waar verwerking van persoonsgegevens plaats vinden, zoals de aanschaf van ICT-systemen. Aan de voorkant van dit proces input kunnen leveren op het gebied van gegevensbescherming kan problemen na afsluiten van de overeenkomst voorkomen. Dit hoeft niet altijd de FG zelf te zijn maar kan ook de PO-er zijn. Ook geeft een respondent aan dat betrokken inkoopadviseurs zelf scherp zijn en weten waar ze op moeten letten in een inkooptraject. Een respondent geeft aan dat in de aanbestedingsdocumenten standaardpassages zijn opgenomen. In deze passages staan de eisen waaraan de inschrijvende partij moet voldoen op het gebied van gegevensbescherming. Er vindt geen controle plaats of dit daadwerkelijk ook zo wordt uitgevoerd.

<u>Aanvulling model:</u>
Binnen gemeentelijke organisaties beginnen projecten met een initiatieffase en een inkooptraject start met het opstellen van de inkoop/aanbestedingsdocumenten. Vanuit de interviews en analyse komt naar voren dat FG's die hier tijdig aan tafel zitten kunnen zorgen voor projecten en producten waar gegevensbescherming een onderdeel van is. Het is niet de FG die aan tafel moet komen een privacyadviseur kan dit advieswerk ook heel goed doen. Dan kan de FG in een latere fase toezichthouden. Omdat projecten en aanbestedingen de momenten zijn om tijdig betrokken te worden, zullen *'Projecten'* en *'Aanbestedingen'* als aanvullingen op het model in het onderdeel '*Organisatie/Tijdig betrekken'* worden opgenomen. Dit is een aanvulling die de organisatie helpt zijn FG te positioneren.

4.5.2. Toegang verschaffen

Om zijn werkzaamheden goed te kunnen uitoefenen moet de organisatie de FG toegang verschaffen tot persoonsgegevens en verwerkingsactiviteiten. Uit de interviews komt naar voren dat er op dit gebied weinig beperkingen zijn. De meeste respondenten geven aan niet standaard de toegang te hebben tot alle systemen of locaties en dit nadrukkelijk ook niet te willen. Indien ze iets nodig hebben dan worden er geen belemmeringen ervaren. Dit is overal goed ingericht.

4.5.3. Benodigde middelen

De organisatie moet de FG in de uitvoering van zijn taken voorzien van de benodigde middelen. Aan respondenten is gevraagd of zij hier de beschikking over hebben. Ook is gevraagd wat ze als cruciale middelen zien en of ze nog middelen missen. Bijna alle respondenten hebben de beschikking over de benodigde middelen. De inrichting is verschillend, waar de een eigen budget heeft, ervaart de ander, die geen budget heeft, geen belemmeringen als er om iets wordt verzocht. Wat wel een aantal respondenten aangeven is dat ze meer capaciteit zouden willen, een extra PO-er of een extra FG. Er is veel behoefte aan extra capaciteit om op de werkvloer advies te geven.

Wat een aantal keer genoemd wordt is dat het cruciaal is dat de rol van FG serieus wordt genomen en op waarde geschat, erkenning als deskundige is belangrijk. Ook moet de FG benaderbaar zijn. Ook hier wordt opgemerkt dat dit in tijden van de Covid-19 pandemie lastiger is. Even rondlopen en je gezicht laten zien zit er nu niet in terwijl dit wel voor de uitvoering van de functie van belang is.

> *Dat je rol serieus wordt genomen. Dat een advies op waarde wordt geschat. Als dat draagvlak er niet is dan houdt het snel op. Ik merk ook wel dat als mijn naam er onder staat dat men weet, het staat nu op papier, ik moet hier echt wat mee. Als dat niet meer gebeurt dan ben je je autoriteit erin kwijt. (Respondent 7, p.7)*

Door een aantal respondenten wordt het volgen van scholing ook als cruciaal middel genoemd. Een FG moet in staat zijn om zijn vakkennis bij te houden.

<u>Aanvulling model</u>
Een aantal respondenten gaven zeer specifiek aan dat scholing van de FG heel belangrijk is voor de taakuitoefening van de FG. De FG moet in staat zijn om zijn vakkennis op peil houden. Omdat er voor de FG geen sprake is van verplichte scholing, zoals wel bij accountants of controllers, wordt *'Scholing'* als aanvulling van het model opgenomen onder het onderdeel *'organisatie/benodigde middelen'*. Dit is een aanvulling die de organisatie helpt zijn FG te positioneren.

4.5.4. Geen instructies geven, benadelingsverbod en belangenverstrengeling

De organisatie mag de FG geen instructies geven of benadelen. Geen van de respondenten heeft hier ervaring mee. Hieruit kan de conclusie getrokken worden dat dit goed bekend is binnen de gemeenten en dat de positie van de FG op waarde wordt geschat.
Ook op het gebied van belangenverstrengeling zijn geen aanbevelingen opgehaald.

4.6. De eisen aan de functionaris voor gegevensbescherming

Zoals in paragraaf 2.7.3. opgenomen worden er eisen aan de FG gesteld. De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen (art. 37 lid 5 AVG)

Met de selectie en aanstelling van een FG zal hier rekening mee gehouden moeten worden. Bij geïnterviewden is informatie opgehaald om nader invulling te geven aan dit vereiste en wat van belang is voor een gemeente van middelgroot formaat.

4.6.1. Niveau van deskundigheid

Bijna alle respondenten geven aan dat er geen niveau zoals Hbo of WO op de functie is te plakken. Het gaat veel meer om capaciteiten. Het is van belang dat een FG een goed analytisch denkvermogen heeft en kennis heeft van de gemeentelijke organisatie en processen. Organisatiesensitief en het kunnen schakelen op de diverse niveaus, van vuilnisman tot burgemeester is van belang. Volgens een aantal respondenten hoort hier een iets oudere leeftijd en een zekere senioriteit bij.

> *Belangrijkste kwalificatie vind ik, dat je 'grijze haren hebt'. Dat je het vermogen hebt om gesprekspartner te zijn voor diverse mensen in de organisatie. En met 'grijze haren' ben je vaak beter in staat om op verschillende niveaus te communiceren. De boodschap van privacy, waarom dat zo belangrijk is, over te brengen. En om corrigerend te kunnen toespreken is als jong iemand niet zo effectief, kan je beter 'grijze haren' hebben. Daar hoort levenswijsheid bij. En ook pragmatisme. Het gaat meer over competenties dan over opleidingsniveau. (Respondent 2, p. 6)*

Een aantal respondenten spreken zich wel uit en geven aan dat WO-niveau de voorkeur heeft maar met de aanvulling dat het voor iemand met een Hbo-opleiding ook mogelijk is. Ook hier wordt weer verwezen naar de benodigde capaciteiten en competenties van de betreffende persoon.

Zoals in paragraaf 4.3 is aangegeven hebben een aantal gemeenten bij de selectie van de FG gekeken naar de fase waarin de gemeente zich bevindt en/of het volwassenheidsniveau van de organisatie op het gebied van privacy. Hier is vervolgens een FG geworven die competenties heeft die op dat moment passen bij de organisatie. Is er bijvoorbeeld een FG nodig die heel goed kan bouwen of verbinden. Of is de functie van FG heel toezichthoudend ingericht, dat vraagt andere competenties.

Aanvulling model

Alle respondenten gaven aan dat in de uitvoering van de functie het hebben van de juiste vaardigheden van belang is. Omdat '*Vaardigheden*' door alle respondenten als zeer belangrijk wordt gevonden, wordt dit als aanvulling op het model opgenomen onder het onderdeel '*Eisen aan functionaris/Niveau van deskundigheid*'. Dit is een onderdeel waar de organisatie bij de aanname of ontwikkeling van een FG rekening kan houden. Dit is een aanvulling die de organisatie helpt zijn FG te positioneren.

4.6.2. Professionele kwaliteit

Om de professionele kwaliteit te kunnen bereiken kan scholing helpen. De respondenten geven aan dat het aanbod van scholing op dit moment heel divers is. Er is een divers aanbod en de ervaringen zijn verschillend.

Een aantal respondenten geven aan dat de aangeboden scholing voornamelijk ziet op inhoudelijke kennis. Terwijl voor de FG juist de vaardigheden en competenties van belang zijn. Dit wordt gezien als een tekort in het huidige aanbod. Een aantal FG's zien wel wat in een verplichte opleiding en certificering van de FG. Geen enkele FG wist een opleiding te noemen die op dit moment geheel voldoet. Wat meerdere FG's van belang vinden is het actueel houden van kennis. Een FG ziet hier ook een taak voor de VNG om dit op te pakken. Dit voor gemeente specifieke zaken.

4.6.3. Persoonlijke vaardigheden en kennis

Bij dit onderdeel gaat het om de persoonlijke vaardigheden en positie in de organisatie. Qua plek in de organisatie is in paragraaf 4.3.1. aanbevolen om de FG bij een control/staf afdeling te plaatsten.

Qua persoonlijke vaardigheden is aan de respondenten de vraag gesteld over welke vaardigheden moet een FG beschikken. Alle opgehaalde vaardigheden zijn in de driedeling taken, organisatie en eisen functionaris opgenomen en zijn opgenomen in tabel 2. Als belangrijkste worden genoemd de wijze waarop de functionaris communiceert, op verschillende niveaus kan schakelen, analytisch moet zijn, goede adviesvaardigheden hebben en stevig in zijn schoenen moet staan. Daarnaast is het van belang dat de FG geïnteresseerd is wetgeving/een juridische affiniteit heeft.

Aanvulling model

Door alle respondenten werden diverse competenties genoemd waar een FG aan moet voldoen. Omdat het hebben van de juiste competenties van belang is in de uitvoering van de functie wordt aan het model onder onderdeel *'Eisen aan functionaris/persoonlijke vaardigheden en kennis'* het onderdeel *'Competenties'* toegevoegd. Dit is een onderdeel waar de organisatie bij de aanname of ontwikkeling van een FG rekening kan houden. Het is een aanvulling voor de organisatie.

Tabel 2: Vaardigheden waar een FG voor een middelgrote gemeente over moet beschikken. Waar een vaardigheid meerdere keren is genoemd is dit aantal tussen haakjes opgenomen.

Taken	**Organisatie**	**Functionaris**
Geïnteresseerd in wetgeving/ juridische affiniteit (4)	Weten hoe een gemeente reilt en zeilt (2)	Communicatief vaardig en helder kunnen communiceren (5)
Begrijpen hoe processen zijn ingeregeld (2)	Organisatie overzien	Verschillende niveaus kunnen schakelen/diplomatiek (5)
		In staat zijn om mensen te motiveren (4)
Kennis van techniek/ICT (2)	Kennis organisatie	Analytisch inzicht/denken (4)
	Aan tafel komen van bestuurder	Goede adviesvaardigheden (4)
		Stevig in schoenen staan/ dikke huid hebben (4)
		Overtuigend zijn (3)
		In staat zijn om kennis over te dragen (2)
		Goed kunnen schrijven/onderbouwen (2)
		Werkervaring/levenswijsheid (2)
		Geduld (2)
		Pragmatisch zijn (2)
		Kritisch zijn
		Onafhankelijk kunnen opereren
		Nee kunnen verkopen
		Impact hebben
		Benaderbaar zijn
		Kunnen omgaan met tegengestelde belangen
		Maatschappelijk betrokken
		Weten welke competenties een PO-er nodig heeft
		Punctueel
		Leiderschapsstijlen beheersen
		Rust uitstralen

5. CONCLUSIES EN MODEL

5.1. Inleiding

In dit hoofdstuk worden de deelvragen zoals geformuleerd in hoofdstuk 1 beantwoord. Vervolgens zal de onderzoeksvraag worden beantwoord.

5.2. Beantwoording deelvragen

Deelvraag 1
Wat zijn de uitgangspunten (vanuit de regelgeving) waaraan voldaan moet worden zodat de functionaris gegevensbescherming zijn functie kan uitoefenen.

De uitgangspunten in de regelgeving staan geformuleerd in de Algemene Verordening Gegevensbescherming. In artikel 37 lid 1 sub a AVG is opgenomen dat een gemeentelijke organisatie verplicht is om er een aan te stellen. In de artikelen 37, 38 en 39 AVG zijn de eisen die gesteld worden aan de FG en de worden de taken van de FG nader uitgewerkt. In aanvulling op de AVG is door de Groep gegevensbescherming artikel 29 een nadere uitwerking gegeven aan een aantal uitgangpunten zoals in de AVG geformuleerd.

De uitgangspunten waaraan voldaan moet worden zodat een FG zijn functie kan uitoefenen zijn in een drietal onderdelen op te delen. Het gaat om de taken van de functionaris, de eisen waaraan de organisatie moet voldoen en de eisen die gesteld worden aan de functionaris zelf.

De taken van de functionaris voor gegevensbescherming betreffen het informeren en adviseren, toezien op de naleving van regelgeving, toezien op de naleving van gemeentelijk beleid, zichtbaar zijn naar het personeel, toetsen van data protection impact assessments, contactpersoon van de Autoriteit Persoonsgegevens zijn en hier ook mee samenwerken. Ook moet er gerapporteerd worden aan de hoogste leidinggevende.

Om deze taken goed te kunnen uitoefenen moet de gemeentelijke organisatie aan een aantal eisen voldoen. Uit de regelgeving is op te maken dat de gemeente de functionaris voor gegevensbescherming naar behoren en tijdig moet betrekken. De functionaris moet toegang hebben tot alle persoonsgegevens en verwerkingsactiviteiten. Daarnaast moet de functionaris over voldoende middelen beschikken. De functionaris mag geen instructies ontvangen of benadeeld worden. De functionaris moet toegang hebben tot hoogste leidinggevende. Hij moet goed bereikbaar zijn voor betrokkenen, is gehouden aan geheimhouding en vertrouwelijkheid en er mag geen belangenverstrengeling ontstaan.

Aan de functionaris voor gegevensbescherming worden ook eisen gesteld. Deze moet een aan een bepaald niveau van deskundigheid voldoen, beschikken over professionele kwaliteiten en het vermogen hebben tot vervullen van de taken.

De eisen aan de functionaris voor gegevensbescherming zijn door de Groep gegevensbescherming artikel 29 nader uitgewerkt en komen erop neer dat de FG ervaring met wetgeving, met name op het gebied van gegevensbescherming, moet hebben. De FG moet beschikken over kennis van de bedrijfstak en organisatie

waar die werkzaam is. Daarnaast moet de FG inzicht hebben in de verwerkingsactiviteiten, kennis van administratieve regels en procedures hebben en beschikken over persoonlijke vaardigheden en kennis. Als laatste is zijn positie in de organisatie van belang. Hij moet in de organisatie gepositioneerd worden dat hij zijn werkzaamheden goed kan uitoefenen.

Aanvullend is literatuuronderzoek gedaan naar het begrip 'toezichthouder'. Hierbij kan worden opgemerkt dat volgens Ruimschotel (2014) het bij een functionaris die toezicht houdt gaat om het 'kijken of het goed gaat, maar ook zorgen dat het goed gaat'. Ruimschotel (2014) heeft het bij toezicht over een actief waakzame houding vanuit een plicht die bestaat uit de volgende vier kenmerken: Toezicht staat aan de zijlijn (1), actieve waakzaamheid van buiten zichzelf (2), conserverend en creëert niet (3) en is meer dan blinde uitvoering (4).

In de functie van Functionaris voor Gegevensbescherming zit ook een zeer nadrukkelijke adviestaak dat de functionaris niet altijd aan de zijlaan staat maar ook vaak in het veld meespeelt. Geconcludeerd kan worden dat de definitie die Ruimschotel (2014) aan toezichthouder geeft niet altijd op gaat voor de functionaris voor gegevensbescherming.

Waar veel toezichthouders ook zelfstandige handhavingsbevoegdheden hebben is dit niet het geval bij de functionaris voor gegevensbescherming. Handhaven is een taak van de Autoriteit Persoonsgegevens.

Deelvraag 2
Zijn al deze uitgangspunten van gelijkwaardig belang.

Uit de regelgeving is niet gebleken dat er aan de uitgangspunten zoals opgenomen bij de beantwoording van deelvraag 1 een gradatie is aan te brengen. Het betreffen allemaal uitgangspunten waaraan voldaan moet worden.
Geconcludeerd kan worden dat alle eisen van gelijkwaardig belang zijn.

Deelvraag 3
Hoe kan de organisatie waarborgen dat aan deze uitgangspunten voldaan worden.

Middelgrote gemeente hebben vaak een gelijke organisatiestructuur die is opgebouwd volgens een directiemodel. Hierbij zijn afzonderlijke bedrijfsvoeringsafdelingen binnen de organisatie gepositioneerd zoals een afdeling financiën, HRM en ICT. Deze afdelingen bedienen de gehele organisatie. In deze structuur past het ook om een afzonderlijke afdeling te hebben waar de interne toezichthouders gepositioneerd zijn.

Gemeenten werken daarnaast vaak middels het principe van three lines of defence. Er is een eerste lijn, de vakafdeling, die is zelf verantwoordelijk voor haar activiteiten. In het geval van gegevensbescherming binnen een gemeente is de vakafdeling zelf verantwoordelijk voor het product dat de afdeling aflevert, inclusief een goede gegevensbescherming. De manager is integraal verantwoordelijk. Hierbij kan de afdeling ondersteuning, van een meer gespecialiseerd iemand krijgen, dit is de tweede lijn. Op het gebied van gegevensbescherming zijn dit vaak privacy officers, zij hebben inhoudelijk meer kennis dan op de afdeling aanwezig is. Vervolgens is er de derde lijn, dit betreft de controle functie zoals de concerncontroller, de Chief Information Officer (CIO) en op het gebied van gegevensbescherming zou de Functionaris voor Gegevensbescherming als derde lijn gezien kunnen worden.

Door de organisatie-indeling en verantwoordelijkheden goed uit te dragen kan geborgd worden dan aan de uitgangspunten van de regelgeving voldaan kan worden.

Deelvraag 4
Hoe kan de functionaris gegevensbescherming in de organisatie gepositioneerd worden.

Kijkend naar de wijze waarop de middelgrote gemeente is ingedeeld, de taken van de FG en de eisen die aan de organisatie en de FG worden gesteld kan geconcludeerd worden dan de FG het best gepositioneerd worden in de derde lijn bij een staf/control afdeling. Door de FG op deze afdeling te plaatsen is die geen onderdeel van het primaire proces, het speelveld maar staat die ernaast. Hierdoor kan de FG zijn toezichthoudende taak uitoefenen en zal het advies ook vanuit dit toezichthoudende kader gegeven kunnen worden.

Op basis van het literatuuronderzoek is het model zoals weergegeven in figuur 1 opgesteld. In dit model is opgenomen een overzicht van de taken van de functionaris voor gegevensbescherming, de eisen die gesteld worden aan de organisatie en de eisen die gesteld worden aan de functionaris voor gegevensbescherming.

Deelvraag 5
Levert het veldonderzoek nieuwe uitgangspunten op die aan het model, dat op basis van de theorie is opgesteld, toegevoegd moeten worden.

Het veldonderzoek heeft nieuwe elementen opgeleverd die aan aanvulling zijn op het theoretisch model, figuur 1. Het gaat om aanvullingen die een middelgrote gemeente helpen bij de positionering van de functionaris voor gegevensbescherming in de organisatie en de functionaris zelf behulpzaam zijn bij de uitvoering van zijn taken.

Als eerste zijn er aanvullingen op het model die de organisatie kan doen om de functionaris voor gegevensbescherming in de organisatie te positioneren en zorgen dat die zijn werkzaamheden goed kan uitoefenen. In de driedeling die in het model gebruikt is wordt na het kwalitatieve onderzoek op dit onderdeel het volgende toegevoegd.

Bij het onderdeel *taken van de functionaris voor gegevensbescherming*: Verantwoordelijkheid voor gegevensbescherming binnen de organisatie goed vastleggen en uitdragen.

Bij *eisen aan de organisatie* wordt toegevoegd: Het in positie brengen van het onderwerp gegevensbescherming bij projecten en aanbestedingen, de FG de mogelijkheid bieden om zich te scholing en regelmatig overleg voeren met de hoogste leidinggevende.

Bij de *eisen aan functionaris voor gegevensbescherming* wordt aan het model toegevoegd: Vaardigheden, competenties, plaatsing bij een afdeling staf/control en het organiseren van vervanging.

Als tweede gaat het om aanvullingen die de functionaris voor gegevensbescherming behulpzaam kunnen zijn bij zijn taakuitoefeningen. In de driedeling die in het model is gemaakt zijn op dit onderdeel alleen aanvullingen bij *taken van de functionaris voor gegevensbescherming*. Hieraan wordt toegevoegd: Het gebruik maken van het borgingsdocument VNG, aanwezige audits en het organiseren van samenwerkingen. Het opstellen van eigen toezichtsbeleid, zorgen van zichtbaarheid in de organisatie en kenbaarheid in de organisatie indien de Autoriteit Persoonsgegevens contact opneemt. Voor het afleggen van verantwoording kan aangesloten worden bij het gemeentelijke jaarverslag.

5.3. Beantwoording onderzoeksvraag

De onderzoeksvraag is in paragraaf 1.2.2. als volgt geformuleerd:

Ontwerp een model met hierin opgenomen de uitgangspunten voor de middelgrote gemeente en de daar aangestelde functionaris voor gegevensbescherming. Voor de gemeentelijke organisatie is dit model een hulpmiddel om de functionaris voor gegevensbescherming te positioneren en tot een juiste taakuitoefening te laten komen. Voor de functionaris gegevensbescherming biedt dit model een handvat voor een juiste uitoefening van zijn taken.

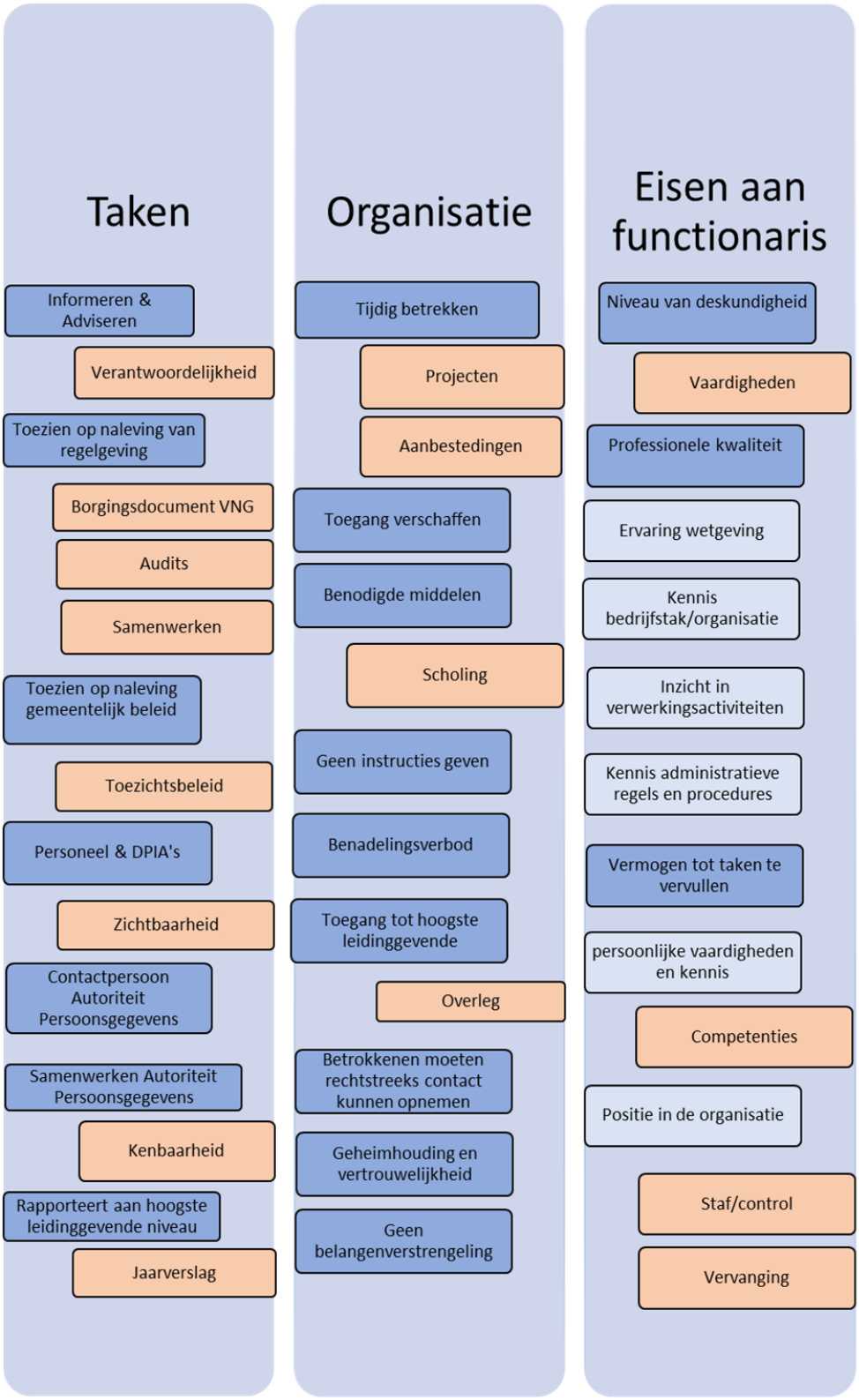
Het doel van het onderzoek is te komen met een model specifiek voor de middelgrote gemeente. Dit model is opgesteld en weergegeven in figuur 2. Het model betreft de wettelijke uitgangspunten waar gemeenten rekening mee moeten houden bij de aanstelling en positionering van de functionaris voor gegevensbescherming. Dit model is nader ingevuld met de uitwerking van de Groep gegevensbescherming artikel 29. Vervolgens is het model nader aangevuld met uitgangspunten die vanuit het veldonderzoek naar voren zijn gekomen.

Uit het veldonderzoek is niet naar voren gekomen dat er een discrepantie is tussen de wettelijk geformuleerde uitgangspunten. Wel is er nadere invulling gegeven aan begrippen uit de regelgeving. Zo is invulling en aanvulling gegeven aan belangrijke begrippen uit de regelgeving. Ook kwam duidelijk naar voren dat de FG kan meelopen in het ritme van de stad door gebruik te maken van bestaande processen en reeds aanwezige documenten.

Uit het onderzoek blijkt dat de functionaris voor gegevensbescherming naast toezicht houden ook een hele duidelijke adviestaak heeft. Uit het kwalitatieve onderzoek kwam naar voren dat deze adviestaak verschillend wordt ingevuld. Dit heeft met name te maken met de fase waarin de gemeentelijke organisatie zich bevindt. Hoe minder kennis op het gebied van gegevensbescherming in de organisatie hoe meer de functionaris voor gegevensbescherming aan de voorkant van processen betrokken is en adviseert. Indien er meer bewustzijn in de organisatie zelf aanwezig is, of als er een duidelijke keuze is gemaakt dat de FG een toezichthoudende taak heeft dan wordt de adviesrol meer vanuit een toezichthoudend kader uitgevoerd.

Dit geheel is schematisch weergegeven in het model figuur 2. De gemeente kan dit model gebruiken om haar functionaris voor gegevensbescherming in de organisatie te positionering en kan de functionaris zelf behulpzaam kan zijn bij de uitvoering van zijn taken.

In het model figuur 2 zijn de blauwe blokken uitgangspunten afkomstig uit de regelgeving. De licht blauwe blokken zijn nadere aanvullingen van de Groep gegevensbescherming artikel 29. De oranje blokken zijn de nadere invulling uit het veldonderzoek. Het model is voorzien van een toelichting.



Figuur 2. Model positionering functionaris voor gegevensbescherming voor de middelgrote gemeente.

Toelichting model:

Dit model is een hulpmiddel voor de middelgrote gemeente en de daar aangestelde functionaris voor gegevensbescherming (FG).

Het model betreft de wettelijke uitgangspunten waar gemeenten rekening mee moeten houden bij de aanstelling en positionering van de functionaris voor gegevensbescherming (donker blauwe blokken). Het model is nader ingevuld met uitwerkingen van de Groep gegevensbescherming artikel 29 (licht blauwe blokken). Vervolgens is het model aangevuld met uitgangspunten die vanuit kwalitatief onderzoek naar voren zijn gekomen (oranje blokken). Deze laatste aanvullingen zijn geen (wettelijke) eisen maar kunnen de gemeente en de FG ter ondersteuning zijn. In de tekstuele toelichting zijn deze door een inspringing in de kantlijn te herkennen.

Taken

Informeren & Adviseren: De FG informeert en adviseert de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen uit de AVG en andere wet- en regelgeving die gaat over gegevensbescherming.

> *Verantwoordelijkheid:* Leg binnen de gemeentelijke organisatie goed vast wie, op het gebied van gegevensbescherming, waarvoor verantwoordelijk is. Is er sprake van integraal management dan is de (afdelings)manager zelf verantwoordelijk voor de producten van de afdeling, inclusief een goede gegevensbescherming. Dit kan worden vastgelegd in de organisatieregeling/verordening of het privacybeleid. Draag dit actief uit.

Toezien op naleving van regelgeving: Toezien op naleving van de AVG, EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming.

> *Borgingsdocument VNG*: Het borgingsdocument AVG van de VNG kan de FG als toezichtskader gebruiken.
>
> *Audits:* Gemeentelijke audits, zoals de ENSIA, audits op Digi-D, suwi-net, wet gebruik Politiegegevens en onderzoeken van de gemeentelijke rekenkamer kunnen de FG van informatie voorzien en behulpzaam zijn in de uitvoering van de taken.
>
> *Samenwerken*: Intern optrekken met privacy officer, de Chief Information Security Officer en Concerncontroller. Extern met FG's uit een samenwerking of in de regio.

Toezien op naleving gemeentelijk beleid: Toezien op de naleving van het privacybeleid. Toezien op naleving van overig gemeentelijk beleid daar waar het om de verwerking van persoonsgegevens gaat.

> *Toezichtsbeleid:* Maakt als FG kenbaar waar toezicht op wordt gehouden. Als er een rapportage wordt opgesteld kan hierin worden meegenomen wat de komende periode de aandachtpunten zijn. Om risicogestuurd te kunnen werken kan de FG gebruik maken van de BIO, het verwerkingenregister, het toezichtskader van de AP en de aandachtpunten/jaarplan van de CISO. Er kan gekozen worden om mee te lopen met het ritme van de VIC-controle.

Personeel & DPIA's: Het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het personeel en betrokkenheid bij DPIA's.

Zichtbaarheid: Door acties richting het personeel te ondernemen, zoals bewustwordingsacties of scholing, wordt het bewustzijn rond gegevensverwerking en de zichtbaarheid en vindbaarheid van de FG vergroot.

Contactpersoon Autoriteit Persoonsgegevens: Meld de FG aan bij de Autoriteit Persoonsgegevens.

Samenwerken Autoriteit Persoonsgegevens: De FG is het aanspreekpunt voor de Autoriteit Persoonsgegevens.

Kenbaarheid: Zorg dat in de organisatie bekend is dat als de Autoriteit Persoonsgegevens contract opneemt direct de FG wordt ingeschakeld.

Rapporteer aan hoogste leidinggevende niveau: Ambtelijk kan rapport worden uitgebracht aan de gemeentesecretaris. Bestuurlijk aan het betreffende bestuursorgaan: het college van burgemeester & wethouders, de burgemeester en/of de gemeenteraad.

Jaarverslag: De FG kan een afzonderlijk jaarverslag maken of verantwoording afleggen in het gemeentelijke jaarverslag dat vaak onderdeel is van de jaarstukken.

Organisatie

Tijdig betrekken: De FG naar behoren en tijdig betrekken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Projecten: Indien er binnen de gemeente projectmatig wordt gewerkt maak gegevensbescherming een vast onderdeel van de iniatief/startfase het project.

Aanbestedingen: Bij de start van een inkoop/aanbesteding nagaan of binnen de opdracht sprake is van (verwerking van) persoonsgegevens.

Toegang verschaffen: De FG krijgt bij de vervulling van zijn taken toegang tot persoonsgegevens en verwerkingsactiviteiten.

Benodigde middelen: De benodigde middelen voor het vervullen van de taken van de FG en het in standhouden van zijn deskundigheid worden ter beschikking gesteld.

Scholing: De FG zal zijn vakkennis op peil moeten houden middels scholing.

Geen instructies geven: Er worden geen instructies gegeven met betrekking tot de uitvoering van de taken van de FG.

Benadelingsverbod: De FG mag door de gemeente niet worden ontslagen of gestraft voor de uitvoering van zijn taken.

Toegang tot hoogste leidinggevende: Er wordt rechtstreeks verslag uit gebracht aan de hoogste leidinggevende.

Overleg: Plan een regelmatig overleg met de hoogste leidinggevende. Ambtelijk de gemeente secretaris en bestuurlijk de portefieullehouder privacy.

Betrokkenen moeten rechtstreeks contact kunnen opnemen: Betrokkenen moeten rechtstreeks contact kunnen opnemen met de FG over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van de AVG.

Geheimhouding en vertrouwelijkheid: De FG is met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid gehouden.

Geen belangenverstrengeling: Indien de FG andere taken en plichten vervult dan mogen deze niet tot een belangenconflict leiden.

Eisen aan functionaris

Niveau van deskundigheid: Zorg dat dit in verhouding is met de gevoeligheid en complexiteit van de gegevens en organisatie.

> *Vaardigheden:* Naast diploma's en inhoudelijke kennis zijn de vaardigheden van de FG van belang. Ga goed na aan welke vaardigheden de organisatie behoefte heeft.

Professionele kwaliteit: Bij professionele kwaliteit gaat het om integriteit, ethiek en kennis.

Ervaring wetgeving: De FG moeten enige ervaring hebben met nationale en Europese wetten en praktijken op het gebied van gegevensbescherming.

Kennis bedrijfstak/organisatie: Zorg dat de FG goed bekend is met de gemeente en de taken die de de gemeente uitvoert.

Inzicht in verwerkingsactiviteiten: Voldoende inzicht hebben in de uitgevoerde verwerkingsactiviteiten, de informatiesystemen en de behoeften van de verwerkingsverantwoordelijke op het vlak van gegevensbeveiliging en gegevensbescherming. Een gemeentelijke organisatie is complex. Zorg dat de FG bekend is met de diverse gemeentelijke processen.

Kennnis administratieve regels en procedures: Gedegen kennis van de administratieve regels en procedures van de organisatie.

Vermogen om taken te vervullen: Vakinhoudelijk, de juiste competenties en ook de juiste plek in de organisatie.

Persoonlijke vaardigheden en kennis: Een FG heeft een fundamentele rol in het creëren van een cultuur van gegevensbescherming binnen de organisatie en helpt ook bij de implementatie van essentiële uitgangspunten uit de algemene verordening gegevensbescherming.

> *Competenties:* Een FG moet aan diverse competenties voldoen. Een aantal belangrijke zijn: goed kunnen communiceren, op verschillende niveaus kunnen schakelen, analytisch zijn, goede adviesvaardigheden hebben en stevig in de schoenen staan. Daarnaast is het van belang dat de FG geïnteresseerd is wetgeving en een juridische affiniteit heeft.

Positie in organisatie: Dit is een verwijzing naar zijn persoonlijke vaardigheden en kennis, maar ook de positie binnen de organisatie.

> *Staf/control:* Plaats de FG bij een staf of control afdeling. Indien mogelijk samen met de CISO.
>
> *Vervanging:* Stel een vervanger van de FG in.

6. REFLECTIE

Elk onderzoek heeft zijn beperkingen. Hieronder een reflectie en aanbeveling voor vervolgonderzoek.

Als eerste een reflectie op het veldonderzoek dat betrekking heeft op het voorbereiden van de geïnterviewden. Nadat een aantal transcripten, de letterlijke uitwerking van de bandopname, aan geïnterviewden was toezonden bleef bij een aantal geïnterviewde een reactie uit. Uit navraag bleek dat deze deelnemers geschrokken waren van de tekst en zich iets te vrij hadden uitgedrukt. Hier is extra aandacht aanbesteed door uit te leggen dat het onderzoek geen evaluatie betreft en ook niet gebruikt wordt om te kijken welke gemeente het goed of slecht doet. Daarnaast is ook de anonimiteit en niet-herleidbaarheid besproken. Voor één geïnterviewde was dit toch niet voldoende en die heeft geen akkoord op de uitgeschreven tekst gegeven. De bijdrage van deze respondent is geheel verwijderd en ook niet meegenomen in de analyse. De anderen, totaal 12, hebben akkoord gegeven. Mogelijk dat een nog betere informatievoorziening voorafgaand en tijdens het interview dit had kunnen voorkomen.

Daarnaast is er de beperking van de kwalitatieve analyse. Door Boeije (2016) wordt de kwalitatieve analyse benoemd als 'vaag' en te omschrijven als een 'nevelig karakter'. Wat er gebeurt tussen de data en conclusies is een 'black box'. Om deze vaagheid te voorkomen wordt geadviseerd om de werkwijze van de analyse te bespreken, dit is door mij in hoofdstuk 3 gedaan door in te gaan op de codering en verwerking. Door deze analyse te beschrijven wordt deze benoemde vaagheid verminderd en is de lezer van het onderzoek beter in staat om de analyse te controleren. Boeije (2016) wijst er ook op dat het een belangrijke vraag is welke informatie de lezer van een onderzoeksvraag precies nodig heeft om na te gaan of de analyse van de gegevens tot geldige bevindingen heeft geleid. Ook hier zal de omschrijving van de onderzoekanalyse en dan de codering, in paragraaf 3.2.4. de lezer duidelijkheid kunnen verschaffen.

Kijk ik naar de persoon van de onderzoeker schrijft Boeije (2016), er blijft altijd een aspect van kunst en creativiteit aan de analyse verbonden. De analyse bestaat voor een groot gedeelte over nadenken over de probleemstelling op basis van de verzamelde gegevens en de beschikbare literatuur. Dit denken kan maar op zekere hoogte worden geleerd en gestuurd (Boeije, 2016). Door tijdens de procedure steeds de onderzoeksvraag en de deelvragen in het achterhoofd te houden is getracht om de analyse hierop te concentreren. Ook de opgestelde driedeling, de taken van de functionaris voor gegevensbescherming, de eisen gesteld aan de organisatie en de eisen gesteld aan de functionaris hielp om de focus aan te brengen en is steeds als uitgangspunt in de analyse genomen.

Ten slotte zijn in dit onderzoek alleen functionarissen voor gegevensbescherming geïnterviewd. Deze insteek is gekozen om zoveel mogelijk informatie van degene die de functie uitoefenen op te halen. Het onderzoek had ook breder getrokken kunnen worden. Er zou ook bij andere medewerkers van de gemeente een interview afgenomen kunnen worden, zoals bijvoorbeeld de concerncontroller. Wat vindt die ervan om de FG in zijn afdeling op te nemen. De aanvullingen op het theoretische model zijn nu alleen afkomstig van de functionarissen van gegevensbescherming zelf. Die op dit moment voornamelijk invulling aan hun functie geven met adviestaken. Mogelijk dat andere functionarissen die al langer toezicht houden en ervaring hebben met het opstellen van toezichtskaders/plannen en het uitvoeren van audits van hulp kunnen zijn bij het verder invullen van de toezichthoudende taak van de FG. Mogelijk zou dit in vervolgonderzoek wel meegenomen kunnen worden.
Andere mogelijkheid voor vervolgonderzoek zou zijn om een evaluatie te houden. Heeft de functionaris voor gegevensbescherming daadwerkelijk gebracht wat de wetgever in Brussel ermee beoogd had toen deze functie als verplichting voor organisaties in de regelgeving is opgenomen. En dan zou het met name

interessant zijn om na te gaan of de burger een betere gegevensbescherming heeft gekregen dan voorheen.

LITERATUURLIJST

Aardema, H. (2002). *Doorwerking van BBI. Evaluatie van een veranderingsbeweging bij de Nederlandse gemeenten.* Rijksuniversiteit Groningen.

Aardema, H., & Korsten, A. F. A. (2009). Gemeentelijke organisatiemodellen - Hoe integraler het moet, hoe minder je het ziet'. In A. Bekke, C. Breed, & P. D. Jong (Eds.), *Naar een collegiaal en samenhangend overheidsbestuur* (pp. 209-227). SDU Uitgevers.

Anderson, R.J. (2006). *Tussen schakelen en switchen Over de rol van de controller in gemeentelijke organisaties.* Erasmus University Rotterdam.

Algemene Rekenkamer. (2008*). Kaders voor toezicht en verantwoording*. Ando B.V.

Autoriteit Persoonsgegevens. (2017), *Richtlijnen voor functionarissen voor gegevensbescherming*. Geraadpleegd op https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp243rev01_nl.pdf

Berkvens, J. M. A., & Prins, J. E. J. (2014*).* De bescherming van persoonsgegevens. *Recht en computer*, 179-211. Kluwer.

Boeije, H. R. (2016). *Analyseren in kwalitatief onderzoek*. Boom Lemma.

Boersma- De Jong, M., Benedictus, R., Rutkens-Oudman, L., & van Tulder, R. (2017). Control in tijden van maatschappelijke complexiteit. Van het besturen van een illusie naar het stimuleren van werkelijke impact. *Maandblad voor Accountancy en Bedrijfseconomie* 91(9/10): 308-314. Geraadpleegd op https://mab-online.nl/articles.php?id=24058

De Bruijne, M., Steenhuisen, B., & Van der Voort, H. (2015). Pas op! Over beheerst risico's beheersen in het governancetijdperk. *Bestuurskunde*, 24(3), 45–56. Geraadpleegd op https://doi.org/10.5553/bk/092733872015024003005

Centrum voor Informatiebeveiliging en Privacybescherming. (2018). *Enquête Functionarissen Gegevensbescherming Een onderzoek naar de invulling van de functie van FG in de praktijk en hoe FG's hun werk en werkomgeving ervaren.* Geraadpleegd op https://ib-p.nl/download/cip-enquete-fg/

Drahmann, A. (2019). Grip op de digitale overheid: tijd voor beginselen van behoorlijk bestuur 2.0? *Computerrecht*, 131(4), 235–236. Geraadpleegd op https://openaccess.leidenuniv.nl/bitstream/handle/1887/83347/

Drewer, D., & Miladinova, V. (2018). The canary in the data mine. *Computer Law & Security Review*, 34(4), 806–815. Geraadpleegd op https://doi.org/10.1016/j.clsr.2018.05.019

Dijck, J., Poell, T., Waal, M., van Dijck, J., & de Waal, M. (2016). *De platformsamenleving*. Amsterdam University Press.

Engelfriet, A., & Chew-Meij, L. K. P. (2017). *Handboek - De Algemene Verordening Gegevensbescherming (GDPR)*. Ius Mentis Amsterdam.

Geschillenkamer Gegevensautoriteit 28 april 2020, AH-2019-0013.

Groep gegevensbescherming artikel 29 (2017). *Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO).* Geraadpleegd op https://ec.europa.eu/newsroom/article29/items/612048

Helden, G.J. van, Jansen, E.P. (2002), New Public Management in Dutch Local Government, Rijksuniversiteit Groningen.

Hood, C.C. (1995), Contempory public management: a new global paradigm?, *Public Policy and Administration*, 10.

Hood, C. (1991). A public management for all seasons?, *Public Administration*, 69(1), 3–19. Geraadpleegd op https://doi.org/10.1111/j.1467-9299.1991.tb00779.x

Informatiebeveiligingsdienst. (2020) *Baseline Informatiebeveiliging Overheid (BIO) ed. 1.04*. Geraadpleegd op https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

Institute van Internal Auditors. (2013). The Three Lines of Defense in Effective Risk Management and Control - IIA position paper. Geraadpleegd op https://www.iia.nl/actualiteit/nieuws/the-three-lines-of-defense-in-effective-risk-management-and-control--iia-position-paper

Kadir, R. F. (2018). *Praktijkboek functionaris voor gegevensbescherming*. SDU uitgevers.

Meijer, A., Schäfer, M. T., & Branderhorst, M. (2019). Principes voor goed lokaal bestuur in de digitale samenleving. *Bestuurswetenschappen*, 73(4), 8–23. Geraadpleegd op https://doi.org/10.5553/bw/016571942019073004003

Moore, M. H. (1995). *Creating Public Value*. Harvard University Press.

Rathenau Instituut. (2017). *Opwaarderen. Borgen van publieke waarden in de digitale samenleving.* Geraadpleegd op https://www.rathenau.nl/nl/digitale-samenleving/opwaarderen

Robertson, B.J. (2015) *Holacracy: The new management system for a rapidly changing world.* New York: Henry Holt and Company.

Ross, David. "GDPR and the Role of the Data Protection Officer." *Risk Management*, vol. 65, no. 9, Oct. 2018, p. 16+. Gale Academic OneFile. Geraadpleegd op https://go.gale.com/ps/anonymous?id=GALE%7CA558823701&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00355593&p=AONE&sw=w

Ruimschotel, D. (2014). *Goed toezicht*. Mediawerf Amsterdam.

Schindler, P. S. (2019). *Business research methods*. 13th ed. McGraw-Hill/Irwin.

Schuiling, K. F., & Winter, H. B. (1997). Juridische controlling in opkomst. *Gemeentestem*, 2, 1–5.

Turnbull, N & Hoppe, R (2018): Problematizing 'wickedness': a critique of the wicked problems concept, from philosophy to practice, *Policy and Society*. doi: 10.1080/14494035.2018.1488796

Tweede Kamer (2000-2001). *Kaderstellende Visie op Toezicht* nr. 27831, nr. 1. Geraadpleegd op https://zoek.officielebekendmakingen.nl/kst-27831-1.html

Tweede Kamer (2005-2006), *Minder last, meer effect zes principes van goed toezicht* bijlage bij 27831 nr. 15. Geraadpleegd op https://zoek.officielebekendmakingen.nl/kst-27831-15-b1

Velden, H.P.F. van der (2002), De ‘losse’ controller, *ControllersMagazine*.

VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming). Geraadpleegd op https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679

Verhoeven, N. (2018). *Wat is onderzoek?* Boom Lemma.

Vosselman, E.G.J. (2011) *Rekenschap en management control in de publieke sector: hoofdweg, dwaalweg en uitweg.* Vrije universiteit.

Vosselman, E. G. J. (2012). Control in de moderne overheidsorganisatie: van opportunistische agenten naar betrouwbare stewards. *Tijdschrift voor Public Governance, Audit & Control*, 5, 4-8.

Winter, H.B., & Mein, A.G. (2017). De staat van toezicht en handhaving door gemeenten. *Gemeentestem*, (2017)7464, 938-934.

Wolters, P.T.J. (2017) De rechten van de betrokkenen onder de AVG, *Tijdschrift voor Consumentenrecht en Handelspraktijken*, 2018, 3, pp. 130-140.

BIJLAGE A

Uitnodiging tot onderzoek

Beste functionaris voor gegevensbescherming,

Ik mail als collega FG met een verzoek.

Mijn naam is Angelique Schepers, ik ben teammanager juridische zaken en ook functionaris voor gegevensbescherming bij de gemeente Zoetermeer. Naast mijn werkzaamheden voor de gemeente volg ik bij de universiteit Twente de master public management. Voor mijn eindthesis heb ik als onderwerp de functionaris voor gegevensbescherming.

Met mijn onderzoek wil ik een model ontwerpen. Een model voor de middelgrote gemeente met uitgangspunten voor de organisatie en de functionaris voor gegevensbescherming waar minimaal aan voldaan moet worden om te komen tot een zo goed mogelijke taakuitoefening.

Als definitie van middelgrote gemeente ben ik aangesloten bij de deelnemers van de G40-gemeenten. Van de 40 gemeenten die deelnemen in dit overleg zou ik er 10 willen interviewen voor mijn onderzoek. Vanuit een steekproef ben ik bij jouw gemeente uitgekomen.

Het doel van het interview is om te achterhalen hoe bij jouw gemeente invulling wordt gegeven aan de uitgangspunten zoals opgenomen in de regelgeving.

Een voorbereiding is niet noodzakelijk. Hieronder een aantal onderwerpen waar ik op in zou willen gaan.

- Ben je full time FG of combineer je het met andere werkzaamheden?
- Hoe is dit binnen jouw gemeente georganiseerd?
- De indeling van de organisatie.
- Waar ben jij als FG binnen gepositioneerd?
- Waaruit bestaan jouw werkzaamheden merendeels, advies of toezicht?
- Hoe ga je om met de verschillende rollen?
- Aan welke persoonlijke eigenschappen moet een FG voldoen?

(mocht je willen meewerken zal ik voorafgaand aan het interview nog meer informatie toezenden)

Het interview zal 1 uur duren en zou ik graag via Microsoft-teams of telefonisch afnemen.

Mijn verzoek is, zou je hieraan willen meewerken?

Met vriendelijke groet,

mr. A. (Angelique) Schepers

teammanager Juridisch en Inkoop, afdeling Jabo

& functionaris voor gegevensbescherming

Gemeente Zoetermeer

BIJLAGE B

Toegezonden informatie voorafgaand interview

Beste (naam),

Hartelijk bedankt dat je wilt meewerken aan mijn onderzoek.

Voor mijn masterthesis van de opleiding Master Public Management aan de universiteit van Twente doe ik een onderzoek naar de functionaris voor gegevensbescherming binnen de gemeentelijke organisatie. Het doel van het onderzoek is om te komen met een model met hierin opgenomen de uitgangspunten waar de organisatie en functionaris voor gegevensbescherming minimaal aan moeten voldoen om te komen tot een juiste taakuitvoering.

Doel interview

Het doel van het interview is om te achterhalen hoe jij invulling geeft aan de uitgangspunten zoals gegeven in de regelgeving. Deze uitgangpunten zijn in bijgevoegde figuur opgenomen. Daarnaast ben ik benieuwd of de eisen zoals gesteld in de regelgeving voldoen of dat die nog aangevuld moeten worden.

Verwachte vragen

- Een voorbereiding is niet noodzakelijk. Ik zal een aantal algemene dingen willen weten zoals:
- Ben je full time FG of combineer je het met andere werkzaamheden?
- Hoe is dit binnen de gemeente georganiseerd?
- De indeling van de organisatie (directiestructuur of dienstenmodel).
- Waar ben jij als FG binnen gepositioneerd (staf of onderdeel van een afdeling)?
- Waaruit bestaan jouw werkzaamheden merendeels, advies of toezicht?
- Hoe ga je om met de verschillende rollen?
- Aan welke persoonlijke eigenschappen moet een FG voldoen?

Ik gebruik hiervoor de uitgangspunten zoals in het schema hieronder opgenomen.

Proces

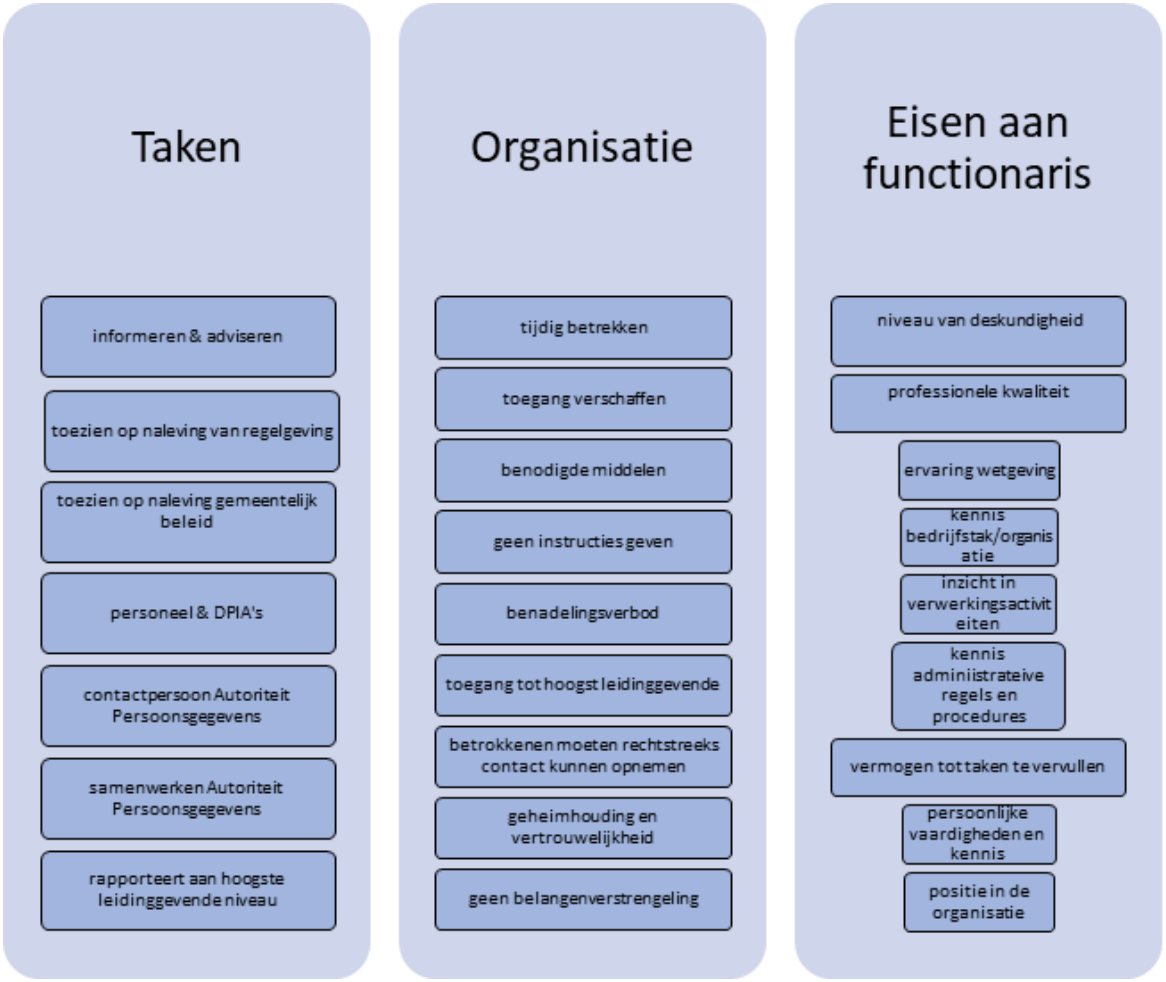
Van het interview zal middels de dictafoon een geluidsopname worden gemaakt. Deze wordt slechts gebruikt voor de uitwerking van het interview. Na uitwerking van het interview zal ik je die voorleggen met het verzoek of het een juiste weergave van het gesprek is. Na jouw akkoord op het uitgewerkte verslag zal ik de bandopname verwijderen.

Anonimiteit

In de verslaglegging van het gesprek zal alleen de gemeente genoemd worden en dit verslag wordt alleen gebruikt ter verantwoording aan de universiteit. In mijn onderzoeksrapport zal in de bijlage een lijst worden opgenomen van deelnemende gemeenten. In het rapport zelf zullen de gemeenten en de geïnterviewden niet bij naam genoemd worden. Ik zal bij totaal 10 gemeenten interviews afnemen.

Als er voorafgaand nog vragen zijn dan hoor ik het graag.

Figuur: Uitgangspunten regelgeving.



Met vriendelijke groet,

Angelique Schepers

Teammanager Juridische Aangelegenheden & Bestuursondersteuning

Functionaris Gegevensbescherming

BIJLAGE C

Interview schema

Vragen & Uitwerkingen
Algemene informatie: Naam: Gemeente: Wijze van interview: In- of extern: Hoelang in dienst: Opleiding: Achtergrond:
Vraag: Ben je Full time FG? **Indien niet fulltime bij de betreffende gemeente:** **Deelvraag:** Welke werkzaamheden doe je er naast?
Vraag: Kan je iets meer vertellen over de organisatie? **Deelvraag:** Inrichting, directie/dienstenstructuur?
Vraag: Waar ben je in de organisatie gepositioneerd?
Vraag: Waaruit bestaan jouw werkzaamheden als FG? **Deelvraag:** Hoe ga je om met de verschillende rollen advies en toezicht (is er ook sprake van rollenconflict)?
Schema doornemen:
toezien op naleving van regelgeving

Deelvraag: Zie je meer als adviseur of als toezichthouder
Deelvraag: Waaruit bestaan je werkzaamheden als adviseur.
Deelvraag: Waaruit bestaan jouw werkzaamheden als toezichthouder.
Deelvraag: Houd je ook toezicht bij externe partijen?
Subvraag: bv ICTsysteemchecks en
Subvraag: Audits op de dienstverlening door ICT bedrijven (ISAE 3402, EDP auditing)

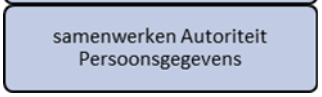
Vraag: doe je aan risicogedreven toezicht?
Deelvraag: hoe bepaal je de risico's

Vraag: Vind je informeren & adviseren en toezien op de naleving van regelgeving in één functie passen?

Vraag: Wie is er verantwoordelijk voor het privacybeleid?
Vraag: Is er toezichtsbeleid? Wie schrijft dit?
Deelvraag: Is er een jaarplan, waar wordt extra aandacht aan besteed.

Vraag: Doordat jij FG bent is er dan binnen de organisatie verschil met dat er geen FG/toezicht zou zijn.
Deelvraag: wat zou er anders zijn met dat jij er niet bent/of is er nu extra.

Vraag: Wat zijn jouw acties richting het personeel?
Vraag: Voer je zelf DPIA's uit?
Deelvraag: Hoeveel per jaar ongeveer.



Vraag: Zie je jezelf als een verlengstuk van de AP?
Vraag: Hoe vaak heb je het afgelopen jaar contact gehad (zelf of door AP)?
Deelvraag: Over wat voor zaken?

Vraag: Wie zijn nog meer je samenwerkingspartners?

rapporteert aan hoogste leidinggevende niveau **Vraag:** Wie zie je als hoogste leidinggevende niveau? **Deelvraag:** Heb je makkelijk toegang tot deze persoon? **Vraag:** Aan wie rapporteer je?
tijdig betrekken **Vraag:** Word je tijdig betrokken bij relevante zaken in de organisatie? **Vraag:** Waar word je niet bij betrokken en zou je wel betrokken moeten worden. **Vraag:** Word je betrokken bij (Europese aanbestedingen voor ICT toepassingen?)
toegang verschaffen **Vraag:** Heb je daadwerkelijk toegang tot alle benodigde systemen.
benodigde middelen **Vraag:** Beschik je over de benodigde middelen? **Vraag:** Welke middelen zijn cruciaal? **Vraag:** Welke middelen mis je nog?
geen instructies geven **Vraag:** Ontvang je instructies over de uitvoering van je werkzaamheden? **Vraag:** indien ja, welke
benadelingsverbod **Vraag:** Heb je hier ervaring mee, dat je benadeeld wordt omdat je FG bent.
geen belangenverstrengeling **Vraag:** Heb je hier last van? **Deelvraag:** zijn er conflicterende werkzaamheden?
Eisen aan functionaris

professionele kwaliteit **Vraag:** Wat is het minimumniveau HBO/WO? **Vraag:** Moet er een verplichte opleiding worden gevolgd? **Deelvraag**: Indien Ja, welke?
vermogen tot taken te vervullen **Vraag:** Wat moet er nog in organisatie gebeuren zodat jij je functie goed kan uitoefenen.
persoonlijke vaardigheden en kennis **Vraag:** Over welke persoonseigenschappen/vaardigheden moet een functionaris voor gegevensbescherming voldoen.