MYOBI Opinion #10, 1 december 2016

Bijdrage van H. van der Linde RA, managing partner bij Europe Compliance

Functionaris Gegevensbescherming – een pracht professie

Overweging 97 naast artikel 37 uit de Europese Algemene verordening gegevensverwerking (Avg) geeft een belangrijke aanwijzing waaraan een Functionaris Gegevensbescherming (FG) moet voldoen om zijn taken en verplichtingen onafhankelijk te vervullen, ongeacht of hij in dienst is van de verwerkingsverantwoordelijke. Daarbij geeft deze overweging aan dat de FG toeziet op de verwerking door een overheidsinstantie[1] of een verwerkingsverantwoordelijke in de particuliere sector die als kerntaak heeft verwerkingsactiviteiten uit te voeren die grootschalige regelmatige en systematische observatie van betrokkenen vereisen dan wel dat de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van persoonsgegevens en van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten. In die situaties wordt een FG aangesteld die met deskundigheid omtrent gegevensbeschermingswetgeving en -praktijken de verwerkingsverantwoordelijke of de verwerker bij staat bij het toezicht op de interne naleving van deze verordening. Het vereiste niveau van deskundigheid dient met name te worden bepaald op grond van de uitgevoerde gegevensverwerkingsactiviteiten en de bescherming die voor de door de verwerkingsverantwoordelijke of de verwerker verwerkte gegevens vereist is.

Deze overweging stelt drie zaken aan de orde:

1. De FG wordt aangesteld door zowel een verantwoordelijke als een verwerker als de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, indien het om grootschalige verwerking van bijzondere categorieën van gegevens gaat of om verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen;
2. De FG dient een adequaat niveau van deskundigheid en ervaring te hebben om zijn taken en verplichtingen onafhankelijk te kunnen vervullen, en;
3. De FG behoeft niet in Loondienst te zijn maar mag ook als een externe FG worden ingehuurd, zolang de FG voldoet aan het onder punt 2 gestelde.

De meetlat voor de professionaliteit van de FG is hiermee gesteld. Deze meetlat kan feitelijk voor iedere FG worden gehanteerd. De professionaliteit van de FG betekent tevens verantwoordelijkheid voor de FG. Brengt nu deze verantwoordelijkheid ook risico's van aansprakelijkheid in het functioneren van de FG met zich mee? En indien zo, kunnen deze risico's worden gemitigeerd?

Aanstelling en positie van de FG

De FG wordt aangesteld door de verwerkingsverantwoordelijke (statutair bestuur van een organisatie) en de verwerker die namens de verwerkingsverantwoordelijke betrokken is bij de verwerking van persoonsgegevens. De Avg besteedt daarin ruim de aandacht in het betreffende artikel 'de aanwijzing van de FG' inzake de voorwaarden waaronder een FG wordt ingesteld. Aangegeven is dat een FG altijd wordt aangesteld indien de verwerkingsverantwoordelijke een overheidsinstantie is of de verwerkingsverantwoordelijke of de verwerker

[1] Met uitzondering van gerechten of onafhankelijke rechterlijke autoriteiten die handelen in het kader van hun gerechtelijke taken.

hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van persoonsgegevens[2]. Grootschalige verwerking is niet verder meer onderbouwd[3].

Ten aanzien van de positie stelt de Avg in artikel 38 verder dat de verwerkingsverantwoordelijke en de verwerker:

- De FG altijd tijdig bij alle aangelegenheden in verband met de bescherming van persoonsgegevens betrekt;
- De FG ondersteunt wordt in de uitvoering van al zijn taken inzake verwerkingsactiviteiten van persoonsgegevens en dat hem daartoe de middelen ter beschikking worden gesteld om die taken naar behoren te vervullen en in stand te houden;
- De FG geen instructies geven met betrekking tot de uitvoering van zijn taken;
- De FG niet kunnen ontslaan of straffen voor de uitvoering van zijn taken;

Verder wordt gesteld dat:

- De FG rechtstreeks verslag uitbrengt aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker;
- Betrokkenen met de functionaris voor gegevensbescherming contact kunnen opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten uit hoofde van de Avg;
- De FG met betrekking tot de uitvoering van zijn taken tot geheimhouding of vertrouwelijkheid is gehouden;
- De FG andere taken en plichten kan vervullen zolang taken of plichten niet tot een belangenconflict leiden.

Taken van de FG en de professionele betekenis

De Avg heeft een duiding gegeven van het minimum takenpakket van de FG. Daarbij vervult de FG ten minste de volgende taken:

- de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van deze verordening[4];
- toezien op naleving van deze verordening 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;
- desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan;
- met de toezichthoudende autoriteit samenwerken;
- optreden als contactpunt voor de toezichthoudende autoriteit inzake de met de verwerking verband houdende aangelegenheden.

Informeren en adviseren inzake verplichtingen uit de Avg omvat veel. Heel nadrukkelijk kunnen we stellen dat de FG de verplichtingen in de Avg moet kunnen interpreteren naar andere invalshoeken dan alleen de juridische invalshoek. In artikel 24 Avg, ook wel het artikel dat de 'Notion of Accountability' duidt, wordt gesproken over passende technische en organisatorische maatregelen en het kunnen waarborgen en kunnen aantonen dat deze overeenkomstig de Avg worden uitgevoerd. Deze bepaling alleen al betekent dat de FG kennis moet hebben van andere disciplines dan alleen de juridische. De FG zal kennis moeten hebben van die maatregelen. Deze maatregelen kunnen technisch van aard zijn met als kenmerk dat deze maatregelen gegevens, waaronder

---

[2] Persoonsgegevens met betrekking tot ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond, of gegevens die betrekking hebben op genetische bepaling, biometrische bepaling met het oog op de unieke identificatie van een persoon, gezondheid, of tot iemands seksueel gedrag of seksuele gerichtheid.

[3] In eerdere tekstversies van de Avg werd melding gemaakt van een organisatie met tenminste 250 FTE aan medewerkers of 5.000 verwerkingen van persoonsgegevens binnen een twaalfmaandsperiode.

[4] Aangevuld met andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen.

persoonsgegevens, transporteren binnen de ICT-infrastructuur. Daarnaast zijn er ook maatregelen betrokken die beveiligingshandelingen op de gegevenstransporten binnen de ICT-infrastructuur uitvoeren. Kortom de FG dient naast juridische kennis om de verplichtingen uit wetgeving te kunnen interpreteren ook duidelijk kennis te hebben omtrent ICT-infrastructuren, maatregelen om het transport en beveiliging van gegevens te kunnen beoordelen en te kunnen inzetten en misschien wel het belangrijkste hoe deze in de governance maatregelen (interne beheersing) van een organisatie moeten worden ingebed. De Notion of Accountability vereist daarbij dat de vroegere regel 'Comply or Explain' niet meer geldig is. Artikel 24 Avg vraagt nu 'Comply and Demonstrate Compliance'. Dat betekent dat de FG op een geheel andere wijze moet toezien hoe compliance wordt aangetoond.

Conclusies uit deze interpretatie

De conclusie is gerechtvaardigd dat de FG een goede theoretische en praktische onderbouwing nodig heeft om zich van zijn taken te kunnen kwijten, om de professionele taken te kunnen uitvoeren die hem wettelijk zijn opgedragen, ook vanuit de interpretatie van die taken. De Leergang Functionaris voor Gegevensbescherming[5] speelt hierop in door het bieden van een opleiding waar alle facetten aan de orde komen. Van de juridische en praktische interpretatie van de plichten uit die wetgeving tot het organiseren van de plichten in governance oplossingen. Dit omvat ook de te nemen passende technische en organisatorische maatregelen van die oplossingen en het vaststellen van compliance van de werking daarover, inclusief het afdoende vastleggen daarvan in een Privacy & Security Accounting administratie als basis voor het kunnen afleggen van verantwoording. Zonder een dergelijke gekwalificeerde opleiding staat een aangestelde FG wankel in zijn schoenen en niet zonder risico's inzake eigen functioneren.

Daarnaast is het van belang dat de aangestelde FG niet alleen goed is opgeleid, maar ook over een zekere professionele houding, een vorm van volwassenheid, beschikt in zijn onafhankelijkheid, zijn integriteit en niet in de laatste plaats zijn overtuigingskracht naar de hoogste leiding van de organisatie. Zonder deze professionele houding kan het vervullen van de rol van FG een uitdaging worden, ondanks alle goede theoretische en praktische onderbouwing opgedaan in een afgeronde Leergang FG.

Ervaringen uit de praktijk

Uit de contacten met deelnemers uit de Leergang FG en in de uitvoering van diverse rollen als FG door medewerkers binnen Duthler Academy bij klanten komt een aantal ervaringsfeiten naar de oppervlakte. Een paar voorbeelden:

a. De materie om compliance met de Avg (en natuurlijk ook met de Wet bescherming persoonsgegevens (Wbp)) te organiseren is complex. Het blijkt een uitdaging om zowel de hoogste leiding, maar ook de eerste twee van de drie Lines of Defense[6] te overtuigen omtrent te nemen maatregelen, de betekenis daarvan en de noodzaak tot waarborging en zekerstelling van het aantonen van compliance met Avg van de genomen maatregelen. De FG loopt hierbij soms tegen zijn 'eigen eenzame' positie aan;
b. Als gevolg mist de FG zijn klankbord die hij nodig heeft om de adviezen te toetsen die hij heeft gevormd en uiteindelijk naar de hoogste leiding wil communiceren. Ook de FG ervaart hierin dat zijn professional judgement een complexe materie behelst. Daarin mag en wil hij niet falen. De FG wil niet aangesproken worden dat hij tekort is geschoten in zijn advies aan de hoogste leiding, zijn overtuigingskracht daarin en wellicht ook zijn geloofwaardigheid;
c. De FG komt helemaal in een lastige positie indien de hoogste leiding het wel goed vindt dat hij een FG heeft aangesteld. Indien de hoogste leiding verder geen notie neemt van de FG-adviezen, misschien wel zegt tegen de FG 'los maar op', is de FG in dezelfde positie beland als voorheen het hoofd ICT. Met dien verstande dat de FG, als onafhankelijk adviseur en intern toezichthouder, geen mogelijkheden en al

[5] http://www.duthleracademy.nl/nl/leergang-fg, Leergang Functionaris Gegevensbescherming ingesteld door Duthler Academy
[6] In het Governance Risk en Compliance model herkent men 'Three Lines of Defence' (3LoD). Eerste LoD betreft het lijnmanagement. De tweede LoD ondersteunt het lijnmanagement (Beleidsvoorbereiding en integrale risk assessment). De derde LoD betreft Internal Audit.

helemaal geen bevoegdheid heeft ook maar iets op te lossen. Ofwel komt de FG in het nauw doordat de hoogste leiding nog steeds geen verantwoordelijkheid wil nemen.

Uit deze drie (niet limitatieve voorbeelden) komt naar voren dat de FG-rol een risico positie kan zijn. Indien de FG niet serieus wordt genomen, de hoogste leiding tegenover de Autoriteit Persoonsgegevens (AP) als gevolg in het nauw wordt gebracht, zal deze 'zijn' FG hierop aanspreken. *De FG staat dan machteloos!*

Hoe kan de rol van FG robuust worden gemaakt

Er zijn diverse mogelijkheden om de uitvoering van de rol van FG robuust te maken:

- De net aangestelde FG aanvaardt de uitdaging deze rol in te vullen onder de uitdrukkelijke eis dat hij een adequate opleiding krijgt. Zonder adequate opleiding heeft geen enkele aangestelde FG de mogelijkheid professioneel, betrouwbaar en geloofwaardig zijn rol in te vullen;
- In het aanstellingsgesprek stelt de FG de voorwaarden op te zullen stellen waaronder hij zijn rol adequaat wil gaan invullen. Het gaat erom dat over en weer het verwachtingspatroon wordt vastgesteld en dat deze verwachtingspatronen in professionaliteit door beiden worden gerespecteerd om naleving te kunnen garanderen;
- De FG zal bij zijn aanstelling verzoeken om een aanspreekpunt te krijgen binnen de Raad van Toezicht (of Commissarissen), en bijv. de 'Audit Committee' te krijgen. Beter nog zou het zijn indien de FG wordt aangesteld door de Raad van Toezicht en/of Audit Committee, waarbij het eenvoudiger wordt om de afspraken onder de eerste twee bullets gematerialiseerd te krijgen;
- Indien de FG wordt ingehuurd, hetgeen naar verwachting een gebruikelijke keuze kan gaan worden, worden bovenstaande drie punten in de afspraken geformuleerd. In dit kader zal de aanstelling van de FG gestuurd worden vanuit afspraken in een 'Weerbare Bewerkersovereenkomst' (Wbo) onder regie van een Trusted Third Party[7];
- De FG maakt gebruik van de mogelijkheid om te sparren met vakgenoten binnen de FG community. Duthler Academy organiseert daartoe regelmatige bijeenkomsten waar gezamenlijk of met enkele deelnemers uit die FG community kan worden gesproken inzake de adviezen die de FG wil geven eventueel gebaseerd op observaties vanuit zijn toezichtsrol;
- De FG verlangt het gebruik van zijn FG-dossier. Dit is vormgegeven door een Dossier Personen (DP) welke beheerd wordt door de Trusted Third Party. Door hierin al zijn observaties, adviezen, constateringen en alles wat hij van belang vindt te bewaren, kan de FG zijn verweer opbouwen, mocht een dispuut met de hoogste leiding escaleren en hij ook niet voldoende steun vindt bij zijn aanspreekpunt in de Raad van Toezicht.

Het is van belang in de open dialoog naar de aanstelling bovenstaande punten met de hoogste leiding te bespreken en het liefst ook met (het aanspreekpunt binnen) de Raad van Toezicht. Indien dit tot heldere afspraken heeft geleid en de mogelijkheden geboden, zal de aangestelde FG zijn taken professioneel naar behoren en bovenal met uitdaging en plezier kunnen invullen.

Voor de hoogste leiding geeft deze opinion context aan wat die hoogste leiding zal willen bereiken in transparante naleving van de Avg (en Wbp). Het motto daarin voor de hoogste leiding, de verantwoordelijke:

"Laat de AP niet het eindpunt worden van een dispuut. Dat helpt noch u noch de door u aangestelde FG. Het gaat om respect en wederzijds vertrouwen in de kundige adviezen van de FG en de respectvolle opvolging, binnen de prioriteiten en mogelijkheden van de organisatie, bekrachtigd door de hoogste leiding".

[7] Mind Your Own Business Information (www.MYOBI.eu) is een geschikt voorbeeld daarvoor