AUTORITEIT
PERSOONSGEGEVENS

<Onderzoeksrapport>

Hoe opereert de FG in het ziekenhuis?

Onderzoek naar de positie en taakuitoefening van functionarissen voor de gegevensbescherming in elf ziekenhuizen

Juni 2019

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

1. Inleiding en achtergronden

De functionaris voor de gegevensbescherming (FG) heeft een belangrijke rol in de naleving van de nieuwe Algemene verordening gegevensbescherming (AVG) door organisaties. De FG is binnen organisaties adviseur en toezichthouder op het gebied van privacy. Als de FG-functie binnen een organisatie goed is ingebed, dan bevordert dat de naleving van de AVG. Daarbij is uiteindelijk de patiënt gebaat. Goed functionerende FG's zijn de "oren en ogen" van de Autoriteit persoonsgegevens (AP) binnen organisaties. De AP hecht daarom veel waarde aan de taken en de rol van de FG.

De rol van de FG binnen ziekenhuizen wordt in de toekomst alleen maar groter. Ziekenhuizen krijgen steeds meer te maken met medisch-technologische ontwikkelingen en de daarmee samenhangende digitalisering. Deze ontwikkelingen bieden volop kansen voor de patiëntenzorg, maar doen tegelijkertijd een groot beroep op de ziekenhuizen om een hoog beschermingsniveau te blijven bieden ten aanzien van de verwerking van medische persoonsgegevens. Als ziekenhuizen meer datagedreven gaan werken en het volume van dataverwerkingen toeneemt, vraagt dat extra aandacht voor de bescherming van patiëntgegevens. Ziekenhuizen zijn zelf verantwoordelijk om hierover na te denken en hun handelen daarop af te stemmen. Deze eigen verantwoordelijkheid is een belangrijk uitgangspunt in de AVG ('accountability'). De FG speelt hierin – als adviseur en toezichthouder – een onmisbare rol.

In augustus 2018 heeft de AP onderzoek gedaan naar de vraag of ziekenhuizen en zorgverzekeraars conform de verplichtingen uit de AVG een FG hebben aangesteld en aangemeld bij de AP. Inmiddels heeft elk ziekenhuis een FG aangesteld. Nu in ieder ziekenhuis in Nederland een FG actief is, heeft de AP onderzoek gedaan naar de positionering en het functioneren van FG's. De AP heeft onderzocht hoe de positie van FG's is ingebed binnen ziekenhuizen en hoe FG's invulling geven aan hun taken op grond van de AVG.

De aard van het onderzoek is verkennend. De AP heeft een algemeen beeld willen krijgen. Het vaststellen van overtredingen en het treffen van handhavingsacties zijn in dit onderzoek niet aan de orde. In het onderzoek staan de volgende hoofdvragen centraal:

1. Hoe geven ziekenhuizen vorm en invulling aan de AVG-verplichting om een FG aan te stellen?
2. Hoe geven FG's binnen ziekenhuizen invulling aan hun functie en taken op grond van de AVG?

Het rapport bevat ook tips en aanbevelingen voor de praktijk. Deze aanbevelingen zijn gebaseerd op de schriftelijke inlichtingen die de AP van de elf onderzochte ziekenhuizen heeft ontvangen en op de gesprekken die de AP bij vijf ziekenhuizen heeft gehad. Zij vormen een aanvulling op de aanbevelingen in de richtlijn van de voormalige Artikel 29-werkgroep over de FG.[1] Van belang is om te realiseren dat dit uitsluitend *best practices* zijn, die het goede functioneren van de FG binnen het ziekenhuis kunnen bevorderen. Het gaat dus niet om verplichtingen die bovenop de wettelijke regels gelden.

Leeswijzer

Hoofdstuk 2 bevat de conclusies en aanbevelingen. In hoofdstuk 3 legt de AP uit hoe zij het onderzoek heeft aangepakt en uitgevoerd. Hoofdstuk 4 bevat de bevindingen van het onderzoek. In de eerste bijlage is een weergave gegeven van de relevante wettelijke bepalingen. Daarnaast bevat die bijlage een samenvatting van de richtlijnen van de voormalige Artikel 29-werkgroep. In de tweede bijlage zijn de vragenlijsten aan de raden van bestuur en de FG opgenomen.

[1] Article 29 Data Protection Working Party, *Guideluines on Data Protection Officers ('DPOs')*, aangenomen op 13 december 2016, laatstelijk gewijzigd op 5 april 2017, te raadplegen op www.autoriteitpersoonsgegevens.nl..

2. Conclusies en aanbevelingen

De FG speelt een belangrijke rol in de naleving van de AVG door ziekenhuizen. Deze adviserende en toezichthoudende rol wordt steeds belangrijker vanwege de medisch-technologische ontwikkelingen waarmee ziekenhuizen te maken hebben. De AP heeft onderzoek verricht naar de positionering en functieuitoefening van FG's binnen elf ziekenhuizen in Nederland.[2]

De algemene conclusie van de AP is dat FG's goed op weg zijn om een volwaardige positie binnen de ziekenhuizen te verwerven. De AP is tevreden over de wijze waarop FG's binnen ziekenhuizen opereren en hoe zij invulling geven aan hun taken op grond van de AVG. Dit alles moet in sommige ziekenhuizen wel nog beter schriftelijk worden verankerd.

Meer concreet trekt de AP de volgende conclusies:

1 Het beeld van de AP is dat raden van bestuur van de onderzochte ziekenhuizen de FG-functie op een AVG-conforme wijze hebben ingebed binnen de organisatie. FG's kunnen hun werk onafhankelijk uitvoeren en hebben voldoende middelen tot hun beschikking. FG's en raden van bestuur zijn tevreden over hun onderlinge contact en afstemming.

2 Van de onderzochte ziekenhuizen hebben de kleinere ziekenhuizen onvoldoende schriftelijk vastgelegd wat de positie, taken en bevoegdheden van de FG's zijn en wat de verhouding is tussen de FG's en andere commissies en functionarissen die zich bezighouden met privacy en gegevensbescherming. Bij grotere en academische ziekenhuizen is dit beter op orde.

3 Het beeld van de AP is dat de FG's van de onderzochte ziekenhuizen hun wettelijke rol goed oppakken. De FG's van de onderzochte ziekenhuizen hebben een belangrijke rol gespeeld bij de implementatie van de AVG en houden zich actief bezig met het creëren van bewustwording op het gebied van privacy. Daarnaast is er sprake van gevraagde en ongevraagde advisering van FG's aan de raden van bestuur. Adviezen van de FG worden door de raden van bestuur van de onderzochte ziekenhuizen opgevolgd. In alle onderzochte ziekenhuizen is de FG betrokken bij DPIA's[3] en datalekken. In de helft van de onderzochte ziekenhuizen is de FG belast met het opstellen en bijhouden van het register van verwerkingsactiviteiten. Alle FG's worden betrokken bij klachten van patiënten over privacy-aangelegenheden.

4 De FG geldt vaak als dé privacy-vraagbaak van raad van bestuur en medewerkers op de werkvloer. Daardoor ligt in de praktijk het accent meer op de adviserende dan op de toezichthoudende rol.

[2] Dit betreft ongeveer 10% van alle ziekenhuizen in Nederland.
[3] DPIA is een Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling) als bedoeld in artikel 35 AVG.

Aanbevelingen aan de raden van bestuur:

1 Stel interne regels en richtlijnen vast over de positie van de FG of werk dit uit in het interne privacybeleid. Maak in die stukken duidelijk wat de taken, werkzaamheden en bevoegdheden van de FG zijn en de afbakening en verhouding met andere privacy-gerelateerde functies. Waarborg in die stukken ook dat de FG geen taken krijgt toebedeeld die conflicteren met de functie van FG.

2 Besef dat de raad van bestuur verantwoordelijk is voor de naleving van privacywetgeving. Zorg ervoor dat FG's voldoende middelen krijgen om hun werk goed te kunnen doen, ten behoeve van de privacycompliance. Laat aan de organisatie zien dat het werk van FG's belangrijk is en gedragen wordt door de raad van bestuur.

3 Zoek zelf actief contact met de FG. Laat dit niet uitsluitend over aan een manager of secretaris.

Aanbevelingen aan FG's:

4 Houd een goede balans tussen adviserende en toezichthoudende taken. Probeer meer aandacht te besteden aan de toezichthoudende rol.

5 Voorkom dat de adviserende en de toezichthoudende rol met elkaar conflicteren. Maak binnen de organisatie duidelijk welke rol je wanneer inneemt. Regel ook hoe te handelen als er daadwerkelijk sprake is van een belangenconflict.

6 Maak duidelijke interne afspraken over de verdeling van verantwoordelijkheden en de rol van de FG, bijvoorbeeld als zich een datalek voordoet.

7 Zoek als FG het contact met de werkvloer en ga het gesprek aan. Wees zichtbaar binnen de organisatie. Zichtbaarheid zorgt ervoor dat medewerkers de FG aanspreken en dat de FG signalen ontvangt over knelpunten in de naleving van de AVG.

8 Zoek contact en wissel ervaring en kennis uit met andere FG's in de regio of bij andere zorgaanbieders in het land. Veel FG's hebben te maken met dezelfde problematiek en vaak hoeft het wiel niet opnieuw te worden uitgevonden. Leer van elkaar!

3. Onderzoeksmethode en aanpak

In dit hoofdstuk legt de AP uit hoe zij het onderzoek heeft aangepakt.

Uitgangspunt voor het onderzoek is het juridisch kader omtrent de FG. Dit juridisch kader wordt gevormd door artikel 37 tot en met 39 van de AVG. Daarnaast heeft de AP de *guidelines* over de FG van de gezamenlijke Europese toezichthouders (de voormalige Artikel 29-werkgroep) bij het onderzoek betrokken.[4] Bijlage 1 bevat een samenvatting van het juridische kader.

De AP heeft een willekeurige selectie gemaakt van negen (van de circa negentig) algemene en STZ-ziekenhuizen[5] en twee (van de acht) academische ziekenhuizen. De ziekenhuizen zijn evenredig verdeeld naar omvang en zijn geografisch verspreid over Nederland.

De AP heeft de geselecteerde ziekenhuizen in eerste instantie benaderd met schriftelijke vragen. Deze vragen hebben in grote lijn betrekking op de verplichting die ziekenhuizen hebben om een FG aan te stellen (artikel 37 AVG), de eisen die gelden voor de positie van de FG binnen een ziekenhuis (artikel 38 AVG) en de wettelijke taken van de FG (artikel 39 AVG). Er zijn afzonderlijke vragenlijsten opgesteld voor de FG's en voor de raden van bestuur. De vragenlijsten zijn opgenomen in bijlage 2 bij dit rapport.

Mede aan de hand van de schriftelijke reacties heeft de AP een selectie gemaakt van vijf ziekenhuizen waar de AP is langsgegaan voor een verdiepend interview. De AP heeft bij de keuze van de bezochte ziekenhuizen rekening gehouden met de omvang en de geografische spreiding van die vijf ziekenhuizen. Tijdens de bezoeken heeft de AP interviews afgenomen met (een afvaardiging van) de raad van bestuur en met de FG. De interviews met de raad van bestuur en de FG hebben telkens afzonderlijk van elkaar plaatsgevonden.

De AP aan de ziekenhuisbesturen en FG's ook gevraagd welke verwachtingen zij van de AP hebben en ten aanzien van welke onderwerpen zij behoefte hebben aan extra voorlichting.

[4] Article 29 Data Protection Working Party, *Guideluines on Data Protection Officers ('DPOs')*, aangenomen op 13 december 2016, laatstelijk gewijzigd op 5 april 2017, te raadplegen op www.autoriteitpersoonsgegevens.nl.
[5] STZ-ziekenhuizen zijn samenwerkende topklinische ziekenhuizen, die ook medisch-specialisten mogen opleiden. Doorgaans zijn dit de grotere ziekenhuizen. Er zijn 26 STZ ziekenhuizen in Nederland.

4. Bevindingen

4.1 Aanstelling en positie van de FG binnen het ziekenhuis

4.1.1 De inbedding van de functie in het ziekenhuis en vastlegging daarvan in documenten

In alle onderzochte ziekenhuizen heeft de FG een aanstellingsbrief of een arbeidsovereenkomst ondertekend, waarin de aanstelling van de FG is vastgelegd. In de meeste ziekenhuizen bedraagt de invulling van de functie 24-36 uur per week. In vier van de elf ziekenhuizen is extern een FG geworven; in zeven van de elf ziekenhuizen betreft het een interne benoeming. In acht van de elf onderzochte ziekenhuizen is er naast een FG ook een Chief Information Security Officer (CISO). In drie van de elf ziekenhuizen is er alleen een FG.

In sommige ziekenhuizen is er een uitgebreide functieomschrijving van de FG aanwezig die als bijlage bij de aanstellingsbrief of arbeidsovereenkomst is gevoegd. Uit het onderzoek is gebleken dat voornamelijk de grotere ziekenhuizen de functie, taken en bevoegdheden van de FG gedetailleerd hebben omschreven in hun privacybeleid. In zoverre is het functioneren en de positie van de FG onderdeel van het algehele privacybeleid. In kleinere ziekenhuizen lijkt hiervan minder sprake. De positie van de FG wordt weliswaar omschreven in het privacybeleid, maar de verhouding met andere functionarissen en commissies met privacy en informatiebeveiliging als aandachtsgebied is vaak onduidelijk. Ook de inbedding van de FG in het gehele privacybeleid wordt vaak niet gedetailleerd toegelicht. De twee academische ziekenhuizen beschikken over een uitgebreider en completer privacybeleid, waarin de inbedding van de FG is opgenomen en beschreven. Ook geven zij een gedetailleerde beschrijving van de werkzaamheden, de onafhankelijkheid, de taken en de bevoegdheden van de FG.

In de meeste onderzochte ziekenhuizen is de FG organisatorisch ondergebracht bij een afdeling die verantwoordelijk is voor ICT of voor kwaliteit en veiligheid. In de kleinere ziekenhuizen heeft de FG vaak rechtstreeks contact met de raad van bestuur. In grotere ziekenhuizen betekent deze organisatorische inbedding vaak ook dat de managers van die betreffende afdelingen het eerste aanspreekpunt zijn voor de FG. In een enkel ziekenhuis is de secretaris van de raad van bestuur de eerste die door de FG wordt aangesproken. Dit doet overigens niet af aan het rechtstreekse contact dat er bestaat tussen FG en raad van bestuur. De FG's hebben – indien nodig – direct toegang tot en contact met de raad van bestuur. De FG en management informeren de raad van bestuur door middel van kwartaalrapportages, periodieke datalekrapportages en jaarverslagen, waarin aandacht wordt besteed aan privacybeleid. De FG's en raden van bestuur zijn van mening zijn dat er voldoende informatie over en weer met elkaar wordt gedeeld. In kleine ziekenhuizen zijn de lijnen korter dan in grotere ziekenhuizen. In grote(re) ziekenhuizen verloopt het contact en informatietraject vaker langs een manager van de afdeling waar de FG hiërarchisch onder is 'gehangen'.

De aanstelling en taken van de FG zijn op verschillende manieren bekendgemaakt, meestal door middel van een vermelding op het intranet of in de interne nieuwsbrief en vermelding in het interne en externe privacybeleid van het ziekenhuis. Ten tijde van de inwerkingtreding van de AVG is er meer aandacht geschonken aan het bekendmaken van de FG door middel van een speciale campagne. Vaak heeft de FG een ronde gemaakt in het ziekenhuis langs verschillende afdelingen.

4.1.2 Deelname FG in werkgroepen

In alle ziekenhuizen maakt de FG deel uit van relevante interne overlegorganen of commissies die zich richten op de onderwerpen informatiebeveiliging en gegevensbescherming. Dit loopt uiteen van tijdelijke commissies die opgericht zijn voor de implementatie van de AVG of de inrichting van bijvoorbeeld een elektronisch patiëntendossier tot commissies met een structureler karakter, zoals een autorisatie- en privacycommissie of een commissie die zich bezighoudt met medisch-wetenschappelijk onderzoek.

Als een ziekenhuis beschikt over een CISO en/of een ziekenhuisjurist, dan is er structureel overleg tussen hen en de FG. Uit de reacties van de ziekenhuizen is af te leiden dat dit vaker het geval is in grotere ziekenhuizen simpelweg omdat die in de regel beschikken over dergelijke functionarissen. In sommige ziekenhuizen is de FG voorzitter van een commissie en bepaalt de FG vanuit deze rol de agenda. Geen van de FG's in ziekenhuizen die wij gesproken hebben, ervaart deelname in een commissie als een belemmering of aantasting van hun onafhankelijke positie.

4.1.3 Overleg met de raad van bestuur

In alle ziekenhuizen heeft de FG de mogelijkheid om direct in contact te treden met de raad van bestuur. Toch blijkt dat er in de praktijk niet overal eenzelfde invulling aan gegeven wordt. In de kleinere ziekenhuizen zijn de lijnen korter en vindt er vaak direct en structureel overleg plaats met (een lid van) de raad van bestuur. In de grotere ziekenhuizen is er vaker in eerste instantie overleg tussen de FG met een manager of met de secretaris van de raad van bestuur.

De frequentie van het overleg met de raad van bestuur is bij de ziekenhuizen verschillend en schommelt tussen tweemaandelijks en driemaal per jaar. Ook blijkt dat er tijdens een overleg met de raad van bestuur andere collega's aanschuiven, zoals een privacy-officer of een ziekenhuisjurist. Vaak stelt de raad van bestuur de agenda van het overleg met de FG op , waardoor de raad van bestuur indirect bepaalt bij welk agendapunt de FG aanschuift. Indien de FG wordt uitgenodigd ontvangt die tijdig de benodigde stukken.

De onderzochte ziekenhuizen merken op dat de adviezen van de FG in vrijwel alle gevallen geheel of gedeeltelijk door de raad van bestuur worden overgenomen. Bij verschillen van inzicht krijgen de FG's altijd de mogelijkheid hun afwijkende mening kenbaar te maken. Als het besluit van de raad van bestuur afwijkt van het advies van de FG, dan voorziet de gangbare werkwijze binnen ziekenhuizen erin dat dat schriftelijk wordt vastgelegd, meestal in de notulen van bestuursvergaderingen. Het is de AP in dit onderzoek niet gebleken dat een dergelijke situatie zich heeft voorgedaan.

"Wij nemen de adviezen van de FG altijd zeer serieus"

- lid raad van bestuur van één van de onderzochte ziekenhuizen -

4.1.4 Onafhankelijkheid van de FG

Schriftelijke waarborgen

Alle raden van bestuur en de FG's van de onderzochte ziekenhuizen zijn zich bewust van de wettelijk verplichte onafhankelijke positie van de FG binnen de organisatie. Nagenoeg alle ziekenhuizen hebben de onafhankelijkheid van de FG schriftelijk vastgelegd in de arbeidsovereenkomst met de FG of in de functieomschrijving van de FG. Een enkel ziekenhuis heeft die onafhankelijkheid nog eens benadrukt in een afzonderlijke memo aan de FG. Een aantal (kleine) ziekenhuizen is van mening dat de onafhankelijkheid van de FG niet afzonderlijk in de arbeidsovereenkomst hoeft te worden opgenomen, omdat dit reeds in de AVG is bepaald.

Voorkomen van belangenconflicten

De meeste onderzochte ziekenhuizen hebben geen nadere interne regels of afspraken gemaakt om belangenconflicten te vermijden. Een aantal ziekenhuizen geeft daarvoor als reden dat de FG geen nevenfuncties vervult en dus in de praktijk niet te maken krijgt met belangenconflicten. In één ziekenhuis is in de aanstellingsbrief expliciet bepaald dat de FG geen taken opgelegd krijgt die kunnen leiden tot belangenconflicten. Daarnaast heeft één FG een "Verklaring van persoonlijke onafhankelijkheid" ondertekend.

Zoals de AP in paragraaf 4.1.1 van dit rapport heeft aangegeven, komt het in de praktijk voor dat de FG onderdeel uitmaakt van een afdeling die organisatorisch en hiërarchisch valt onder een afzonderlijke manager. Geen van de FG's ervaart een dergelijke constructie als een (mogelijke) aantasting van de onafhankelijkheid. In de grotere ziekenhuizen komt het vaker voor dat de FG direct aan de manager rapporteert en/of werkoverleggen met deze manager voert. Deze overleggen gaan vaak over dagelijkse werkzaamheden, meldingen met relatief laag privacyrisico, incidenten, de stand van zaken ten aanzien van verwerkingsregisters, advies- en beleidsstukken en lopende projecten. De manager heeft vervolgens zelf periodiek overleg met de raad van bestuur en doet aldaar verslag. De AP heeft op basis van de documentatie en de gevoerde gesprekken geen aanleiding om aan te nemen dat de onafhankelijkheid van FG's in een dergelijke organisatorische constellatie in de knel komt. In dat verband is mede van belang dat de AP heeft vastgesteld dat er in alle gevallen hoe dan ook rechtstreeks contact mogelijk is tussen FG en raad van bestuur.

Meerdere/onverenigbare functies

Op één ziekenhuis na vervult de FG bij de onderzochte ziekenhuizen geen andere functies binnen het ziekenhuis. Gelet hierop vinden de ziekenhuizen het ook niet nodig om expliciet vast te leggen welke functies onverenigbaar zijn met de FG-rol. Bovendien vinden de ziekenhuizen dat hiermee ook feitelijk de onafhankelijkheid van de FG is gewaarborgd, ook al is dat niet schriftelijk vastgelegd in interne beleidsdocumenten. In één van de kleine ziekenhuizen vervult de FG naast deze functie ook de functie van risicomanager en manager medische techniek. In een ander (middelgroot) ziekenhuis was tijdelijk een externe FG werkzaam die tevens de rol van ISO vervult, maar hierin komt binnenkort verandering.

Voorkomen van instructies van het bestuur en ontslagbescherming

Geen van de FG's in dit onderzoek heeft aangegeven inhoudelijke instructies van de raad van bestuur of managers te ontvangen. De meeste ziekenhuizen hebben hierover niets in interne documentatie vastgelegd, omdat de AVG dat al regelt. Hetzelfde geldt voor de ontslagbescherming van de FG. Een aantal ziekenhuizen geeft overigens aan te overwegen om die onderwerpen in de toekomst toch op te nemen in intern beleid.

4.1.5 De middelen voor FG's binnen ziekenhuizen

In het algemeen zijn FG's tevreden over de beschikbaarheid van middelen voor de uitoefening van hun functie. Dit loopt uiteen van fysieke werkruimte en gebruiksvoorwerpen tot de toegang tot systemen of de ondersteuning van c.q. samenwerking met andere collega's. In alle onderzochte ziekenhuizen hebben de FG's voldoende effectieve toegang tot de verwerkingsactiviteiten en relevante diensten binnen de organisatie. Daarnaast worden alle FG's van de onderzochte ziekenhuizen in de gelegenheid gesteld om relevante informatiebijeenkomsten en symposia te bezoeken en gebruik te maken van opleidingsmogelijkheden. Uit de beantwoording maakt de AP op dat de FG's hiervan gebruik maken. Wel geeft één FG aan behoefte te hebben aan de aanschaf van *tooling* voor ondersteuning bij (inhoudelijke) werkzaamheden, zoals voor het opstellen en bijhouden van het verwerkingenregister.

Veel FG's hebben contact en vakinhoudelijk overleg met collega-FG's van ziekenhuizen en/of andere zorgaanbieders in de regio. Een aantal FG's is actief lid van de NGFG en deelt in dat verband hun ervaringen en kennis met andere FG's. Ziekenhuisbestuurders stimuleren hun FG om aan dergelijke initiatieven en netwerken deel te nemen.

Van de onderzochte ziekenhuizen geven de meeste FG's aan nauw samen te werken met – voor zover aanwezig – de (C)ISO, ICT-specialisten, privacy officer(s), juristen en andere collega's. Desondanks geeft ongeveer een derde van de FG's aan behoefte te hebben aan (meer) ondersteunend personeel voor het borgen van de privacybescherming binnen het ziekenhuis, vaak vanwege de toegenomen werkdruk. De meeste van deze FG's geven bovendien aan dat zij behoefte hebben aan een privacy-officer voor de uitvoerende taken en/of een informatiebeveiligingsspecialist ((C)ISO).

De meeste ziekenhuizen bieden zo nodig de mogelijkheid voor de FG om aanvullende capaciteit, faciliteiten en budget aan te vragen. Sommige FG's hebben daarvoor een eigen budget, maar bij de meeste onderzochte ziekenhuizen dient daartoe een verzoek te worden gedaan bij de raad van bestuur of de verantwoordelijk manager.

4.1.6 Conclusies

- Het algemene beeld van de AP is dat raden van bestuur van de onderzochte ziekenhuizen de FG-functie op een AVG-conforme wijze hebben ingebed binnen de organisatie. De FG wordt tijdig betrokken bij aangelegenheden die verband houden met de bescherming van persoonsgegevens. In nagenoeg alle onderzochte ziekenhuizen is sprake van periodiek overleg tussen de FG en de raad van bestuur. De ziekenhuisbesturen lijken de FG's voldoende te ondersteunen bij de vervulling van hun taken door hen te laten beschikken over voldoende middelen om hun werk te kunnen doen. Daarnaast lijken raden van bestuur zich voldoende bewust van de onafhankelijke positie van de FG binnen de organisatie.

- FG's en raden van bestuur zijn tevreden over hun onderlinge contact en afstemming. In alle onderzochte ziekenhuizen kunnen FG's zich rechtstreeks wenden tot de raad van bestuur. In de praktijk blijkt dat in de kleinere ziekenhuizen het contact tussen FG en raad van bestuur laagdrempelig is. In de grotere ziekenhuizen heeft de FG vaker een eerste contact met het 'lijnmanagement', maar dat laat de mogelijkheid om rechtstreeks contact op te nemen met de raad van bestuur onverlet.

- Alle raden van bestuur en de FG's van de onderzochte ziekenhuizen zijn zich bewust van de wettelijk verplichte onafhankelijke positie van de FG binnen de organisatie. De AP stelt vast dat de ziekenhuizen deze onafhankelijke positie vaak niet schriftelijk – en in aanvulling op de wettelijke bepalingen – in interne documenten hebben opgenomen.

4.2 De taakuitoefening van FG's binnen ziekenhuizen

4.2.1 Rol bij implementatie van de AVG

Alle FG's hebben een actieve rol gespeeld bij de implementatie van de AVG. Hierbij valt te denken aan het opstellen van plannen van aanpak, interne beleidsstukken, richtlijnen en werkprocessen. Tot de activiteiten van de FG's behoorden ook het organiseren van informatiebijeenkomsten, het ontwikkelen van e-learningprogramma's, het geven van presentaties, het opstellen van nieuwsbrieven en het delen van informatie op het intranet. In met name de kleinere ziekenhuizen hebben de FG's de feitelijke uitvoering van de AVG-implementatie zelf op zich genomen. In andere, voornamelijk grotere ziekenhuizen, hebben FG's een meer adviserende en toezichthoudende rol gehad, terwijl de feitelijke uitvoering en verantwoordelijkheid voor de implementatie bij een privacy-officer of CISO lag.

4.2.2 Creëren van een gegevensbeschermingscultuur

Alle FG's houden zich bezig met het vergroten van het privacybewustzijn binnen de organisatie. FG's ondernemen van alles om het personeel beter bewust te maken van het belang van privacy en zo een gegevensbeschermingscultuur te stimuleren. In dat kader zijn onder meer de volgende activiteiten genoemd:

- het houden van presentaties tijdens introductiesessies voor nieuwe medewerkers;
- het bijwonen van teamvergaderingen;
- het delen van informatie op het intranet van het ziekenhuis;
- het aanbieden van e-learnings over privacy voor alle medewerkers;
- het geven van algemene presentaties voor medewerkers.

Een greep uit de overige activiteiten:

- het organiseren van een dagelijkse *stand-up meeting* waarbij alle managers en de secretaris van de raad van bestuur bij elkaar zijn en waar de risico's van de dag met elkaar worden gedeeld;
- het uitvoeren van phishingtesten;
- een wekelijks inloopspreekuur voor de medewerkers van het ziekenhuis bij de FG.

4.2.3 Advisering

Advisering aan de raad van bestuur

In alle onderzochte ziekenhuizen is sprake van gevraagde en ongevraagde advisering van de FG aan de raad van bestuur. In de meeste gevallen is er binnen de raad van bestuur één lid verantwoordelijk voor ICT en informatiebeveiliging dan wel privacy en gegevensbescherming. Dat bestuurslid is dan het aanspreekpunt.

De raad van bestuur vraagt de FG doorgaans om advies bij vraagstukken waarbij privacy en gegevensbescherming een rol spelen en bij grotere projecten met een privacy-component. Verder weten raden van bestuur de FG voor advies te vinden bij het sluiten van verwerkersovereenkomsten en andere contracten met een privacy-aspect. Daarnaast wordt de FG geraadpleegd bij beveiligingsincidenten en datalekken. In

veel ziekenhuizen komt de FG regelmatig met ongevraagde adviezen aan de raad van bestuur. Dat is bijvoorbeeld het geval als mediaberichten daartoe aanleiding geven of bij incidenten binnen de organisatie, zoals datalekken en autorisatieproblemen. Ook hieruit blijkt dat er in dergelijke gevallen direct contact is tussen de raad van bestuur en de FG.

Vooral in kleinere ziekenhuizen is het contact tussen de FG en de raad van bestuur vaak laagdrempelig. Bij grotere ziekenhuizen komt het vaker voor dat de raad van bestuur niet rechtstreeks advies vraagt aan de FG, maar aan een privacycommissie waarvan de FG deel uitmaakt.

"Zeg als FG niet alleen dat het niet mag, maar ook hoe het wel kan"

- één van de FG's van de onderzochte ziekenhuizen -

Advisering door de FG binnen de organisatie

Vaak wordt de FG op ad-hocbasis geconsulteerd door collega's op de werkvloer. FG's zijn doorgaans, zeker bij kleinere ziekenhuizen, goed zichtbaar binnen de organisatie en staan intern bekend als dé privacy-expert en vraagbaak. Zij worden gemakkelijk benaderd door mensen van de werkvloer. Dit leidt er soms wel toe dat FG's in kleinere ziekenhuizen voornamelijk bezig zijn met het reactief adviseren aan medewerkers en minder toekomen aan proactieve taken, zoals het houden van intern toezicht binnen de organisatie. In met name grotere ziekenhuizen kunnen medewerkers voor vragen ook terecht bij een privacycommissie of een CISO.

Intern draagvlak bij advisering door de FG

De AP krijgt op basis van de schriftelijke inlichtingen en gesprekken de indruk dat privacy en gegevensbescherming de nodige aandacht krijgen van raden van bestuur. Wel is de AP uit het onderzoek duidelijk geworden dat sommige ziekenhuizen deze thema's relatief laat aandacht hebben gegeven en dat er in enkele ziekenhuizen nog wel werk aan de winkel is.

Daarnaast lijkt het erop dat de adviezen van de FG's doorgaans serieus worden genomen door het management. Op de werkvloer komen FG's vaker weerstand tegen. Men ervaart privacy en gegevensbescherming dan als bureaucratische last die bovenop de zorgverlening komt. Bij weerstand gaan FG's doorgaans het gesprek aan, waarbij zij bijvoorbeeld benadrukken dat privacy onlosmakelijk onderdeel uitmaakt van kwalitatief goede zorgverlening. Daarnaast proberen veel FG's in overleg met de afdeling te zoeken naar een oplossing die recht doet aan de wetgeving en tegelijkertijd praktisch werkbaar is. Eén FG benadrukte dat niet alleen gezegd moet worden dat het niet mag, maar ook hoe het wél kan.

Advisering bij DPIA's

In alle onderzochte ziekenhuizen geeft de FG advies bij DPIA's. De adviezen hebben betrekking op de vraag of er al dan niet een DPIA moet worden uitgevoerd, hoe het format van de DPIA eruit moet zien en welke methodiek er moet worden gevolgd. Daarnaast geven FG's advies over risico's die uit de DPIA volgen. Verder bestaat de betrokkenheid van FG's vaak uit het controleren en toetsen van de uitvoering van DPIA's. Een enkel ziekenhuis geeft aan dat de gang van zaken en de rol van de FG bij het uitvoeren van DPIA's nog nader moet worden uitgewerkt.

4.2.4 Toezicht op de naleving van de AVG

In de onderzochte ziekenhuizen vindt toezicht op de naleving van de AVG op veel verschillende manieren plaats. In de meeste gevallen vindt het toezicht plaats aan de hand van contacten met medewerkers en het aanwezig zijn bij werkoverleggen waarbij privacy een rol speelt. Zichtbaarheid binnen de organisatie leidt ertoe dat medewerkers de FG snel benaderen met vragen en opmerkingen. Dat kan voor de FG aanleiding zijn om bepaalde risico's te signaleren en toezicht te houden. Andere wijzen van toezichthouden zijn: het opvragen van documenten, het periodiek controleren van de logging, het afleggen van onaangekondigde bezoeken, het signaleren van trends uit incidenten en datalekken, het uitvoeren van audits, het monitoren van verbetermaatregelen en het doen van steekproefsgewijze controles.

De FG's ervaren de combinatie van adviseren en toezichthouden doorgaans niet als problematisch. Een enkele FG geeft aan dat deze combinatie de beide taken juist kan versterken. Dat kan bijvoorbeeld het geval zijn als uit toezichtsactiviteiten blijkt dat op sommige onderwerpen meer advisering gewenst is. Een andere FG zegt dat deze combinatie wel lastig kan zijn, omdat het soms onduidelijk is of de FG de toezichthoudende of de adviserende rol heeft. Medewerkers van ziekenhuizen kunnen dat als verwarrend ervaren.

4.2.5 Overige werkzaamheden van de FG

Betrokkenheid register van verwerkingsactiviteiten

In de helft van de onderzochte ziekenhuizen is de FG door de raad van bestuur belast met het opstellen en bijhouden van het register van verwerkingsactiviteiten. In de andere helft van de gevallen wordt dat gedaan door iemand anders, bijvoorbeeld de privacy-officer, CISO of data-architect. In één ziekenhuis is de CISO belast met het opstellen en bijhouden van het verwerkingenregister en heeft de FG daarbij een adviserende en controlerende rol. Die adviserende rol hield in dat geval tevens in dat de FG een format voor het verwerkingenregister had opgesteld.

Betrokkenheid bij klachten van patiënten over privacy

In alle onderzochte ziekenhuizen behandelt de FG klachten van patiënten over privacy-aangelegenheden. In enkele gevallen gebeurt dat in samenwerking met de klachtenfunctionaris, bij wie patiënten in eerste instantie klachten over de zorgverlening kunnen indienen en waarbij soms ook privacy-aspecten een rol spelen.

Betrokkenheid bij datalekken

In alle onderzochte ziekenhuizen is de FG op een of andere manier betrokken bij datalekken. In zes van de elf onderzochte ziekenhuizen verzamelt de FG de relevante feiten en doet de FG de melding van het datalek bij de AP en/of bij de betrokkene. In de overige gevallen is de rol van de FG beperkt tot het geven van advies en doet iemand anders binnen de organisatie de melding, bijvoorbeeld de CISO of privacy-officer. Afhankelijk van de ernst van het datalek wordt de raad van bestuur rechtstreeks ingeschakeld.

4.2.6 Verhouding met de AP

Het overgrote deel van de FG's van de onderzochte ziekenhuizen heeft slechts sporadisch (één of twee keer per jaar) contact met de AP. Als er contact is, dan gaat dat doorgaans over het melden van datalekken en de afwikkeling daarvan. Twee FG's hebben weleens een concreet vraagstuk aan de AP voorgelegd.

De FG's kijken op verschillende manier aan tegen de verhouding tussen de AP en de FG. Opgemerkt wordt dat de AP voornamelijk de 'externe' toezichthouder is en de FG de 'interne' toezichthouder. Eén FG zei dat de FG "de handen en voeten van de AP ter plaatse" is. Daarnaast kwam de opmerking voor dat de FG de "vooruitgeschoven post" van de AP is. Een andere FG merkt op dat de FG optreedt als verbindende factor tussen de AP en de verwerkingsverantwoordelijke.

4.2.7 Conclusies

- De FG's van de onderzochte ziekenhuizen hebben een belangrijke rol gespeeld bij de implementatie van de essentiële elementen van de AVG in de ziekenhuizen. Het verschilde daarbij of de FG uitsluitend een adviserende had of ook uitvoerende taken op zich nam.

- Alle FG's van de onderzochte ziekenhuizen houden zich actief bezig met het creëren en bevorderen van een gegevensbeschermingscultuur binnen de ziekenhuizen. De FG's ondernemen verschillende activiteiten en initiatieven om het privacybewustzijn in de organisatie te stimuleren. Daarnaast is het algemene beeld van de AP dat privacy en gegevensbescherming de nodige aandacht krijgen van raden van bestuur en dat adviezen van de FG's er daadwerkelijk toe doen.

- In alle onderzochte ziekenhuizen is er sprake van gevraagde en ongevraagde advisering van de FG aan de raad van bestuur. De raad van bestuur vraagt de FG doorgaans om advies bij vraagstukken, overeenkomsten en projecten waarbij privacy een rol speelt en bij beveiligingsincidenten en datalekken. Daarnaast komen FG's regelmatig met ongevraagde adviezen aan de raad van bestuur, bijvoorbeeld als berichten in de media of incidenten binnen de organisatie daartoe aanleiding geven. Het algemene beeld van de AP is dat de adviezen van de FG ertoe doen, aangezien alle ziekenhuizen aangeven dat de adviezen van de FG door de raden van bestuur worden opgevolgd. Vooral in kleinere ziekenhuizen is de FG dé privacy-vraagbaak van raad van bestuur en medewerkers op de werkvloer.

- Het toezicht op de naleving van de AVG door de FG's vindt op veel verschillende manieren plaats, bijvoorbeeld aan de hand van contacten met en vragen van medewerkers, het opvragen van documenten, het periodiek controleren van de logging, het signaleren van trends uit incidenten en datalekken en het uitvoeren van audits.

- In alle onderzochte ziekenhuizen geeft de FG advies bij DPIA's. De adviezen hebben betrekking op de vraag of er al dan niet een DPIA moet worden uitgevoerd, hoe het format van de DPIA eruit moet zien en welke methodiek er moet worden gevolgd. In alle onderzochte ziekenhuizen behandelt de FG klachten van patiënten over privacy-aangelegenheden en is de FG op een of andere manier betrokken bij datalekken binnen het ziekenhuis. In de helft van de onderzochte ziekenhuizen is de FG belast met het opstellen en bijhouden van het register van verwerkingsactiviteiten.

- Het overgrote deel van de FG's van de onderzochte ziekenhuizen heeft in het kader van de uitvoering van taken slechts sporadisch contact met de AP.

Bijlage 1 Juridisch kader

Relevante bepalingen uit de AVG

Artikel 37 - Aanwijzing van de functionaris voor gegevensbescherming

1. De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin:
a. de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken;
b. een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
c. de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.
2. Een concern kan één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is.
3. Wanneer de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie of overheidsorgaan is, kan één functionaris voor gegevensbescherming worden aangewezen voor verschillende dergelijke instanties of organen, met inachtneming van hun organisatiestructuur en omvang.
4. In andere dan de in lid 1 bedoelde gevallen kunnen of, indien dat Unierechtelijk of lidstaatrechtelijk is verplicht, moeten de verwerkingsverantwoordelijke of de verwerker of verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, een functionaris voor gegevensbescherming aanwijzen. De functionaris voor gegevensbescherming kan optreden voor dergelijke verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen.
5. 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.
6. De functionaris voor gegevensbescherming kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten.
7. De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de toezichthoudende autoriteit.

Artikel 38 - Positie van de functionaris voor gegevensbescherming

1. De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
2. De verwerkingsverantwoordelijke en de verwerker ondersteunen de functionaris voor gegevensbescherming bij de vervulling van de in artikel 39 bedoelde taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.
3. De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de functionaris voor gegevensbescherming geen instructies ontvangt met betrekking tot de uitvoering van die taken. Hij wordt door de verwerkingsverantwoordelijke of de verwerker niet ontslagen of gestraft voor de uitvoering van zijn taken.

De functionaris voor gegevensbescherming brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.
4. Betrokkenen kunnen met de functionaris voor gegevensbescherming contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van deze verordening.
5. De functionaris voor gegevensbescherming is met betrekking tot de uitvoering van zijn taken overeenkomstig het Unierecht of het lidstatelijk recht tot geheimhouding of vertrouwelijkheid gehouden.
6. De functionaris voor gegevensbescherming kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

Artikel 39 - Taken van de functionaris voor gegevensbescherming
1. De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
   a. de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van deze verordening en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen;
   b. toezien op naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
   c. desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 35;
   d. met de toezichthoudende autoriteit samenwerken;
   e. optreden als contactpunt voor de toezichthoudende autoriteit inzake met verwerking verband houdende aangelegenheden, met inbegrip van de in artikel 36 bedoelde voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.
2. De functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

De guidelines van de voormalige Artikel 29-werkgroep

In een *guideline* heeft de voormalige Artikel 29-werkgroep nadere richtlijnen gegeven voor wat betreft de taakuitoefening door FG's.[6] Deze richtlijnen bevatten een toelichting en aanbevelingen voor de taakuitoefening van FG's. Hierna vat de AP die richtlijnen en aanbevelingen per deelonderwerp samen.

Ten aanzien van de verplichte aanwijzing:
- de FG moet zich inzetten voor het creëren van een gegevensbeschermingscultuur binnen de organisatie;
- de FG moet helpen met de implementatie van essentiële elementen van de AVG, zoals de beginselen van gegevensverwerking, de rechten van de betrokkenen, *privacy by design* en *privacy by default*, de administratie van gegevensverwerkingen, beveiliging van het verwerkingsproces en melding van en communicatie over datalekken.

[6] Zie voetnoot 1 en 4 van het onderzoeksrapport.

Ten aanzien van de positie van de FG:

- de FG moet zo vroeg mogelijk worden betrokken wordt bij privacy-aangelegenheden;
- de FG moet binnen een organisatie als een gesprekspartner worden gezien en moet deel uitmaken van de relevante werkgroepen die binnen de organisatie gegevens verwerken;
- de FG moet regelmatig worden uitgenodigd om vergaderingen van het hogere management en het middenkader bij te wonen;
- de aanwezigheid van de FG wordt aanbevolen wanneer beslissingen worden genomen die gevolgen hebben voor de gegevensbescherming; daarbij moet alle relevante informatie tijdig aan de FG worden bezorgd, zodat de FG passend advies kan verlenen;
- aan de mening van de FG dient altijd passende waarde gehecht te worden, bij geschillen moet worden vastgelegd waarom het advies van de FG niet gevolgd is;
- als de organisatie beslissingen neemt die niet in de lijn liggen van de AVG en het advies van de FG, moet de FG de kans krijgen om zijn/haar afwijkende mening duidelijk te maken aan de hoogste leidinggevende en aan diegenen die de beslissingen nemen;
- de FG moet meteen worden geconsulteerd zodra zich een gegevensinbreuk of een ander incident voordoet;
- in de overeenkomst met de FG en in informatie die aan werknemers, management wordt verstrekt, moeten duidelijk de precieze taken van de FG en hun omvang worden vastgelegd, met name wat betreft het uitvoeren van een DPIA.

Ten aanzien van de benodigde middelen:

- doorgaans moeten aan de FG meer middelen ter beschikking worden gesteld naarmate de verwerkingsactiviteiten complexer en/of gevoeliger zijn;
- actieve ondersteuning van de functie van FG door het hogere management;
- voldoende tijd voor de FG's om hun taken te vervullen;[7]
- adequate ondersteuning op het vlak van financiële middelen, infrastructuur (kantoren, faciliteiten, apparatuur) en waar nodig personeel;
- de aanstelling van de FG moet officieel zijn bekend gemaakt, zodat iedereen in de organisatie op de hoogte is van het bestaan van deze functie;
- de FG moet zo nodig toegang hebben tot andere diensten zoals HR, juridische dienst, IT en beveiliging, zodat de FG's van die andere diensten de benodigde essentiële ondersteuning, bijstand of informatie kunnen ontvangen;
- voortgezette opleiding;[8]
- afhankelijk van de grootte en structuur van een organisatie kan het nodig zijn om een team rond de FG samen te stellen.

Ten aanzien van de onafhankelijkheid:

- FG's mogen bij het vervullen van hun taken geen instructies ontvangen over hoe ze een bepaalde aangelegenheid moeten behandelen;

[7] Dit is vooral belangrijk wanneer een interne FG op deeltijdse basis is aangesteld of wanneer de externe FG naast zijn andere taken ook voor gegevensbescherming instaat. Tegenstrijdige prioriteiten zouden er anders toe kunnen leiden dat de taken van de FG verwaarloosd worden.

[8] FG's moeten de kans krijgen om op de hoogte te blijven van nieuwe ontwikkelingen op het vlak van gegevensbescherming. Daarbij moet het de bedoeling zijn het niveau van de deskundigheid van de FG's permanent te verhogen en hen aan te moedigen deel te nemen aan opleidingen over gegevensbescherming.

- FG's mogen geen instructies ontvangen om een bepaald standpunt in te nemen in een aangelegenheid die verband houdt met de AVG.[9]

Ten aanzien van belangenconflicten:

- de FG mag binnen de organisatie geen functie bekleden waarbij hij of zij de doelstellingen van en de middelen voor de verwerking moet bepalen;
- om belangenconflicten te voorkomen, doet de organisatie er goed aan om:
  - de posities te identificeren die incompatibel kunnen zijn met de functie van FG;
  - interne regels op te stellen om belangenconflicten te vermijden;
  - een meer algemene uitleg over belangenconflicten op te nemen in interne regels;
  - te verklaren dat hun FG geen belangenconflict heeft in zijn functie als FG;
  - in het huisreglement van de organisatie waarborgen op te nemen en ervoor te zorgen dat de vacature voor de positie van FG of de dienstverleningsovereenkomst voldoende gepreciseerd en gedetailleerd is om belangenconflicten te vermijden.

Ten aanzien van de taken van de FG:

- de FG moet informatie verzamelen om verwerkingsactiviteiten te identificeren;
- de FG moet de naleving van verwerkingsactiviteiten analyseren en controleren;
- de FG moet de verwerkingsverantwoordelijke of de verwerker informeren, adviseren en aanbevelingen doen.[10]

Ten aanzien van de rol bij DPIA's:

Aangeraden wordt om de FG om advies te vragen over onder andere de volgende aangelegenheden:

- of er al dan niet een DPIA moet worden uitgevoerd;
- welke methodologie bij een DPIA moet worden gevolgd;
- of de DPIA intern uitgevoerd of uitbesteed moet worden;
- welke waarborgen moeten worden toegepast om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de DPIA al dan niet correct is uitgevoerd en of de conclusies al dan niet in overeenstemming zijn met de AVG;
- als de organisatie niet met het door de FG verleende advies instemt, moet in de documentatie over de DPIA specifiek en schriftelijk worden gemotiveerd waarom met het advies geen rekening is gehouden.

Risico gebaseerde aanpak:

- FG's moeten hun activiteiten prioriteren en hun inspanningen richten op zaken die een hoger risico voor de bescherming inhouden.

Ten aanzien van het bijhouden van registers:

Niets weerhoudt de organisatie ervan om de FG te belasten met het bijhouden van het verwerkingsregister, onder toezicht van de organisatie. Een dergelijk register is voor de FG een hulpmiddel om zijn of haar taken uit te voeren, met name toezien op de naleving, alsook informatie verlenen aan en adviseren van de organisatie.

[9] Dit betekent overigens niet dat FG's over meer beslissingsbevoegdheid beschikken dan voor hun taken vereist is; de verwerkingsverantwoordelijke of verwerker blijft verantwoordelijk voor de naleving van de AVG.

[10] Controle op naleving betekent niet dat de FG persoonlijk verantwoordelijk is bij een eventuele niet-naleving. In de AVG staat duidelijk dat het de verwerkingsverantwoordelijke en niet de FG gegevensbescherming is die passende technische en organisatorische maatregelen [treft] om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd" (artikel 24, lid 1).

Bijlage 2 Vragenlijsten

Vragen aan de verwerkingsverantwoordelijke (raad van bestuur)

Ten aanzien van de aanstelling en positie van de FG binnen het ziekenhuis (artikel 37 en 38 AVG):

1. Hoe is de FG functie ingebed in uw ziekenhuis? Zijn er interne richtlijnen, beleidsstukken of andere documenten waarin de positionering en de taken van de FG binnen uw organisatie worden omschreven en geprotocolleerd? De AP verzoekt u deze stukken toe te sturen.
2. Hoe heeft het bestuur de positie van de FG organisatorisch geregeld? Heeft het bestuur er bijvoorbeeld in voorzien dat de FG standaard deel uitmaakt van relevante werkgroepen die binnen het ziekenhuis gegevens verwerken?
3. Is de aanstelling van de FG intern bekend gemaakt, zodat iedereen binnen de organisatie op de hoogte is van het bestaan van deze functie en wie deze functie bekleedt?
4. Op welke wijze worden medewerkers van het ziekenhuis geïnformeerd over de precieze taken van de FG en de omvang van die taken? Wordt daarbij ook ingegaan op de functie van de FG bij het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA)? Kunt u dit met documentatie onderbouwen?
5. Hoe waarborgt het bestuur dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die te maken hebben met de verwerking van persoonsgegevens? Waar blijkt dit uit? Te denken valt aan interne richtlijnen, beleidsdocumenten, etc.
6. a. Hoe vaak heeft het bestuur (periodiek) overleg met de FG?
   b. Wordt de FG regelmatig uitgenodigd om vergaderingen van het bestuur bij te wonen?
   c. Als de FG wordt uitgenodigd een vergadering bij te wonen, wordt dan tijdig alle benodigde informatie aan de FG verstrekt?
   d. Kan de FG op eigen initiatief rechtsreeks in contact komen met het bestuur?

Ten aanzien van de benodigde middelen (artikel 38 AVG):

7. Geeft het bestuur de FG effectief toegang tot persoonsgegevens en verwerkingsactiviteiten, voor zover dat noodzakelijk is voor de uitoefening van zijn/haar functie? Hoe waarborgt u dit? Waar blijkt dit uit? Denk bijvoorbeeld aan interne richtlijnen, de (arbeids)overeenkomst met de FG, etc.
8. Welke middelen stelt het bestuur de FG ter beschikking voor het vervullen van zijn taken? Stelt het bestuur bijvoorbeeld financiële middelen, infrastructuur (kantoor, faciliteiten, apparatuur) en personeel ter beschikking? Kunt u dit met documentatie onderbouwen?
9. Verschaft het bestuur de FG zo nodig toegang tot andere diensten binnen het ziekenhuis, zoals HR, juridische zaken, IT en beveiliging, zodat de FG van die diensten de benodigde ondersteuning of informatie kan ontvangen?
10. Biedt het bestuur de FG opleidingsmogelijkheden? Zo ja, welke?
11. Hoe ondersteunt het bestuur de FG verder bij zijn taken? De AP verzoekt u – indien van toepassing – relevante interne documenten in dat kader toe te sturen.

Ten aanzien van de onafhankelijkheid en het voorkomen van belangenconflicten van de FG:

12. Hoe wordt gewaarborgd dat de FG onafhankelijk zijn werk kan doen binnen het ziekenhuis? Waar blijkt dit uit? Denk bijvoorbeeld aan interne richtlijnen, de (arbeids)overeenkomst met de FG, etc.
13. Zijn er interne regels opgesteld om belangenconflicten van de FG te vermijden? De AP verzoekt u deze interne regels toe te sturen.
14. Zijn er in de (arbeids)overeenkomst met de FG waarborgen opgenomen die belangenconflicten moeten vermijden?

15. Zijn in huisregels posities/functies binnen het ziekenhuis geïdentificeerd die onverenigbaar zijn met de functie van FG? Zo ja, welke functies zijn dat?
16. Hoe wordt gewaarborgd dat de FG geen instructies van (het bestuur van) het ziekenhuis ontvangt en dat de FG niet kan worden ontslagen of gestraft voor de uitvoering van zijn/haar taken? Waar blijkt dit uit? Denk daarbij bijvoorbeeld aan interne documentatie, de (arbeids)overeenkomst met de FG, etc.

Ten aanzien van de wettelijke taken van de FG (artikel 39 AVG):

17. a. In welke gevallen vraagt het bestuur om advies van de FG?
    b. Geeft de FG ook ongevraagde adviezen? Zo ja, kunt u hier voorbeelden van geven?
    c. Hoe gaat het bestuur om met adviezen van de FG? Kunt u een schatting maken van het aantal adviezen van de FG dat al dan niet wordt opgevolgd?
    d. Legt het bestuur meningsverschillen of geschillen met de FG vast?
    e. Indien het bestuur beslissingen neemt die niet in lijn liggen met adviezen van de FG, geeft het bestuur de FG dan de gelegenheid om een afwijkende mening duidelijk te maken? Kunt u dit met documentatie onderbouwen?
18. Consulteert het bestuur direct de FG, zodra zich een gegevensinbreuk of een ander incident voordoet? Waaruit blijkt dit? Hoe wordt dit binnen het ziekenhuis gewaarborgd?
19. Is de FG belast met het bijhouden van het verwerkingenregister?
20. Welke rol heeft de FG bij het uitvoeren van DPIA's?

Vragen aan de functionaris gegevensbescherming (FG)

Ten aanzien van de aanstelling en positie van de FG binnen het ziekenhuis (artikel 37 en 38 AVG):

1. Hoe is uw aanstelling formeel geregeld? De AP verzoekt u relevante documentatie toe te sturen, bijvoorbeeld de (arbeids)overeenkomst tussen u en het ziekenhuis, indien van toepassing. Daarbij mag u vertrouwelijke informatie, zoals NAW-gegevens en salarisgegevens, onzichtbaar maken.
2. Hoeveel dagen per week besteedt u gemiddeld aan de FG-taak?
3. Wordt u tijdig door het bestuur en door anderen binnen de organisatie betrokken bij aangelegenheden omtrent privacy? Kunt u daar voorbeelden van geven?
4. Maakt u standaard deel uit van relevante werkgroepen die binnen het ziekenhuis gegevens verwerken?
5. Rapporteert u rechtstreeks aan het bestuur? Zo ja op welke wijze? Zo nee aan wie rapporteert u en op welke wijze?
6. a. Hoe vaak hebt u (periodiek/structureel) overleg met de directie van het ziekenhuis?
    b. Wordt u regelmatig uitgenodigd om vergaderingen van het bestuur bij te wonen?
    c. Als u wordt uitgenodigd een vergadering bij te wonen, wordt dan tijdig alle benodigde informatie aan u verstrekt?
    d. Kunt u op eigen initiatief rechtstreeks contact opnemen met het bestuur?

Ten aanzien van de benodigde middelen (artikel 38 AVG):

7. Welke middelen worden u ter beschikking gesteld om uw functie te kunnen uitoefenen? Staan u financiële middelen, infrastructuur (kantoor, faciliteiten, apparatuur) en personeel ter beschikking? Maakt u daarvan daadwerkelijk gebruik? Mist u bepaalde middelen om uw functie goed te kunnen uitoefenen?
8. Krijgt u ondersteuning van andere medewerkers van het ziekenhuis (zoals privacyofficers, CISO's e.d.)? Werkt u bijvoorbeeld in een team of stuurt u een team aan?

9. Hebt u effectieve toegang tot persoonsgegevens en verwerkingsactiviteiten, voor zover dat noodzakelijk is voor de uitoefening van uw functie?
10. Hebt u effectieve toegang tot en ondersteuning van andere diensten binnen het ziekenhuis, zoals HR, juridische zaken, IT en beveiliging?
11. Biedt het ziekenhuis opleidingsmogelijkheden voor de FG functie aan en zo ja, welke? Beschikt u bijvoorbeeld over een opleidingsbudget? Maakt u daarvan gebruik?
12. Welke ondersteuning biedt het management van het ziekenhuis u verder bij uw werkzaamheden?

Ten aanzien van de onafhankelijkheid en het voorkomen van belangenconflicten van de FG:

13. Vervult u naast uw functie als FG ook nog andere functies in het ziekenhuis? Zo ja welke?
14. Zijn er in de (arbeids)overeenkomst tussen u en het ziekenhuis waarborgen opgenomen die belangenconflicten moeten vermijden?
15. Krijgt u weleens instructies van het bestuur van het ziekenhuis over hoe u uw taken dient uit te voeren of om een bepaald standpunt in te nemen? Kunt u dat toelichten?

Ten aanzien van de wettelijke taken van de FG (artikel 39 AVG):

16. Wat is/was uw rol bij de implementatie van essentiële elementen van de AVG, zoals de beginselen van gegevensverwerking, de rechten van betrokkenen, *privacy by design* en *privacy by default*, de administratie van gegevensverwerkingen, beveiliging van het verwerkingsproces en melding van en communicatie over datalekken?
17. a. Hoe vult u uw adviesrol in?
    b. In welke gevallen vraagt het bestuur u om advies?
    c. Geeft u weleens ongevraagd advies aan het bestuur?
    d. Wat wordt er met uw adviezen gedaan? Kunt u een schatting maken van het aantal adviezen dat door het bestuur wordt opgevolgd?
    e. Wat doet u als het bestuur uw advies niet volgt?
    f. Worden meningsverschillen of geschillen met het bestuur vastgelegd? Zo ja, wie doet dat en op welke wijze?
    g. Heeft u de indruk dat privacy adviezen soms als belemmerend worden ervaren? En zo ja hoe gaat u daarmee om?
    h. Indien het bestuur beslissingen neemt die niet in lijn liggen met uw adviezen, geeft het bestuur u dan de gelegenheid om een afwijkende mening duidelijk te maken?
18. Houdt u zich actief bezig met de beoordeling of afwikkeling van datalekken? Wordt u direct geconsulteerd zodra zich binnen de organisatie een gegevensinbreuk of een ander incident voordoet?
19. Bent u betrokken bij het beoordelen of uitvoeren van DPIA's? Zo ja op welke wijze? Denk daarbij bijvoorbeeld aan adviezen omtrent de verplichting om een DPIA uit te voeren, welke methodologie moet worden gevolgd, welke waarborgen er moeten worden toegepast, etc.
20. Bent u belast met het bijhouden van het verwerkingsregister? Zo ja op welke wijze doet u dat?
21. Wat doet u om het privacybewustzijn van de organisatie te vergroten? Waaruit blijkt dat?
22. Hoe houdt u intern toezicht? Hoe geeft u dat interne toezicht vorm en inhoud? Hoe ervaart u de combinatie van adviserende en toezichthoudende taken?
23. Behandelt u ook klachten omtrent privacy-aangelegenheden van patiënten?
24. Hoe prioriteert u uw activiteiten?
25. Hoe vaak hebt u in het kader van uw activiteiten contact met de AP?
26. Hoe ziet u uw eigen toezichthoudende taak in relatie tot de toezichthoudende taak van de AP?

AUTORITEIT
PERSOONSGEGEVENS

Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.