MYOBI Opinion, #12, 17 januari 2017

Bijdrage door mr. dr. Anne-Wil Duthler, advocaat bij First Lawyers

De Functionaris Gegevensbescherming in het hart van de Europese Algemene verordening gegevensbescherming

Op 13 december 2016 heeft de Artikel 29-werkgroep[1] richtlijnen voor functionaris gegevensverwerking aanvaard.[2] Deze richtlijnen zijn vervolgens in consultatie gegaan. Tot 31 januari 2017 is er gelegenheid feedback op deze richtlijnen in te sturen.

In de richtlijnen wordt door de Artikel 29-werkgroep een aantal interessante uitspraken gedaan en veronderstellingen en uitgangspunten van de Avg bevestigd. In deze opinie licht ik er enkele *highlights* uit. In mijn volgende opinie besteed ik aandacht aan de vraag wanneer organisaties verplicht zijn een FG aan te stellen. Ook daarvoor biedt de Artikel 29-werkgroep handreikingen. Maar nu eerst de FG als kernfunctie in de Avg en zijn/haar rol in het kader van '*accountability*'.

De Artikel 29-werkgroep begint met te bevestigen dat de AVG: *'will provide a modernised, accountability-based compliance framework for data protection in Europe. Data Protection Officers ('DPO's) will be at the heart of this new legal framework for many organisations, facilitating compliance with the provisions of the GDPR'.*

Een mooie samenvatting van de rol en positionering van de FG. De Avg wordt gepositioneerd als een modern, op accountability gebaseerd compliance raamwerk voor gegevensbescherming. FG's functioneren in het hart van dit raamwerk. De FG wordt gezien als een hoeksteen van accountability, faciliteert compliance en is een intermediair tussen verschillende stakeholders zoals toezichthouders, betrokkenen en businessunits in organisaties. Een FG is niet persoonlijk verantwoordelijk en aansprakelijk voor compliance met de Avg. Dat zijn en blijven de verantwoordelijken én bewerkers. De verantwoordelijken en bewerkers hebben wel een cruciale rol om ervoor te zorgen dat de FG zijn taak effectief kan uitvoeren. De FG moet voldoende autonomie krijgen en resources.

De Avg erkent de FG als een sleutelfunctionaris in het nieuwe *data governance systeem* en stelt de voorwaarden voor de aanwijzing, positie en taken. De richtlijnen geven een nadere toelichting op het bepaalde in de Avg en bevatten best practice aanbevelingen. Hieronder volgt een weergave van de toelichting en aanbevelingen voor de belangrijkste onderwerpen, waaronder de taken van de FG, deskundigheid en vaardigheden en positie in de organisatie.

[1] De Artikel 29-werkgroep is een werkgroep die is ingesteld onder de Europese richtlijn 95/46/EC en bestaat uit vertegenwoordigers van de nationale toezichthoudende autoriteiten, vertegenwoordigers van EU-instellingen en een vertegenwoordiger van de Europese Commissie. Het opereert onafhankelijk en heeft een adviserende taak.

[2] *Article 29 Data Protection Working Party, 16/EN WP 243, Guidelines on Data Protection Officers (DPO's)*, 13 december 2016.

Verplichte aanwijzing van een FG

Tenzij het evident is, beveelt de Artikel 29-werkgroep verantwoordelijken en bewerkers aan om de interne analyse om wel of niet een FG aan te stellen te documenteren. Zodat zij in staat zijn om aan te tonen dat de relevante factoren op een juiste wijze in overweging zijn genomen. De werkgroep verwijst daarbij naar artikel 24 van de Avg; de kernbepaling als het gaat om accountability.

FG voor de bewerker

De verplichte aanwijzing van een FG is zowel op de verantwoordelijke van toepassing als op de bewerker. Daar waar de verantwoordelijke verplicht is een FG aan te stellen, hoeft dat niet altijd ook te gelden voor de bewerker en vice versa. Desondanks beveelt de Artikel 29-werkgroep wel aan om ook dan een FG aan te stellen. Zo'n FG van een bewerker houdt vervolgens niet alleen toezicht op de verwerkingen die de bewerker voert ten behoeve van de verantwoordelijke, maar ook op de verwerkingen waarvoor de bewerker zelf verantwoordelijke is.

Taken FG

Opvallend is dat de Artikel 29-werkgroep de taken van de FG genoemd in artikel 39, eerste lid van de Avg als een minimum beschouwt. Op een aantal specifieke taken gaat zij nader in.

Monitoring compliance

De eerste belangrijke taak van een FG is conform artikel 39 lid 1 sub b het monitoren van compliance met de Avg. De Artikel 29-werkgroep koppelt deze onmiskenbaar aan artikel 24 lid 1 van de Avg, het artikel dat gaat over accountability. Tot deze taak behoort:

- Het verzamelen van informatie om verwerkingsactiviteiten te kunnen identificeren;
- Het analyseren en controleren van de compliance van de verwerkingsactiviteiten;
- Het informeren en adviseren van en aanbevelingen geven aan de verantwoordelijke.

Compliance is en blijft wel een *corporate responsiblity*.[3] Het is de verantwoordelijke en de bewerker die passende technische en organisatorische maatregelen moeten nemen om zeker te stellen en aan te tonen dat gegevens worden verwerkt conform de Avg.

Data protection impact assessment (DPIA)

Een tweede taak betreft het ondersteunen van de verantwoordelijke bij het uitvoeren van een DPIA. Ook hier geldt dat het de verantwoordelijkheid is van de verantwoordelijke om een DPIA uit te voeren. De Artikel 29-werkgroep beveelt de verantwoordelijke onder meer in de volgende omstandigheden het advies van de FG te vragen:

- Wel of niet een DPIA uitvoeren;
- Op basis van welke methode een DPIA uit te voeren;
- Een DPIA in huis zelf uitvoeren of uitbesteden;
- Welke waarborgen (inclusief technische en organisatorische maatregelen) toe te passen om risico's te mitigeren voor de rechten en belangen van betrokkenen; *en*
- Is een DPIA correct uitgevoerd en of de uitkomsten compliant zijn met de Avg.

[3] Als er een geval is van non-compliance kan dat de FG niet persoonlijk worden aangerekend.

Als de verantwoordelijke het advies van de FG niet opvolgt, moet gedocumenteerd worden waarom zij dat niet doet.

De Artikel 29-werkgroep adviseert om in het contract met de FG precies vast te leggen welke taken de FG heeft ten aanzien van de DPIA en wat de reikwijdte is. Ook medewerkers, management en andere stakeholders moeten hierover worden geïnformeerd.

De rol van de FG in het bijhouden van het register van verwerkingen

Het is de taak van de verantwoordelijke, cq. bewerker om een register bij te houden van verwerkingen. Nu de Avg een lijst van taken opsomt4 die niet uitputtend is of bedoeld is als een minimum is het goed voorstelbaar dat de FG de taak krijgt het register bij te houden. Dit register is een van de tools die de FG nodig heeft om compliance met de Avg te kunnen monitoren en de verantwoordelijke en verwerker daarover te adviseren. Het bijhouden van het register is tevens een voorwaarde voor compliance en op zichzelf te beschouwen als een effectieve accountability maatregel. Dit betekent dat het register actueel en volledig moet zijn.

Risk-based benadering

De accountability eis – het aantoonbaar voldoen aan de Avg – vraagt om een evidence-based benadering. Het bijhouden van het register bijvoorbeeld dat steeds volledig en juist moet zijn is immers een voorwaarde voor het kunnen aantonen van de compliance met de Avg. Net zoals het bewijs dat de maatregelen hebben gewerkt om incidenten tijdig te kunnen detecteren en eventuele datalekken tijdig te kunnen melden bij de toezichthouder en zo nodig betrokkenen. De uitoefening van de taken van de FG daarentegen is risk-based.

De FG moet bij de uitvoering van zijn taken naar behoren rekening houden met het aan verwerkingen verbonden risico, en met de aard, omvang, context en de verwerkingsdoeleinden.[5] Dit betreft een algemeen principe, dat relevant is voor veel aspecten van zijn dagelijkse werkzaamheden. Het vereist dat de FG prioriteiten aanbrengt in zijn werkzaamheden en zijn focus legt op zaken met hogere risico's voor gegevensbescherming.

Deskundigheid en vaardigheden van de FG

De Avg schrijft voor dat de FG 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] Overweging 97 bepaalt dat het vereiste niveau van deskundigheid met name dient te worden bepaald op grond van de uitgevoerde gegevensverwerkingsactiviteiten en de bescherming die voor de verwerkte gegevens vereist is. De Artikel 29-werkgroep zegt hierover dat het kennisniveau zal moeten sporen met en of evenredig moet zijn aan de gevoeligheid, complexiteit en hoeveelheid van de gegevens die worden verwerkt. Als er bijvoorbeeld veel gevoelige data worden verwerkt en de gegevensverwerkingsactiviteiten zijn bepaald complex heeft de FG een hoger kennisniveau en support nodig. Ook maakt het verschil of gegevens systematisch buiten de EU worden verwerkt of dat dat incidenteel gebeurt.

[4] Zie artikel 39, eerste lid Avg.

[5] Op grond van artikel 39, tweede lid.

[6] Zie Artikel 37 lid 5.

Professionele kwaliteit

Hoewel de Avg geen expliciete eisen stelt, stelt de Artikel 29-werkgroep dat de FG expertise moet hebben op het gebied van nationale en Europese gegevensbeschermingswetgeving en praktijken, en een diepgaand begrip[7] van de Avg. De werkgroep merkt daarbij op dat het behulpzaam is als de nationale toezichthouders adequate en regelmatige training promoten. Daarnaast is kennis van de bedrijfssector en de organisatie van de verantwoordelijke nuttig. De FG moet ook voldoende begrip hebben van de operationele processen[8] die worden uitgevoerd alsook van de informatiesystemen en de behoefte van de verantwoordelijke aan databeveiliging.

Vermogen taken te vervullen

Het vermogen om zijn taken te vervullen ziet niet alleen op de persoonlijke kwaliteiten en kennis van de FG, maar ook op de positie in de organisatie. De persoonlijke kwaliteiten hebben bijvoorbeeld betrekking op integriteit en hoge professionele ethiek.[9] Onder meer om die reden heeft de Duthler Academy een werkgroep ethiek opgezet.[10] De primaire zorg van een FG zou moeten zijn het op gang brengen en mogelijk maken van compliance met de Avg. De FG speelt een sleutelrol bij het creëren van een cultuur van gegevensbescherming binnen de organisatie en helpt bij het implementeren van essentiële elementen van de Avg. Denk bij het laatste aan de beginselen van gegevensverwerking, rechten van betrokkenen, gegevensbescherming by design and by default, registers van verwerkingen, informatiebeveiliging en de afhandeling van datalekken.

Service contract

Het is mogelijk om een FG in te huren van een organisatie buiten die van de verantwoordelijke of bewerker. Ook die FG moet aan alle eisen van de Avg voldoen en er mag geen sprake zijn van belangenverstrengeling. Tegelijkertijd wordt ook die FG beschermd door de bepalingen van de Avg die zien op bijvoorbeeld ontslagbescherming. Daarnaast mag het servicecontract niet 'unfair' worden beëindigd. Het voordeel van een servicecontract met een externe organisatie is dat individuele vaardigheden en sterktes van meerdere individuen kunnen worden benut zodat zij als team efficiënter hun cliënten kunnen bedienen.

Positie

De FG moet in staat zijn zijn taken en verplichtingen onafhankelijk te vervullen, ongeacht of hij in dienst is van de verantwoordelijke. [11]

Betrokkenheid van de FG

De FG moet in alle zaken die gerelateerd zijn aan dataprotectie in een zo vroeg mogelijk stadium worden betrokken. Het is belangrijk dat hij of zij wordt gezien als een discussiepartner binnen de organisatie en dat hij of zij deelneemt aan de relevante werkgroepen binnen de organisatie.

---

[7] De artikel 29 werkgroep spreekt van '*understanding*'.

[8] 'Processing operations carried out'.

[9] High professional ethics.

[10] De werkgroep ethiek is in december een eerste keer bij elkaar geweest. Belangstellenden kunnen zich voor deelname nog aanmelden.

[11] Zie overweging 97 van de Avg.

De organisatie moet daarom waarborgen dat de FG regelmatig wordt uitgenodigd voor vergaderingen van het senior en *middle* management. Als er besluiten worden voorgenomen dan dient alle relevante informatie tijdig aan de FG worden verstrekt zodat hij of zij in staat is adequaat advies te geven. Aan het advies van de FG dient het juiste gewicht worden gegeven. Als ervan wordt afgeweken, dan beveelt de Artikel 29-werkgroep aan om de overwegingen daarvoor goed te documenteren. De FG moet onmiddellijk worden geconsulteerd op het moment dat er een datalek of ander incident heeft plaatsgevonden. In voorkomende gevallen zouden de verantwoordelijke en de bewerker gegevensbeschermingsrichtlijnen en programma's kunnen ontwikkelen die uiteenzetten wanneer de FG moet worden geconsulteerd.

Benodigde middelen

De volgende aspecten moeten daarbij in aanmerking worden genomen:

- Support van de functie van de FG door het senior management zoals het niveau van de Raad van Bestuur (board level);
- Voldoende tijd voor de FG om zijn taken te vervullen;
- Financiën, infrastructuur, faciliteiten, instrumenten en een staf in voorkomende gevallen;
- Officiële aankondiging van de aanstelling van de FG zodat de gehele staf op de hoogte is van het bestaan en functie van de FG;
- Benodigde toegang tot andere diensten, zoals human resources, juridische zaken, IT, beveiliging, etc., zodat de FG essentiële ondersteuning, input en informatie kan ontvangen van die andere diensten;
- Permanente training: de FG moet de gelegenheid hebben om *up to date* te blijven van relevante ontwikkelingen met als doel op een steeds hoger kennisniveau te komen. De FG moet gestimuleerd worden om te participeren in trainingen en andere vormen van professionele ontwikkeling; *en*
- Afhankelijk van de omvang en structuur van een organisatie kan het noodzakelijk zijn om een FG-team inclusief staf op te zetten. In die gevallen moet de structuur van het team en de taken en verantwoordelijkheden van elk lid van het team duidelijk beschreven zijn.

In het algemeen geldt dat hoe complexer en gevoeliger de processing operations, hoe meer resources aan de FG ter beschikking moeten worden gesteld.

Geen instructies en onafhankelijk handelen

Art. 38 lid 3 bevat enige basisgaranties om ervoor te zorgen dat de FG in staat wordt gesteld zijn taken op een voldoende autonome wijze uit te voeren binnen zijn organisatie. In het bijzonder zijn verantwoordelijken en bewerkers verplicht ervoor te zorgen dat de FG 'geen enkele instructie krijgt voor de uitoefening van zijn taken'. Overweging 97 voegt daaraantoe dat de FG – of hij nu wel of niet een medewerker is van de verantwoordelijke - , in een positie moet worden gebracht dat hij zijn taken en bevoegdheden op een onafhankelijke wijze kan uitoefenen.

Dit betekent onder meer dat de FG geen instructie mag krijgen hoe om te gaan met een specifieke zaak, welk resultaat bijvoorbeeld eruit moet komen, hoe een bezwaar of klacht te behandelen en of nu wel of niet de AP moet worden geconsulteerd. Ook mag de FG niet worden geïnstrueerd om een bepaald standpunt in te nemen of hoe een specifieke wettelijke bepaling moet worden geïnterpreteerd. De autonomie van de FG gaat echter niet zo ver dat de FG besluitvormingsmacht heeft die verder gaan dan de uitvoering van de in artikel 39 Avg genoemde taken.

Daar staat wel tegenover dat de verantwoordelijke of bewerker te allen tijde zelf verantwoordelijk blijft voor compliance met de privacywetgeving en in staat moet zijn de compliance aan te tonen. Letterlijk staat er 'to demonstrate compliance'. Als de verantwoordelijke of bewerker beslissingen neemt die in tegenspraak zijn met de Avg en het advies van de FG, moet de FG de mogelijkheid hebben zijn 'dissenting opinion' duidelijk te maken aan hen die de beslissingen nemen.

Geen ontslag of straf

Artikel 38 lid 3 van de Avg bepaalt dat de FG door de verantwoordelijke of bewerker niet wordt ontslagen of gestraft voor de uitvoering van zijn taken als FG. Deze bepaling versterkt de autonomie van de FG en moet eraan bijdragen dat de FG zich onafhankelijk gedraagt en zich voldoende beschermd weet bij de uitoefening van zijn taken.

Sancties kunnen zich in verschillende vormen voordoen en direct of indirect van aard zijn. Denk aan uitstel van promotie of geen promotie, geen carrièreontwikkeling, geen *employee benefits* die andere werknemers wel krijgen. Ook het dreigen daarmee kan al als sanctie worden gekwalificeerd. Het is niet noodzakelijk dat de sanctie daadwerkelijk wordt toegepast. Ontslag om andere redenen dan die van de uitoefening van zijn taken als FG, blijft – uiteraard – nog steeds mogelijk.

De Artikel 29-werkgroep pleit voor een degelijk contract. Hoe steviger een contract is en hoe meer garanties deze bevat tegen oneerlijk ontslag, hoe makkelijker het zal zijn voor een FG om zich onafhankelijk te gedragen.

Belangenconflict

De FG kan andere taken en plichten vervullen dan die voortvloeien uit zijn functie van FG.[12] De verantwoordelijke of de bewerker moet ervoor zorgen dat deze niet tot een belangenconflict leiden. De afwezigheid van een belangenconflict hangt nauw samen met de eis van onafhankelijkheid aan de FG. Dit betekent dat de FG volgens de Artikel 29-werkgroep nooit in een positie terecht mag komen dat hij doel en middelen van de gegevensverwerking bepaalt. Voorbeelden van functies die volgens de art. 29 werkgroep niet gecombineerd kunnen worden met die van FG zijn seniormanagementposities zoals CEO, COO, CFO, CMO[13], hoofd van een marketingafdeling, hoofd van een personeelsafdeling of hoofd van een ICT-afdeling, maar ook lagere functies in de organisatie als zij de bepaling van doel en middelen van een gegevensverwerking met zich meebrengen. De Artikel 29-werkgroep beveelt verantwoordelijken en bewerkers aan om de posities die niet te verenigen zijn met de FG-functie te identificeren; interne regels te formuleren om belangenconflicten te voorkomen; een algemene uitleg van belangenconflicten te formuleren en te verklaren dat hun FG geen belangenconflict heeft als een manier om bewustzijn te creëren; en waarborgen in de interne regels op te nemen en te verzekeren dat de vacaturetekst voor de FG-functie of service contract voldoende precies en gedetailleerd staat beschreven om belangenconflicten te voorkomen. Belangenconflicten kunnen verschillende vormen aannemen, al naar gelang een DPO intern wordt gerekruteerd of extern geworden.

Tot slot

Overall valt op dat ook de Artikel 29-werkgroep accountability als leidend principe neemt bij de uitwerking van zijn functie, positie en taken. Uitvoerig beschrijft de werkgroep de taken en de positie van de FG. Hoewel veel van de aanbevelingen evident lijken, is het prettig dat de werkgroep deze nog eens heeft uitgeschreven. Hoe vaak krijgt een FG niet de vraag gesteld waar een recht of verplichting omtrent zijn functioneren staat 'in de wet'. Het is plezierig en handig dat een FG in zo'n geval kan verwijzen naar deze richtlijnen.

Tot 31 januari aanstaande is er gelegenheid zoals gesteld feedback te sturen op deze richtlijnen. Graag nodig ik de studenten van de Duthler Academy uit om zo nodig input daarvoor te leveren voor 24 januari aanstaande.

[12] Volgens het zesde lid van artikel 38 Avg.

[13] Chief Medical Officer.