Opmerkingen NGFG bij Richtlijnen voor functionarissen voor de gegevensbescherming van de Artikel 29-werkgroep

Mr. J. de Zeeuw[*]

109

De Artikel 29-werkgroep, de Europese groep van toezichthouders,[1] heeft op 13 december 2016 een waardevol document aangenomen, namelijk: Richtlijnen voor functionarissen voor gegevensbescherming (WP 243). De richtlijnen vormen een belangrijk middel voor de interpretatie van de artikelen 37, 38 en 39 van de Algemene verordening gegevensbescherming (AVG). Dat zijn de artikelen die gaan over de benoeming, positie en taken van de Functionaris voor gegevensbescherming, oftewel de FG. De FG speelt een sleutelrol bij het nakomen van de AVG en andere privacy- en gegevensbeschermingswetgeving. Deze richtlijnen zijn van groot belang voor veel organisaties die onder de AVG verwerkingsverantwoordelijke of verwerker zullen zijn. En uiteraard voor (toekomstige) functionarissen voor gegevensbescherming.

De werkgroep heeft, voordat ze de richtlijnen definitief zou vaststellen, de mogelijkheid geboden om feedback te geven. Het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG) heeft van die mogelijkheid gebruikgemaakt en bij brief van 1 februari 2017 commentaar gegeven op de richtlijnen.

Het NGFG is tevreden over het doel en de algemene inhoud van de richtlijnen. Het doel van de richtlijnen is niet alleen om de relevante bepalingen in de AVG te verduidelijken, maar ook om de FG's bij te staan in hun rol. Dat vindt het NGFG een welkome doelstelling. Het NGFG vindt het echter ook belangrijk dat de richtlijnen zo veel mogelijk de doelmatigheid van de FG vergroten. Hij adviseert de groep dan ook aan te geven hoe haar stelling, dat de vrijwillige aanstelling van FG's wordt aangemoedigd, concreet zal worden geëffectueerd. Het NGFG maakt voorts een aantal opmerkingen op onderdelen van de richtlijnen. De opmerkingen hebben in het bijzonder betrekking op de relatie tussen de FG en de toezichthoudende autoriteit, de benoeming van een FG, en de eisen rond de onafhankelijkheid van een FG. Als rode draad geldt daarbij dat de behoefte nog steeds groot is aan *guidance*, vooral wat betreft het borgen van het onafhankelijke karakter van de FG en zijn taak om toezicht te houden.

Het NGFG signaleert allereerst dat er nog steeds veel onduidelijk is m.b.t. de relatie tussen de FG en de toezichthoudende autoriteit.

De FG heeft ingevolge artikel 39 lid 1 onderdeel b AVG een toezichthoudende taak. Hoe de toezichtstaken van de FG en de toezichthoudende autoriteit zich tot elkaar verhouden is niet heel duidelijk. Hun respectieve toezichthoudende taken hebben vaak betrekking op dezelfde verwerkingsverantwoordelijke. Dat werpt automatisch vragen op over de onderlinge 'gezagsverhouding' tussen FG en toezichthoudende autoriteit, eventuele verschillen in benadering, en wat zij elkaar mogen of moeten vertellen over nalevingskwesties. De AVG spreekt heel cryptisch van 'toezicht op de naleving' bij de FG, en 'toezicht op de toepassing' bij de toezichthoudende autoriteit. Waarom? Het is ook niet duidelijk wanneer het voeren van overleg tussen de FG en de toezichthoudende autoriteit 'passend' is, zoals bedoeld in artikel 39 lid 1 onderdeel e AVG.

Wat betreft de benoeming van een FG zag het NGFG de volgende aandachtspunten:

1. Wat betekent precies: 'op grote schaal', waar dit deel uitmaakt van het criterium voor de verplichte benoeming van een FG?[2] Verantwoordelijken hebben behoefte aan meer houvast waar zij geconfronteerd worden met de mogelijke verplichting om een FG aan te stellen, en dus ook met het risico van hoge boetes. Een concretere uitleg van het criterium 'op grote schaal' is daarom heel belangrijk.

2. Hoe kun je weten of een bepaalde FG, of een bepaald FG-team, geschikt is voor de organisatie of groep organisaties waarvoor hij wordt aangesteld? Wanneer voldoet de invulling van die rol aan de eisen? Dat de FG ook een onafhankelijke en toezichthoudende rol heeft, maakt

---

* **Jan de Zeeuw is voorzitter van het NGFG.**

1 Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, gebaseerd op artikel 29 van Richtlijn 95/46/EG. De groep bestaat uit een vertegenwoordiger van de door iedere lidstaat aangewezen toezichthoudende autoriteit(en), een vertegenwoordiger van de voor de Europese instellingen en organen opgerichte toezichthouder voor gegevensbescherming (EDPS), en een vertegenwoordiger van de Europese Commissie.

2 'Buiten de overheid is een FG verplicht als een verwerkingsverantwoordelijke of verwerker hoofdzakelijk is belast met verwerkingen die (…) observatie *op grote schaal* van betrokkenen vereisen, of met *grootschalige* verwerking van bijzondere categorieën van gegevens (…)' (artikel 37 lid 1 onderdeel b en c AVG).

deze vraag des te meer relevant. Alleen maar op passieve wijze bereikbaar zijn is dan niet voldoende. Het NGFG vindt namelijk dat de rol van de FG serieus moet worden ingevuld. De *span of control* wat betreft de omvang van de verwerkingen of de organisatie(s) waarvoor hij is aangesteld, is daarbij van invloed. Wanneer het toezicht zich bijvoorbeeld zal uitstrekken over meerdere concerns, zal een deeltijd-FG in zijn eentje niet of nauwelijks op voldoende wijze een oogje in het zeil kunnen houden. Wanneer is er echter sprake van voldoende capaciteit voor de FG om te kunnen spreken van een geloofwaardige invulling?

3. Nieuw is de mogelijkheid in de AVG om een 'externe FG' aan te stellen, op grond van een dienstverleningsovereenkomst. Ten aanzien van de externe FG spelen echter nog verschillende vragen. Zo is het de vraag hoe in dat geval de bijzondere bevoegdheden van de FG moeten worden uitgelegd. Het gaat daarbij om bevoegdheden zoals onafhankelijkheid, betrokken worden bij alle zaken met betrekking tot gegevensbescherming, het recht op hulpbronnen, en rapportage aan het hoogste managementniveau. De richtlijnen suggereren dat het bij een externe FG ook kan gaan om een 'FG-team'. Betekent dat dat de vergaande bevoegdheden van toepassing zijn op alle leden van het externe team? Kan een externe FG ook een rechtspersoon zijn, in plaats van een natuurlijk persoon? Een andere vraag is hoe een externe FG-dienstverlener situaties moet vermijden waarbinnen een belangenconflict kan ontstaan. Moet de FG-functie niet worden gescheiden van de adviestak van de externe dienstverlener, aangezien die ook andere belangen kan hebben bij opdrachten van de verwerkingsverantwoordelijke?

Het NGFG zou op deze vragen graag de antwoorden zien.

Dan de eisen rond de onafhankelijkheid van een FG:

1. De toezichthoudende taak van de FG wordt in de richtlijnen te weinig uitgewerkt. Er is echter juist ten aanzien van díe taak een grote behoefte aan richtlijnen. Intern toezicht organiseren binnen een organisatie is een complex onderwerp, en ook lastig om goed te borgen. De FG moet zijn adviserende taak combineren met toezicht houden en dat brengt al beperkingen met zich mee. Die taken kunnen immers met elkaar gaan 'botsen'. Zo is het voor een adviseur mogelijk de verantwoordelijke te adviseren om een bepaald risico te accepteren. Bijvoorbeeld omdat bij overtreding van de regels de kans op financiële gevolgen toch maar klein is. Een toezichthouder zie je dat niet snel doen. Nog lastiger wordt het als de FG zijn toezicht zou moeten combineren met het uitvoeren van (andere) taken die de AVG aan een verwerkingsverantwoordelijke oplegt. De FG kan niet geacht worden taken uit te voeren waar hij zelf toezicht op houdt. Van hem kan dus ook niet verwacht worden dat hij taken uitoefent op het gebied van gegevensbescherming, die door de verwerkingsverantwoordelijke moeten worden aangestuurd. Voorbeelden van zulke taken zijn: het uitvoeren van gegevensbeschermingseffectbeoordelingen, het treffen van beveiligingsmaatregelen en het verstrekken van persoonsgegevens. Aan de andere kant moet de FG wel een veelzijdig expert zijn op zijn vakgebied. Zijn deskundigheid moet ook optimaal binnen de organisatie kunnen worden benut. Hier is dus sprake van een dilemma. In verband met dit dilemma is het belangrijk om te weten waar de grenzen liggen, zowel voor de FG zelf, als voor zijn verantwoordelijke of verwerker. De functiescheiding tussen 'toezicht' en 'uitvoering' wordt door de richtlijnen echter niet of nauwelijks uitgewerkt.

2. Een ander punt van aandacht speelt in het kader van het voorschrift dat de verwerkingsverantwoordelijke of de verwerker ervoor moet zorgen dat eventuele andere taken van de FG niet tot een belangenconflict leiden. Welke functies en taken kunnen daar precies toe leiden? De vraag die voor velen relevant zal zijn, en waarvan het dus eigenlijk voor de hand ligt dat die zal worden beantwoord, is in hoeverre de rol van FG te combineren is met de rollen op het gebied van informatiebeveiliging. Het NGFG haalt het antwoord niet direct uit de richtlijnen.

Tot zover de opmerkingen zoals het NGFG die heeft geleverd op de consultatieversie van de richtlijnen. De richtlijnen zijn inmiddels aangepast naar aanleiding van de ontvangen feedback (versie van 5 april 2017). De Artikel 29-werkgroep heeft helaas op lang niet alle punten meer duidelijkheid gegeven. Wel heeft zij o.a. een nieuwe paragraaf (4.3) toegevoegd die gaat over de samenwerking van de FG met de toezichthoudende autoriteit en het optreden van de FG als zijn contactpunt.[3] Dat betreft het eerste punt van het NGFG, namelijk de relatie tussen de FG en de toezichthoudende autoriteit. Daarover wordt nu iets meer duidelijkheid gegeven. In de richtlijnen is hierover nu opgenomen dat de FG fungeert als aanspreekpunt, om de toegang van de toezichthoudende autoriteit tot de documenten en informatie van de verantwoordelijke of de verwerker te vergemakkelijken. Een kritische noot die je hierbij zou kunnen plaatsen, is dat je je kunt afvragen of dit nu bijdraagt aan de vrijwillige aanstelling van FG's door verantwoordelijken en verwerkers. Zo geformuleerd, zou dit verantwoordelijken misschien juist wel eens kunnen doen twijfelen aan de voordelen van een FG. Maar er staat ook iets tegenover. De FG mag namelijk op zijn beurt contact opnemen met, en advies vragen aan de toezichthoudende autoriteit. Artikel 39 lid 1 onderdeel e AVG bepaalt immers dat de FG, indien passend, de toezichthoudende autoriteit 'over elke andere kwestie kan raadplegen'. Het lijkt erop dat hiermee de spelregels zijn gegeven ter vervanging van het 'soepele samenspel' tussen FG en autoriteit zoals we dat tot nu toe kenden onder de Wbp.

3 De samenwerking met de toezichthoudende autoriteit en het optreden als contactpunt als bedoeld in artikel 39 lid 1 onderdeel d en e AVG.