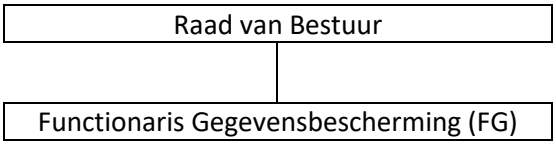
Profiel Functionaris Gegevensbescherming (FG)

Doel van de functie FG:

- Het houden van intern toezicht op de verwerking van (persoons)gegevens binnen de organisatie.
- Het geven van adviezen over de toepassing van privacywetgeving.
- Bevorderen van awareness op de gebieden privacybescherming en informatiebeveiliging.
- Het inventariseren van de verschillende soorten van gegevensverwerking en het adviseren en verstrekken van informatie ten aanzien van privacy en verwerking van (persoons)gegevens aan de Raad van Bestuur, managers en de medewerkers binnen de organisatie.
- Het behandelen en beoordelen van beveiligingsincidenten/datalekken.

Plaats van de FG in de organisatie:

De functionaris ontvangt hiërarchisch en functioneel leiding van de Raad van Bestuur van de organisatie. De functionaris voert de toezichthoudende taken onafhankelijk uit. De functie kan eventueel gecombineerd worden met een andere niet conflicterende positie binnen of buiten de organisatie.



Hoofdactiviteiten van de FG:

- Het houden van toezicht op de naleving van wet- en regelgeving, meer specifiek ten aanzien van privacy en de verwerking van persoonsgegevens (een en ander in afstemming met de Compliance Officer/ Information Security Officer).
- Gevraagd en ongevraagd (juridisch) advies geven en het verstrekken van informatie ten aanzien van privacy en de verwerking van persoonsgegevens.
- Het beoordelen en afhandelen van beveiligingsincidenten/ datalekken met betrekking tot persoonsgegevens en het in opdracht van de Raad van Bestuur melden van deze incidenten aan externe toezichthouder(s) en betrokkenen.

Uitwerking hoofdactiviteiten FG (in processtappen en resultaten):

1. Het houden van toezicht op de naleving van wet- en regelgeving meer specifiek ten aanzien van privacy en de verwerking van persoonsgegevens:

1.1 Het toezien op de naleving van wettelijke regels ten aanzien van het verwerken van persoonsgegevens binnen de organisatie, waaronder de Wet bescherming persoonsgegevens of een daarvoor in de plaats komende regeling (AVG) en de Wet op de geneeskundige behandelingsovereenkomst (een en ander in afstemming met de Information Security Officer).

1.2 Het onafhankelijk onderzoeken en beoordelen van gegevensverwerkingen, waarbij de functionaris de bevoegdheid heeft om voor het onderzoek en beoordeling benodigde informatie op te vragen en ruimten te betreden binnen de organisatie.

1.3 Het bijhouden van een openbaar register van gegevensverwerkingen

1.4 Het afstemmen met de Compliance Officer/ Information Security Officer over activiteiten op het gebied van informatiebeveiliging en het uitvoeren van controles en risicoanalyses die tevens zien op persoonsgegevens. Alsmede het bespreken van de uitkomsten van de controles en risicoanalyses.

1.5 Het onderhouden van externe contacten, waaronder met externe toezichthouders (Autoriteit Persoonsgegevens), en het participeren in (externe) overleggen.
1.6 Het signaleren van relevante wet- en regelgeving en jurisprudentie op het gebied van privacy.

2. Gevraagd en ongevraagd (juridisch) advies geven en het verstrekken van informatie ten aanzien van privacy en de verwerking van persoonsgegevens:

2.1 Het gevraagd en ongevraagd geven van advies en het doen van aanbevelingen ten aanzien van privacy en de verwerking van persoonsgegevens aan de Raad van Bestuur, managers en medewerkers binnen de organisatie. Daaronder tevens begrepen de te nemen maatregelen onder andere voortvloeiende uit controles, risicoanalyses en incidenten.
2.2 Bevorderen van het (organisatie)bewustzijn met betrekking tot de omgang met vertrouwelijke gegevens en het geven van voorlichting en informatie aan medewerkers.
2.3 Het opstellen/toetsen van diverse documenten, waaronder: adviezen, reglementen, procedures, bewerkersovereenkomsten, ten aanzien van privacy en verwerking van persoonsgegevens.

3. Het beoordelen en afhandelen van beveiligingsincidenten/datalekken met betrekking tot persoonsgegevens en het melden van deze incidenten in overleg met de Raad van Bestuur aan externe toezichthouder(s):

3.1 Het beoordelen c.q. onderzoeken of beveiligingsincidenten gemeld moeten worden bij externe toezichthouders als zijnde datalek en of de betrokkene(n) geïnformeerd moet(en) worden.
3.2 Het adviseren van de Raad van Bestuur en de stuurgroep Informatiebeveiliging over het al dan niet melden van beveiligingsincidenten bij externe toezichthouder(s) en/of betrokkene(n).
3.3 Na besluit van de Raad van Bestuur het melden van beveiligingsincidenten bij de externe toezichthouder(s) en/of betrokkene(n) en het coördineren van deze melding.
3.4 Het rapporteren aan de Raad van Bestuur en de stuurgroep Informatiebeveiliging over het gevoerde beleid ten aanzien van privacy en de verwerking van persoonsgegevens, de ontvangen en gedane meldingen (incidenten) en ondernomen acties en getroffen maatregelen.
3.5 Het onderhouden van externe contacten, waaronder met externe toezichthouder(s) en betrokkene(n).
3.6 Het afhandelen van klachten over het gebruik van persoonsgegevens.

<u>Profiel van de functie</u>

Vereiste kennis

- Academisch werk en denkniveau.
- Kennis van relevante en toekomstige wet- en regelgeving omtrent de bescherming van persoonsgegevens.
- Kennis van governance en compliance.
- Kennis van informatie- en communicatietechnologie.
- Kennis van informatiebeveiliging.
- Kennis van de administratieve organisatie.
- Kennis van Privacy Impact Assessment (PIA).
- Kennis van audits.
- Kennis van integriteit en ethiek op het gebied van privacyvraagstukken.
- Heeft kennis van doel, (juridische en organisatie) structuur, beleid en wijze van functioneren van de organisaties.
- Vakkennis dient op peil te worden gehouden, bijvoorbeeld door het lezen van vakliteratuur, het volgen van specifieke bij- en nascholing en cursussen en het bezoeken van studiedagen of symposia op het vakgebied.

Zelfstandigheid

- Werkt binnen de beleidskaders zeer zelfstandig aan de hand van hoofdlijnen waarbij afgewogen keuzes moeten worden gemaakt en waarbij de werkwijze naar eigen inzicht wordt bepaald.
- Is in staat complexe en/of gevoelige incidenten te beoordelen door het combineren c.q. toepassen en hanteren van juridische kennis en begrip en kennis van wet- en regelgeving ten aanzien van privacy en persoonsgegevens. Vertaalt de problematiek en wet- en regelgeving in correcte procedures, adviezen en overige documenten. Is hierbij in staat om zowel zelfstandig als in teamverband te werken.

Sociale vaardigheden
- Bij het geven van (juridisch) advies, het verstrekken van informatie en het behandelen c.q. beoordelen van beveiligingsincidenten/datalekken worden hoge eisen gesteld aan tact, luistervaardigheid, gespreksvoering, probleemoplossend vermogen, het omgaan met tegenstellingen en het kunnen overtuigen.

Risico's, verantwoordelijkheid en invloed
- Er is sprake van professionele verantwoordelijkheid bij het uitbrengen van (juridische) adviezen en het verstrekken van (juridische) informatie, het interpreteren en toepassen van wet- en regelgeving en het behandelen c.q. beoordelen van beveiligingsincidenten betreffende persoonsgegevens.
- Er bestaat kans op materiële en immateriële schade bij het geven van onjuiste of onvolledige informatie en adviezen en bij het onjuist beoordelen of beveiligingsincidenten gemeld moeten worden aan externe toezichthouder(s) en/of betrokkene(n). Bij de diverse in- en externe contacten kan de goede naam van de organisaties nadelig worden beïnvloed.

Uitdrukkingsvaardigheid
- Hoge eisen worden gesteld aan de mondelinge uitdrukkingsvaardigheden bij in- en externe contacten.
- Zeer hoge eisen worden gesteld aan schriftelijke uitdrukkingsvaardigheden. De correcte (juridische) terminologie dient te worden gehanteerd bij het opstellen van de diverse documenten.
- Beschikt verder over het vermogen om ideeën en opvattingen helder en beknopt schriftelijk te verwoorden en gevoelige onderwerpen diplomatiek te beschrijven.

Bewegingsvaardigheid
- Er worden geen bijzondere eisen aan de bewegingsvaardigheid gesteld. Bij de uitvoering van de werkzaamheden wordt veelvuldig gebruik gemaakt van de computer.

Oplettendheid
- Oplettendheid is nodig bij de adviserende, begeleidende en uitvoerende (juridische) werkzaamheden en het beoordelen en behandelen van beveiligingsincidenten betreffende persoonsgegevens, waarbij in ruime mate aandacht is vereist voor zowel grote lijnen als details en de belangen van de organisaties.

Overige functie-eisen
- Beschikt over volharding en een groot doorzettingsvermogen teneinde de nodige informatie te vergaren om een volledig (juridisch) advies dan wel informatie te verstrekken alsmede om een beveiligingsincident op juiste wijze te kunnen beoordelen.
- Systematiek en ordelijkheid is vereist bij de analyse van het vraagstuk op grond waarvan een juridisch advies en informatie wordt geformuleerd.
- Hoge eisen worden gesteld aan het kunnen omgaan met gevoelige informatie, integriteit en

betrouwbaarheid.
- Eisen worden gesteld aan voorkomen en gedrag in verband met het onderhouden van in- en externe contacten binnen het werkveld.
- Aanzienlijke objectiviteit is vereist.

Inconveniënten
- Psychische belasting kan optreden door cumulaties van verantwoordelijke werkzaamheden onder tijdsdruk.
- Tevens kan psychische belasting plaatsvinden doordat men te maken krijgt met conflicterende belangen die kunnen optreden tussen individuele medewerkers en de organisatie, tussen verschillende organisatieonderdelen of in externe samenwerkingsrelaties.

Salaris
Inschaling vindt plaats in schaal 65 van de cao ziekenhuizen.