Functionaris voor de Gegevensbescherming

October 20, 2017

AVGB-update: Functionaris voor de Gegevensbescherming

Inleiding

In deze AVGB-update staat de functionaris voor de gegevensbescherming centraal (de FG). De FG is een natuurlijk persoon die toeziet op de verwerking van persoonsgegevens binnen een organisatie. De FG is daarmee een soort ‘interne toezichthouder’.

Anders dan onder de Richtlijn 95/46/EG en de implementatie daarvan in de Wet bescherming persoonsgegevens (de Wbp), zijn bepaalde organisaties onder de AVGB verplicht om een FG aan te stellen. Onder de Wbp is het aanstellen van een FG ‘slechts’ een mogelijkheid:“(…) een verantwoordelijke (…) kan een eigen functionaris voor de gegevensbescherming benoemen”.

De AVGB bevat echter gedetailleerde regelgeving omtrent de aanstelling van een FG. Voor bepaalde organisaties (zowel verantwoordelijken als verwerkers) is het benoemen van een FG vanaf 25 mei 2018 verplicht. Zodra de AVGB van toepassing is, wordt de FG een hoofdrolspeler waar het gaat om privacy compliance binnen organisaties. De FG streeft de naleving van de AVGB binnen de organisatie na en treedt op als contactpersoon voor de relevante stakeholders (waaronder de betrokkenen en de Autoriteit Persoonsgegevens).

Verplichte aanwijzing FG

Op grond van de AVGB is een organisatie verplicht een FG aan te wijzen, indien:

a. de verwerking wordt verricht door een overheidsinstantie of een overheidsorgaan (met uitzondering van gerechten bij de uitoefening van hun rechterlijke taken);
b. de organisatie hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
c. de organisatie hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van persoonsgegevens (bijvoorbeeld gegevens over de gezondheid), of van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

De punten b) en c) bevatten enkele abstracte begrippen. Relevant in dit kader zijn de richtlijnen van de Artikel 29-werkgroep van Europese privacytoezichthouders (de WG29), waarin aan deze abstracte begrippen een concretere invulling wordt gegeven.

Het begrip ‘hoofdzakelijk’ ziet op kerntaken van een organisatie: de belangrijkste activiteiten die nodig zijn om het doel van de organisatie te bereiken. Hieronder vallen in beginsel niet de ondersteunende activiteiten van organisaties

zoals de salarisverwerking van de werknemers en standaard ICT-ondersteuning.

Wat betreft het begrip ‘verwerking op grote schaal’ geldt dat dit niet gekoppeld is aan concrete cijfers. Diverse factoren dragen bij aan het oordeel dat sprake is van een verwerking op grote schaal, waaronder het aantal betrokkenen, de duur van de verwerking en de geografische reikwijdte ervan.

‘Regelmatige en stelselmatige observatie’ omvat in ieder geval alle vormen van ‘tracking‘ en ‘profiling‘ op het internet, waaronder het tonen van advertenties op basis van het internetgebruik van de betrokkene. Het begrip observatie in dit kader is echter niet beperkt tot de online omgeving. Onder het begrip ‘regelmatig’ verstaat de WG29 een of meer van de volgende voorbeelden: (i) voortdurend of gedurende een bepaalde periode, met bepaalde tussenpozen, (ii) terugkerend of op vaste tijden herhaald of (iii) constant of periodiek. Onder het begrip ‘stelselmatig’ verstaat de WG29 een of meer van de volgende voorbeelden: (i) op basis van een systeem, (ii) vooraf geregeld, georganiseerd of systematisch, (iii) als onderdeel van een algemeen plan voor het verzamelen van gegevens of (iv) als onderdeel van een strategie.

De aanstelling van de FG is uiteindelijk een verantwoordelijkheid van de organisatie zelf. Tenzij het op voorhand duidelijk is dat de organisatie geen plicht heeft om een FG aan te stellen, raden wij organisaties aan de interne analyse omtrent de niet-aanstelling van een FG steeds schriftelijk vast te leggen met het oog op het (ook achteraf) kunnen aantonen van de naleving van de AVGB.

Overigens staat het organisaties altijd vrij om op vrijwillige basis een FG aan te stellen. Organisaties dienen zich er dan wel bewust van te zijn dat in dat geval de FG dezelfde positie, rechten en plichten heeft als een FG die op grond van de AVGB verplicht is. In plaats van het aanstellen van een FG kunnen organisaties er in dit geval ook voor kiezen om bijvoorbeeld een (externe) privacy adviseur in dienst te nemen.

Aanstelling FG binnen een concern

Een groep van ondernemingen kan één FG aanwijzen, mits vanuit elke vestiging van de organisatie gemakkelijk contact kan worden gelegd met de FG. Bovendien zullen organisaties er rekening mee moeten houden dat de FG effectief moet kunnen samenwerken met en worden benaderd door lokale toezichthoudende autoriteiten en betrokkenen (zowel van binnen als van buiten de organisatie). De WG29 raadt aan dat de FG binnen de EU wordt geplaatst, maar dit is niet verplicht (bijvoorbeeld indien de verantwoordelijke geen vestiging binnen de EU heeft).

Dat er vanuit elke vestiging van de organisatie gemakkelijk contact moet kunnen worden gelegd met de FG, betekent in de praktijk onder andere dat de contactgegevens van de FG binnen de organisatie bekend moeten zijn, zodat bijvoorbeeld een werknemer de FG direct en vertrouwelijk kan benaderen, zonder dat de werknemer deze contactgegevens eerst moet opvragen bij zijn of haar leidinggevende. De organisatie kan bijvoorbeeld de gegevens van de FG publiceren op het intranet of op haar website.

Verder betekent ‘gemakkelijk contact leggen’ dat de communicatie tussen de FG en de betrokkene en toezichthoudende autoriteit dient plaats te vinden in de taal of talen die gebruikt wordt/worden door de betrokken autoriteit of betrokkene. Dit betekent niet dat de FG alle talen van de EU-lidstaten hoeft te spreken. Het is voldoende indien hij of zij wordt ondersteund door een team waardoor het voor alle betrokken toezichthouders en de betrokkenen mogelijk is om in hun eigen taal contact te leggen met de FG. In dit verband is ook van belang dat de FG doorgaans een redelijke termijn zal worden gegund om te reageren op verzoeken van toezichthouders en betrokkenen.

Deskundigheid en vaardigheden van de FG

De FG dient te worden aangewezen op grond van zijn of haar professionele kennis en vaardigheden, en in het

bijzonder zijn of haar deskundigheid op het gebied van privacyregelgeving. Hier geldt dat hoe complexer de verwerkingen binnen de organisatie zijn, hoe meer bijzondere persoonsgegevens er worden verwerkt, of hoe meer landen buiten de EU de gegevens ontvangen, des te meer expertise er van de FG verwacht wordt. Daarnaast zal de FG voldoende kennis moeten hebben van de organisatie waarbinnen hij of zij zijn of haar rol vervult en de markt waarin deze organisatie zich bevindt.

Positie van de FG binnen de organisatie

De FG moet zijn of haar taken en verplichtingen onafhankelijk kunnen vervullen, ongeacht of hij of zij in dienst is van de verantwoordelijke of verwerker. De FG kan een personeelslid zijn van de organisatie, maar mag ook extern worden ingehuurd.

Organisaties zijn verplicht om de FG tijdig en naar behoren te betrekken bij alle aangelegenheden met betrekking tot de bescherming van persoonsgegevens. Dit betekent dat de FG onder andere zal moeten kunnen deelnemen aan overleg binnen de organisatie dat betrekking heeft op de bescherming van persoonsgegevens en dat hij of zij direct op de hoogte wordt gesteld van een beveiligingsincident. Indien een privacy impact assessment moet worden uitgevoerd, zal de FG hier al in het beginstadium bij moeten worden betrokken.

Organisaties zijn verder verplicht de FG adequaat te ondersteunen in de uitoefening van zijn of haar taken. Hiertoe zullen organisaties de FG toegang moeten verschaffen tot de verwerkte persoonsgegevens en de verwerkingsactiviteiten en de FG de benodigde (financiële) middelen ter beschikking moeten stellen voor het vervullen van zijn of haar taken en het in stand houden van zijn of haar kennis. Dit betekent dat organisaties een FG staf moeten toekennen en hem of haar in staat moeten stellen regelmatig cursussen te volgen. Ook moet de FG voldoende tijd krijgen om de functie op een juiste manier uit te voeren, in het bijzonder indien de FG zijn of haar functie parttime uitoefent.

Organisaties dienen voldoende waarborgen te implementeren om te garanderen dat de FG zijn of haar taken op onafhankelijke wijze kan uitvoeren. Ter waarborging van deze onafhankelijkheid, mag de FG bijvoorbeeld niet ontslagen of gestraft worden voor de uitvoering van zijn of haar taken. De organisatie mag de FG ook geen instructies geven met betrekking tot de uitvoering van diens taken, bijvoorbeeld omtrent het al dan niet melden van een datalek bij de toezichthoudende autoriteit. Dat de organisatie de FG niet op dergelijke wijze mag sturen, geldt ook nu al onder de Wbp.

Net als onder de Wbp is de FG onder de AVGB met betrekking tot de uitvoering van zijn of haar taken tot geheimhouding of vertrouwelijkheid gehouden. De FG mag andere taken en plichten vervullen naast zijn of haar FG-functie. De organisatie moet er vervolgens voor zorgen dat deze taken of plichten niet tot een belangenconflict leiden. Tegelijkertijd is er een aantal functies dat niet te combineren is met die van de FG. Voorbeelden zijn seniormanagementposities zoals CEO, CFO, CIO, COO, hoofd HR, et cetera. Verder is het wat ons betreft niet aan te raden om een interne bedrijfsjurist als FG aan te wijzen, althans voor zover hij of zij naast de taken van FG tevens zijn of haar taken als bedrijfsjurist uitvoert. In dat geval kan er namelijk spanning ontstaan tussen de wijze waarop de persoon in zijn hoedanigheid van bedrijfsjurist adviseert (mogelijk meer commercieel ingestoken) en de wijze waarop hij of zij als FG dient te opereren, namelijk met strikte inachtneming van de AVGB.

Taken van de FG

Anders dan onder de Wbp zijn de taken van de FG onder de AVGB concreter geformuleerd. De FG heeft in ieder geval de volgende taken:

- de organisatie en de werknemers die persoonsgegevens verwerken, informeren en adviseren over hun verplichtingen

uit hoofde van de AVGB en andere relevante privacyregelgeving;

- toezien op de naleving van de AVGB (en andere relevante privacyregelgeving) en op het beleid van de organisatie met betrekking tot de verwerking van persoonsgegevens. Hieronder vallen het toewijzen van verantwoordelijkheden, het vergroten van bewustwording binnen de organisatie en het opleiden van werknemers;
- het verstrekken van advies ten aanzien van privacy impact assessments en het toezien op de uitvoering daarvan; en
- samenwerking met en optreden als contactpunt voor de toezichthoudende autoriteit(en).

Organisaties mogen aan deze taken uiteraard taken toevoegen. Een van de mogelijkheden is het verantwoordelijk maken van de FG voor het bijhouden van het verplichte register van verwerkingsactiviteiten.

Praktische aanbevelingen

Organisaties zullen allereerst moeten vaststellen of zij een FG moeten aanwijzen. Indien zij besluiten geen FG aan te stellen, zal de interne analyse hieromtrent moeten worden vastgelegd. Ook de adviezen van FG moeten worden opgeslagen, in het bijzonder indien er van de adviezen van de FG wordt afgeweken.

Indien een FG wordt aangewezen is het belangrijk om de juiste omgeving te creëren waarin de FG zijn of haar taken op adequate wijze kan vervullen. Indien een FG verantwoordelijk is voor meerdere landen, is het belangrijk om een team op te zetten dat de FG kan helpen bij het contact met de toezichthouders en de betrokkenen in de verschillende landen.

Een FG heeft een belangrijke rol binnen een organisatie en het is daarom van belang dat de juiste persoon met voldoende kennis en ervaring wordt geselecteerd. FG wordt men niet in één dag dus indien een organisatie intern een FG wil aanwijzen, is het van belang om die persoon tijdig bij dit proces te betrekken zodat hij of zij waar nodig verdere kennis kan opdoen omtrent de AVGB en de wijze waarop persoonsgegevens worden verwerkt binnen de organisatie.

Klik hier om u aan te melden voor deze nieuwsbrief

Overzicht van te behandelen onderwerpen

Januari 2017	Territoriale reikwijdte van de AVGB
Februari 2017	Het concept van toestemming
Maart 2017	Bijzondere persoonsgegevens
April 2017	'Accountability', 'Privacy by Design' en 'Privacy by Default'
Mei 2017	Rechten van betrokkenen (informatievoorziening)
Juni 2017	Rechten van betrokkenen (inzage, correctie en overdraagbaarheid)
Juli 2017	Rechten van betrokkenen (wissing, beperking, bezwaar en geautomatiseerde besluitvorming)
Augustus 2017	Verwerkers
September 2017	Datalekken en meldplichten
Oktober 2017	Functionaris voor de Gegevensbescherming
November 2017	Doorgifte van persoonsgegevens (buiten de EER)
December 2017	Toezichthouders (competenties, taken en bevoegdheden)
Januari 2018	One Stop Shop

Februari 2018	Sancties
Maart 2018	Verwerkingen van persoonsgegevens in arbeidsverhoudingen
April 2018	Profiliering en Retail
Mei 2018	Overview

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Celine van Es
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com