Maastricht University

Werkwijze Functionaris Gegevensbescherming UM (wettelijk en onafhankelijk toezicht)

Op grond van de Algemene verordening gegevensbescherming (EU) 2016/679 (AVG) is de Universiteit Maastricht (UM) verplicht een functionaris voor gegevensbescherming (FG) aan te stellen. De UM volgt daarbij de Richtlijnen voor functionarissen voor de gegevensbescherming (16/NL WP 243 rev.01) van de samenwerkende Europese privacy toezichthouders, de voormalige Groep gegevensbescherming Artikel 29 (WP29)[1] en verklaart deze Richtlijnen leidend aangaande taken, positionering, ondersteuning en omgang met de FG in brede zin.[2]

Om effectief te kunnen functioneren als FG zijn in de wet een aantal aspecten vastgelegd, waaronder de aanwijzing, de positie en de taken van de FG. Bijzondere aandacht daarbij verdient de onafhankelijke rol en dus de autonomie van de FG. Die autonome positie in functioneren kan kwetsbaar zijn nu de FG als tussenpersoon tussen het bestuur en de Autoriteit Persoonsgegevens moet functioneren. Dit vereist dat hierover in de organisatie geen misverstanden kunnen ontstaan. Van belang is dan ook om het inrichtingsvraagstuk omtrent taken en rol van FG als organisatie transparant vast te leggen. Deze werkwijze geeft hieraan de noodzakelijke nadere uitwerking.

Opdracht FG op hoofdlijnen
De opdracht van de FG volgt uit artikelen 37-39 AVG en is in grote lijnen als volgt:

- Toezicht door middel van:
  - informeren en adviseren over wettelijke verplichtingen op het gebied van gegevensbescherming, gevraagd en ongevraagd, met name het College van Bestuur (CvB) en directeuren van de UM, maar ook andere belanghebbenden zoals projectleiders en onderzoekers;
  - toezicht houden op de interne naleving van de AVG, verwante wetgeving en interne beleidsafspraken hierover (gezamenlijk te noemen 'privacy wet- en regelgeving');
- Advies verstrekken over gegevensbeschermingseffectbeoordelingen (GEB), of Data Protection Impact Assessments, DPIA);
- Samenwerken met het nationale centrale toezicht, binnen Nederland is dit de Autoriteit Persoonsgegevens (AP);
- Optreden als contactpunt voor de AP, maar ook voor interne en externe stakeholders op het gebied van gegevensbescherming;
- Het vervullen van een ombudsfunctie voor gegevensbescherming zowel intern (voor medewerkers) als extern (voor alle andere betrokkenen);
- De naleving en toepassing van de AVG ondersteunen met praktische hulpmiddelen voor de UM en waar nodig het voorstellen van nieuw beleid of aanpassingen op bestaand beleid en toezicht houden op de naleving van bestaand beleid;
- Het bijdragen aan communicatie en bewustwording op het gebied van gegevensbescherming door onder andere het toegankelijk maken van relevante informatie en het verzorgen van voorlichting en training.

In Bijlage I zijn de hoofdlijnen van de opdracht de FG nader uitgewerkt in taken en activiteiten.

Positionering en inbedding van de FG
De FG brengt rechtstreeks verslag uit aan de portefeuillehouder privacy en informatiebeveiliging van het CvB. Het uitgangspunt voor de werkzaamheden van de FG is een op risico gebaseerde aanpak. Dat wil zeggen dat de grootste risico's de meeste aandacht krijgen van de FG en dat niet

[1] De Groep gegevensbescherming artikel 29 is op 23 mei 2018 opgeheven en vervangen door de European Data Protection Board.

[2] De AVG biedt een gemoderniseerd, op verantwoording gebaseerd kader voor de naleving van regels inzake gegevensbescherming in Europa. Functionarissen voor gegevensbescherming zijn de sleutelfunctionarissen in deze verantwoording. Naast het feit dat ze de naleving vereenvoudigen door de implementatie van verantwoordingsinstrumenten (zoals het mogelijk maken van Data Protection Impact Assessments en het uitvoeren of mogelijk maken van controles), fungeren functionarissen voor gegevensbescherming als tussenpersonen tussen relevante belanghebbenden (zoals de Autoriteit Persoonsgegevens, betrokkenen wiens persoonsgegevens beschermd dienen te worden en organisatieonderdelen binnen UM).

verwacht kan worden dat de FG te allen tijde een volledig inzicht kan bieden ten aanzien van alle risico's rond gegevensbescherming in de organisatie. Om inzichtelijk te maken (op hoofdlijnen) waar de FG zijn/haar voornaamste aandacht op wil richten zal de FG periodiek, maar minimaal jaarlijks, een UM toezichtagenda functionaris gegevensbescherming opstellen. Dit zal met de portefeuillehouder in het CvB worden besproken en vervolgens bestuurlijk worden vastgesteld.

De FG heeft een toezichthoudende en adviserende rol op het terrein van gegevensbescherming ten opzichte van andere deskundigen die zich in de organisatie met gegevensbescherming bezighouden. 'Aanwijzingen' van de FG kunnen als richtsnoer gelden conform overweging 77 AVG en dienen in beginsel opgevolgd te worden tenzij er gemotiveerd en gedocumenteerd van wordt afgeweken.

De FG heeft periodiek overleg met deze deskundigen.

De FG stemt informatiebeveiligingsaspecten voor zover die samenhangen met de bescherming van persoonsgegevens af met de (corporate) information security officer(s) van de UM.

De FG heeft een rol in de interne audit op het terrein van gegevensbescherming en afstemming zal dan ook plaats vinden met de interne auditor(s) en waar nodig met de externe auditor. In het kader van toezicht op gegevensbescherming is de FG eindverantwoordelijk, audit speelt daarin een belangrijke rol.

Taken van UM
Om de FG in staat te stellen zijn taken goed uit te voeren draagt de UM zorg voor:

- **Betrokkenheid**: De UM betrekt de FG tijdig en naar behoren bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens, daarbij wordt rekening gehouden met de aard en risico's van de verwerking van persoonsgegevens;

- **Benodigde middelen**: De UM verschaft de FG toegang tot persoonsgegevens en verwerkingsactiviteiten en de voor het uitvoeren van zijn taken en het in stand houden van zijn deskundigheid benodigde middelen. Het gaat daarbij met name om:
    - actieve ondersteuning door het CvB en het hogere management, met name waar het gaat om het uitdragen van het belang van de AVG;
    - voldoende tijd om zijn taken uit te voeren;
    - adequate financiële middelen, infrastructuur (kantoor, faciliteiten, apparatuur) en indien noodzakelijk personele resources;
    - officiële interne berichtgeving over de benoeming van de FG;
    - toegang tot de service centra, faculteiten en Maastricht University Office (MUO) zoals HRM, JZ, ICTS, M&C, etc. zodat de FG de benodigde ondersteuning, inbreng en informatie kan verkrijgen vanuit die organisatie-eenheden;
    - (bij)scholing aangaande (ontwikkelingen op het gebied van) gegevensbescherming.

Een en ander gelet op de complexiteit van de organisatie en de verwerkingen, de gevoeligheid van de gegevens en de hoeveelheid werk die daar voor de FG uit ontstaat. De vraag naar extra resources (zowel financieel als personeel) zal bezien worden in de context van een op risico gebaseerde aanpak en in dialoog met de portefeuillehouder privacy en informatiebeveiliging van het CvB, waarbij eveneens de organisatie & prioritering van activiteiten in acht wordt genomen. Beschikbaarstelling van extra resources voor het uitvoeren van de toezichthoudende taken dient geaccordeerd te worden door het CvB.

- **Onafhankelijkheid en onthouding van instructies**[3]: Om te waarborgen dat de FG zijn taken onafhankelijk en autonoom kan uitvoeren vanuit uitsluitend het belang van persoonsgegevensbescherming, geldt dat de FG:
  - geen instructies ontvangt over de uitvoering van zijn taken in relatie tot gegevensbescherming;
  - geen instructies ontvangt over het al dan niet raadplegen of informeren van de Autoriteit Persoonsgegevens (AP), waarbij de FG werkt conform de AVG en de beleidsregels van de AP;
  - geen instructies ontvangt over de gewenste uitkomst van onderzoeken of de afhandeling van klachten van betrokkenen;
  - zich een onafhankelijke visie kan vormen over de uitleg van de AVG;
  - bij beslissingen die niet in lijn zijn met de AVG of zijn adviezen, altijd verslag kan uitbrengen – zonder inhoudelijke aanpassingen – aan het CvB;
  - kan besluiten een jaarverslag op te stellen en te publiceren.

Een en ander staat organisatorische inbedding van de FG bij een interne afdeling niet in de weg, evenmin als het aanwijzen van een directeur als dagelijks leidinggevende die onder andere belast is met zaken als goedkeuring van verlof, declaraties en wat dies meer zij. Desbetreffende directeur zal zich opstellen als een goed hospita en zich onthouden van enige belangenverstrengeling, de FG houdt immers ook toezicht op de gegevensverwerking van desbetreffende afdeling.

Aanvullend op het bovenstaande:
  - Op basis van overleg met de portefeuillehouder privacy en informatiebeveiliging zullen de prioriteiten van de FG op hoofdlijnen worden gemonitord en, indien nodig, gedurende het jaar worden aangepast;
  - In overleg kunnen er, zonder afbreuk te doen aan de wetgeving, aanvullende afspraken gemaakt worden over rapportagelijnen en waarborgen m.b.t. kwaliteit zoals hoor en wederhoor ten aanzien van bevindingen van de FG;
  - De beroepsverenigingen met betrekking tot gegevensbescherming zijn in ontwikkeling. Wanneer best practices en overige instrumenten ontwikkeld worden door, en gedeeld worden binnen, de beroepsvereniging worden deze besproken met de relevante stakeholders en na inhoudelijke overeenstemming op het juiste niveau vastgesteld en geadopteerd binnen de UM;
  - De FG houdt zich aan bestaande regels en processen van de UM. Wanneer deze in strijd zijn met de onafhankelijke positie van de FG zoals beschreven in de AVG dan kaart de FG dit zo snel mogelijk aan bij het CvB en worden er op dit punt specifieke afspraken gemaakt.

- **Vrijwaring van ontslag en sancties**: Om de autonome positie van de FG te versterken mag hij in verband met zijn optreden als FG geen nadelen ondervinden, zoals (dreiging van) sancties (waaronder het uitstellen van promotie, het verhinderen van verdere carrière uitbouw, het weigeren van voordelen die andere werknemers wel genieten) of ontslag. Dat laat onverlet dat de FG nog steeds rechtmatig kan worden gesanctioneerd of ontslagen om andere redenen die niet te maken hebben met zijn optreden als FG c.q. wegens gronden die niet in de uitvoering van zijn taken zijn gelegen.

- **Voorkoming van belangenconflicten**: De UM laat de FG geen andere taken of plichten vervullen en de FG neemt geen nevenfuncties op zich die een mogelijk belangenconflict met zijn kerntaken zou kunnen opleveren.

- **Geheimhouding**: De FG is met betrekking tot de uitvoering van zijn taken tot geheimhouding gehouden. Deze geheimhouding verhindert de FG echter niet om met de AP of externe deskundigen contact op te nemen en om advies te vragen. Formele stukken van de

[3] De Autoriteit Persoonsgegevens beschouwt de functionaris gegevensbescherming als een 2e defence line van de AP waarmee de functionaris als externe auditor in de organisatie wordt gepositioneerd

FG zijn bovendien openbaar, omdat de UM een organisatie is die valt binnen de reikwijdte van de Wet open overheid.

- **Verantwoordelijkheid**: De verantwoordelijkheid voor het naleven van relevante wet- en regelgeving ligt bij de UM, specifiek het CvB, en kan niet worden gedelegeerd aan de FG. De FG vereenvoudigt en bevordert naleving door het implementeren van verantwoordingsinstrumenten zoals het faciliteren en beoordelen van GEB/DPIA en het uitvoeren van controles. Tevens fungeert de FG als tussenpersoon voor belanghebbenden zoals de AP, interne organisatieonderdelen binnen de UM, het CvB en de betrokkenen.

- **Governance**: De UM zal de voorgeschreven en gewenste omgang met de positie van de FG nader uitwerken en opnemen in relevante governance documenten.

BIJLAGE I

De hoofdlijnen van de opdracht de FG nader uitgewerkt in taken en activiteiten:

Op grond van de AVG heeft de FG de volgende kerntaken:

- *Toezicht en controle*
  - toezien op de naleving van de AVG en andere relevante regelgeving;
  - toezien op de naleving van intern vastgesteld beleid ter zake van persoonsgegevensbescherming. Hiertoe worden onder andere door de FG incidenten bijgehouden;
  - bevindingen van het toezicht rapporteren, waaronder voorgekomen incidenten;
  - gevraagd en ongevraagd relevante aanbevelingen en verbetervoorstellen doen;
  - het onderzoeken en beantwoorden van klachten van betrokkenen.

  Het toezicht richt zich daarbij onder meer op:
  - de documentatieplicht en het register van verwerkingen;
  - het faciliteren van de rechten van betrokkenen;
  - het melden en mededelen van inbreuken;
  - het bewustmaken en opleiden van het bij de verwerking betrokken personeel;
  - het uitvoeren of mogelijk maken van audits.

- *Informeren en adviseren*
  - informeren over verplichtingen op grond van de AVG, de UAVG en andere relevante nationale of Europese regelgeving met betrekking tot de bescherming van persoonsgegevens;
  - adviseren hoe de UM het best aan die verplichtingen kan voldoen;
  - adviseren over de daartoe benodigde organisatorische inrichting.

- *Op verzoek adviseren over de DPIA*
  Het gaat daarbij om:
  - de noodzaak van het uitvoeren van een DPIA;
  - de aard, te volgen methodologie, en uitvoeringswijze van de DPIA;
  - of de DPIA intern uitgevoerd of uitbesteed moet worden;
  - of de DPIA juist is uitgevoerd;
  - of gelet op de uitkomsten nakoming van de AVG kan worden gewaarborgd;
  - of de Autoriteit Persoonsgegevens (AP) eerst moet worden geraadpleegd;
  - welke maatregelen en waarborgen bij de verwerking dienen te worden toegepast.

- *Samenwerken met en optreden als contactpunt voor de AP*
  De FG is de contactpersoon van de UM voor de AP:
  - bij de uitoefening van de toezichthoudende, adviserende en handhavende bevoegdheden van de AP;
  - indien de AP toegang tot documenten of informatie vordert;
  - rond het melden en opvolgen van datalekken;
  - in geval van een zogenaamde *voorafgaande raadpleging*.
  - De FG kan, wanneer dit relevant wordt geacht, daarnaast overleg plegen met de AP over enige ander aangelegenheid.

De UM verwacht dat de FG zich naast deze wettelijke kerntaken bezighoudt met:

- *Beleid & praktische hulpmiddelen:*
  - initiëren en (mede)vormgeven van gegevensbeschermingbeleid;
  - opstellen van en bijdragen aan FAQ's, checklists en handleidingen;
  - opstellen van en input leveren voor gedragscodes en modelovereenkomsten;
  - sparringpartner zijn voor verantwoordelijk directeuren;

  - bevorderen van in- en externe samenwerking op het vlak van persoonsgegevensbescherming;
  - bevorderen van uniformering van normenkaders, richtlijnen, gedragscodes (naar zijn aard instellingsbreed, sectoraal, domein- of onderzoeksveldspecifiek en/of internationaal).

- *Communicatie en bewustwording:*
  - toegankelijk maken van informatie rond gegevensbescherming;
  - bevorderen bewustwording rond gegevensbescherming;
  - stimuleren van draagvlak voor gegevensbeschermingbeleid;
  - verzorgen van voorlichting en training.

- *Coördinatie en aanspreekpunt:*
  De FG moet het gezaghebbende UM-aanspreekpunt zijn op het vlak van gegevensbescherming. Daarbij hoort dat hij:
  - zich profileert als het 'gezicht' van gegevensbescherming binnen de UM;
  - benaderbaar is voor betrokkenen, met name in verband met de uitoefening van hun rechten;
  - desgewenst aanschuift bij relevante overleggen;
  - kan doorverwijzen naar juiste in- en externe informatiebronnen en functionarissen;