compliancepeople

De Onderneming
en de Functionaris
Gegevensbescherming

VIJF VEEL VOORKOMENDE MISVATTINGEN

compliancepeople

DE ONDERNEMING EN DE FUNCTIONARIS GEGEVENSBESCHERMING

Vijf veel voorkomende misvattingen over de FG…

Mr R.H. van der Wart CIPP/E, advocaat en interim-jurist

Inmiddels zijn we bijna een jaar onderweg sinds op 25 mei 2018 de Algemene verordening gegevensbescherming (AVG) van toepassing werd. Hoewel vele instellingen en ondernemingen de 'overgangstermijn' van 2 jaar tot de definitieve ingangsdatum niet optimaal benut hebben, is er toch een zekere mate van compliance te bespeuren. De AVG geeft aan dat een behoorlijk aantal datalekken wordt gerapporteerd en in vergelijking met andere Europese landen scoren Nederlandse verwerkingsverantwoordelijken ook hoog qua aantallen meldingen. Nu is het aantal meldingen natuurlijk niet zaligmakend, maar het is een van de weinige meetbare aanwijzingen die we op dit moment hebben.

PERCEPTIE ROL FG

Hoe staat het nu met de Functionaris Gegevensbescherming (FG)? Is die er (altijd) en zo ja, doet deze wat de Europese wetgever heeft bedoeld? Door een commentaar op vijf veelgehoorde misvattingen wil ik helpen bij een juiste 'perceptie' van de rol van de FG.

De FG is bedoeld als toezichthouder. De FG kan, maar hoeft niet in dienst van de Verwerkingsverantwoordelijke of Verwerker te zijn. In een aantal gevallen is een FG verplicht. Aan de FG worden verschillende eisen gesteld in de AVG en de FG geniet ook een bepaalde mate van ontslagbescherming. Maar op welke punten is de perceptie van de 'markt' nu anders dan de AVG bedoelt? Voor de duidelijkheid: de 'misvattingen' zijn steeds vetgedrukt.

1. DE FG STAAT AAN HET HOOFD VAN DE PRIVACYKETEN VAN DE ORGANISATIE

De rol van de FG is het geven van advies en het houden van toezicht. Diens taken staan beschreven in artikel 39 AVG. De FG geeft geen leiding aan de personen die met het beheer van de privacy zijn belast. De FG keurt geen DPIA's goed, neemt niet de beslissing om al dan niet een incident als datalek te melden aan de AP of de betrokkene(n) en gaat geen verwerkersovereenkomsten aan. Vanuit het oogpunt van rollenscheiding (risk management) is het ook niet wenselijk dat de FG zelf leiding geeft aan of beslissingen neemt over de privacyaspecten van een onderneming of instelling. Maar dit betekent niet dat de FG geen inhoudelijke rol kan hebben. De FG moet voldoende invloed en gezag hebben om op bestuursniveau over (de toepassing van) het privacybeleid mee te praten en de besluitvorming te helpen sturen in de door de wetgever aangegeven richting. Opleiding, ervaring en competenties moeten voldoende zijn om dat te bereiken. Maar ook kennis van de branche. De FG rapporteert aan de hoogste leiding van de organisatie. Het verdient aanbeveling in het privacybeleid (privacy governance) duidelijk vast te leggen wie dit is en welke vrijheid de FG daarbij heeft.

Het is in de praktijk belangrijk om een onderscheid te maken tussen een Privacy Officer en de FG. Vaak staat de Privacy Officer wel aan het hoofd van de privacyketen. Verwarrend is dan weer dat in de praktijk de Privacy Officer deze functie vervult, terwijl in de Engelse versie van de AVG (DGPR) de FG wordt aangeduid als Data Protection Officer (DPO). Bij internationale concerns ligt (rol-)verwarring daarom voor de hand.

Bij een datalek is het lijnmanagement (of de Privacy Officer) verantwoordelijk voor de te nemen stappen (onderzoek, aanscherping veiligheidsmaatregelen, melding aan de AP, melding aan betrokkenen). Het ligt volstrekt voor de hand dat een FG als stafadviseur onderdeel uitmaakt van het crisisteam, maar de FG neemt geen beslissingen en voert de acties niet uit. En de eindverantwoordelijkheid ligt uiteindelijk altijd bij het management/bestuur.

TAKEN VAN DE FG

(verkort weergegeven, alles op het gebied van de (U)AVG):

A: Informeren en adviseren van de verwerkingsveranwoordelijke, verwerkers en de werknemers over hun verplichtingen;

B: Toezien op de naleving van de verplichtingen;

C: *Desgevraagd* advies verstrekken over DPIA's en toezien op de uitvoering daarvan;

D: Samenwerken met de AP;

E: Contactpunt voor de AP inzake met verwerking verband houdende aangelegenheden, waaronder zogenaamde 'voorafgaande raadpleging'.

2. DE FG IS ÉÉN PERSOON

De FG hoeft niet één persoon te zijn. Met name in grotere organisaties is het zelfs wenselijk dat er een 'FG-office' is met één FG (of meer dan één), al dan niet ad hoc of permanent ondersteund door een aantal 'subject matter experts' (technisch, juridisch of risk management) naar gelang de noodzaak. De FG hoeft niet in dienst te zijn, maar dat kan wel. Inmiddels zijn er veel bureaus en experts die zich aanbieden als FG. Let er op bij de keuze voor een externe FG op, dat deze niet alleen voldoende juridische en technische kennis heeft, maar ook ervaring heeft in de desbetreffende branche of industrie. De continuïteit van de functionele rol van een FG moet ook geborgd worden. Dit kan bij externen nog lastig zijn, zeker als gebruik wordt gemaakt van softwaremodellen van die externe FG.

3. ALLE CONTACTEN MET DE AP VERLOPEN VIA DE FG

Hoewel de taken van de FG ook contact met de AP omvatten (zie kader), kan het heel goed zijn en ligt het vanuit het perspectief van de AVG zelfs voor de hand dat de Privacy Officer de meldingen van datalekken verricht (na consultatie van de FG) en de registers bijhoudt.

4. DE FG MOET EEN EXPERT ZIJN OP ALLE GEBIEDEN

Hoewel de FG voldoende competenties moet hebben en moet begrijpen wat er gebeurt, wordt niet verwacht dat de FG zelf over alle mogelijk relevante kennis, ervaring en competenties beschikt. Het management moet de FG in staat stellen om over extra interne en externe expertise te kunnen beschikken. Ook moet de FG wel toegang hebben tot de registers en de interne documentatie met betrekking tot de besluitvorming van de onderneming over privacy-aangelegenheden. Waar een OR is, is er ook een instemmingsrecht van de OR op het gebied van privacybeleid. Het ligt daarom voor de hand dat de FG – maar dan wel vanuit diens onafhankelijke rol als toezichthouder en adviseur – regelmatig overlegt met de OR en door de OR wordt uitgenodigd; zeker wanneer (een wijziging van) het privacybeleid op de agenda staat.

5. DE FG KAN NIET WORDEN ONTSLAGEN

De FG moet volgens artikel 38, derde lid, AVG onafhankelijk kunnen werken. De FG mag ook niet worden ontslagen of gestraft voor het uitvoeren van diens taken. Die taken staan in artikel 39 AVG beschreven en hoewel er wel ruimte in zit, valt bijvoorbeeld het melden van datalekken niet a priori onder de taken van de FG. Een FG die zich buiten de reikwijdte van diens taken bemoeit met privacy, bijvoorbeeld het ongevraagd beoordelen van een DPIA, loopt wel degelijk disciplinaire risico's. Mijn advies is om ook dit goed af te bakenen in het privacybeleid.

AFRONDING

De FG vervult een nieuwe functie. Deze is wel vergelijkbaar met die van bepaalde functies van andere compliance officers. Het verdient aanbeveling duidelijk in het privacybeleid vast te leggen welke bevoegdheden de FG heeft en hoe interne escalatie kan worden vormgegeven. Dan gaat het zowel om interne escalatie naar de FG toe (wanneer zijn medewerkers verplicht diens advies in te winnen) als om escalatie van de FG, wanneer deze het idee heeft dat het niet goed gaat: gaat de FG dan naar de Algemeen Directeur, de Portefeuillehouder Privacy van het management team, de Voorzitter van de Raad van Commissarissen of een Raad van Toezicht, de OR of zelfs direct naar de AP? Een goede definitie van de communicatie- en escalatielijnen is essentieel om verwachtingen te managen en conflicten te voorkomen.

KANTOOR AMSTERDAM
Roemer Visscherstraat 44
1054 EZ Amsterdam

KANTOOR DEN HAAG
Kwekerijweg 21
2597 JL Den Haag

KANTOOR MÜNCHEN
Hirschauer Straße 12
D-80538 München

+31(0)20-226 12 10