De FG: een schaap met vele poten

*Door mr. P.G. Coté MBA**

Werken in overeenstemming met de nieuwe regelgeving op het gebied van gegevensbescherming vergt een domeinoverschrijdende aanpak van organisaties. In deze bijdrage wordt verkend welke eisen er gesteld worden en hoe organisaties kunnen voldoen aan de eisen van de voorgestelde Europese privacyverordening en andere regels. Daarbij wordt met name de positie van de functionaris gegevensbescherming (FG) nader bestudeerd. We zullen zien dat een goede FG organisaties voor veel ellende kan behoeden. Maar wat is een goede FG? Wat doet een FG allemaal? Op zoek naar een schaap met meer dan vijf poten.

1. Inleiding

Begin 2012 heeft de Europese Commissie een voorstel voor een privacyverordening gepresenteerd die rechtstreeks van toepassing zal zijn in de lidstaten. In het artikel van Anne-Wil Duthler is geschetst wat er daarna nodig is geweest om de Algemene verordening gegevensbescherming (Avg) in werking te laten treden per 25 mei 2016 (en van toepassing te laten zijn per 25 mei 2018). Een belangrijke wijziging ten opzichte van de huidige wetgeving is dat een verantwoordelijke of verwerker in de zin van de Avg onder bepaalde omstandigheden verplicht wordt om een functionaris voor gegevensbescherming (FG) aan te stellen. Dit is het geval wanneer de verantwoordelijke een overheidsinstantie of -orgaan is, een organisatie is die op grote schaal bijzondere persoonsgegevens verwerkt of een organisatie is die hoofdzakelijk belast is met verwerkingen die regelmatige en stelselmatige observatie van betrokkenen vereisen.

Deze nieuwe verplichting houdt in dat aanstelling van een FG in genoemde gevallen verplicht wordt op straffe van een boete van € 10 miljoen of voor een onderneming tot 2% van de jaaromzet. Er zijn nu

meer dan 550 FG's ingeschreven bij de Autoriteit Persoonsgegeveens (AP). Rekening houdend met uitval en vervanging zal de vraag naar de`FG nieuwe stijl´ in de komende jaren naar schatting zo'n 5.000 à 10.000 per jaar bedragen. De uiteindelijke vervangingsvraag zal na verloop van vijf jaar naar schatting tussen de 1.000 en 5.000 liggen. De verplichting om een FG aan te stellen en de boete op overtreding zullen er dus voor zorgen dat de vraag naar FG's nieuwe stijl´ de komende jaren zeer groot zal zijn.

Vanaf 1 januari 2016 geldt in Nederland niet alleen een meldplicht voor datalekken maar zijn per dezelfde datum de boetebeleidsregels van de AP aangepast. De AP kan nu boetes tot maximaal € 820.000 opleggen bij overtredingen van de Wbp. Deze aanscherping van de privacyregels heeft geleid tot media-aandacht voor privacy en toename van de belangstelling voor de functie van FG.

Wat is een`FG nieuwe stijl´?

De FG moet volgens de verordening op grond van zijn professionele kwaliteiten worden aangesteld en, in het bijzonder, op grond van zijn deskundigheid op het gebied van wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 van de Avg genoemde taken van de FG te vervullen. De FG moet niet alleen beschikken over juridische deskundigheid, maar hij of zij moet ook verstand hebben van ICT en informatiebeveiliging, AO/IC en auditing. Bij datalekken moet de FG snel kunnen handelen als crisismanager. De FG moet vakinhoudelijke kennis en ervaring hebben. Bovendien moet hij of zij met autoriteit de toezicht en compliance rol vervullen. Een FG moet zowel met ICT-deskundigen over praktische informatiebeveiliging kunnen overleggen, als met bestuurders en toezichthouders over governance en risicomanagement. En dan hebben we het nog niet gehad over de dubbelrol van de FG als adviseur en toezichthouder. Om verstandig met deze beide rollen om te gaan moet een FG over bijzondere persoonlijke kwaliteiten beschikken.
Daar komt nog bij dat de 'FG nieuwe stijl' met het van kracht worden van de aanstaande wet- en regelgeving - naast toezichthoudende taken - meer en meer operationele taken krijgt toebedeeld. Denk hierbij aan het vastleggen van documentatie- en informatieverplichtingen, het beantwoorden van verzoeken van betrokkenen en van de toezichthouder en het organiseren van risicomanagement op het vlak van identity-, privacy- & cybersecurity.

In dit artikel wordt onderzocht welke eisen de Avg aan de FG stelt, welke taken de Avg aan de FG toedeelt, en hoe organisaties en FG's daarmee om moeten gaan. Voor we daaraan toekomen is het echter van belang om het karakter en de achtergrond van de Avg te schetsen. Als inleiding op de nieuwe regels wordt eerst de snelle ontwikkeling die het begrip privacy doormaakt, beschreven.

De ontwikkeling van het privacybegrip: Privacy 2.0

"Van mij mogen ze alles weten, want ik heb niks te verbergen", zo luidde vaak de reactie als het over privacy ging. Het onderwerp 'privacy' leek de gemiddelde burger niet erg te interesseren. Opvraag van persoonsgegevens bij telecomproviders, automatische nummerplaatherkenning op snelwegen, cookies die je bijna moet accepteren, overmatige dataverzameling door Google Streetview hebben niet geleid tot opschudding of protestacties. Integendeel, we waren juist massaal bereid om zelf persoonlijke informatie prijs te geven. We deelden gemakkelijk locatiegegevens via onze mobiele telefoon en gaven apps toegang tot de contacten in ons adressenbestand. Veel gebruikers van social media 'posten' of 'tweeten' materiaal zonder zich erg druk te maken over privacy instellingen. Privacy leek geen issue te zijn.

Er lijkt inmiddels sprake van een kentering te zijn. Steeds meer gebruikers van social media realiseren zich dat bedrijven als Google, Apple en Facebook geld verdienen met hun persoonlijke gegevens. Elke klik of 'like' biedt een aanleiding om een gepersonaliseerd aanbod te doen.

Hoe kan het dat privacy pas recent weer meer in de belangstelling is komen te staan? Een deel van het antwoord is ongetwijfeld: omdat we pas aan het begin staan van de digitale revolutie en de ontwikkelingen zo snel gaan dat ons 'maatschappelijk privacybewustzijn' daarmee geen gelijke tred houdt.

Een ander deel van het antwoord is dat de term 'privacy' ons op het verkeerde spoor zet. Privacy betekende van oudsher zoiets als 'het recht om met rust gelaten te worden', maar dat is in het internettijdperk van 'privacy 2.0' een gepasseerd station. Het is bijna onmogelijk om als burger/consument een greep te houden op persoonlijke informatie, want de gemiddelde Nederlander staat geregistreerd in 250 tot 500 bestanden. Gegevens die her en der zijn opgeslagen worden nu met elkaar gecombineerd. Juist die koppeling levert commercieel interessante informatie op.

'Behavioral advertising' is een voorproefje van de mogelijkheden die in het verschiet liggen. Als u eerder op internet heeft gezocht naar een hotel, een vliegreis of een koffiezetapparaat, dan ziet u een volgende keer aanbiedingen voor vergelijkbare zaken op uw scherm verschijnen. Het verdienmodel van ondernemingen die actief zijn op internet is voor een groot deel gebaseerd op gegevens die verzameld worden voor 'behavioral advertising': advertenties die worden afgestemd op eerder zoekgedrag. 'Dynamic pricing', het verschijnsel dat de prijs voor de vliegreis ineens is veranderd bij een nieuw bezoek aan de website, is een ander voorbeeld.

Nu is een aanbieding voor een koffiezetapparaat of de prijs van een vliegreis nog tamelijk onschuldig, maar door meer persoonlijke informatie bij elkaar te brengen krijgt het geheel meer impact op de privacy. Zo maken handelsinformatiebureaus kredietprofielen om voor hun klanten het debiteurenrisico in kaart te brengen. De voorwaarden voor de lening worden bepaald door de informatie die over de betrokkene te vinden is. Handelsinformatiebureaus gebruiken daarbij statistische gegevens over de woonomgeving, zoals het gemiddelde inkomen in de buurt.

Hier gaat het dan niet meer om inbreuken op de persoonlijke levenssfeer puur door het verzamelen van persoonlijke informatie. De inbreuk zit in wat er vervolgens mee gebeurt. Aan de hand van eerdere veronderstellingen en standaard procedures wordt de betrokkene beoordeeld en ingedeeld in een categorie. De informatie wordt gebruikt voor een (al of niet) automatische beslissing of een betrokkene in aanmerking komt voor bijvoorbeeld studiefinanciering of een vergunning of een ziektekostenverzekering.

Het begrip ‘privacy’ heeft door deze invasieve ontwikkelingen een ander karakter gekregen. Privacy is in een volgende fase gekomen. Privacy 2.0 vereist nieuwe regels. De Europese Commissie heeft dat goed begrepen en is daarom gekomen met regels die de burgers van de lidstaten beter moeten beschermen: de empowerment van de betrokkene.

Empowerment als kenmerk van de Avg

De Europese Unie geeft met de Avg blijk van een moderne visie op gegevensbescherming. In het internettijdperk is er behoefte aan een nieuw privacybegrip dat inspeelt op de nieuwe verhoudingen tussen betrokkenen en verantwoordelijken. De Avg kenmerkt zich door het streven om de rechten van betrokkenen zodanig te versterken dat zij ‘in control’ komen van de eigen persoonlijke gegevens.

Een belangrijke aanleiding voor de verordening is voorts de verdere eenwording van de communautaire markt. Door één wettelijk regime voor gegevensbescherming vast te stellen worden handelsbelemmeringen als gevolg van verschillen tussen de 28 lidstaten weggenomen. Zie ook de Column van Wim Buis in deze bundel.

In meer algemene zin wijst de Commissie op de bijdrage van de Avg aan de verwezenlijking van de doelstellingen van de Digitale Agenda voor Europa, het Stockholm-actieplan en de Europa 2020-strategie. Minstens zo belangrijk is echter de emancipatoire doelstelling van de Avg om de gegevens van

burgers beter te beschermen. Degene wiens data verzameld worden, de betrokkene, moet zelf kunnen bepalen wat er wel en niet met de gegevens gedaan mag worden.

Vanuit transatlantisch perspectief hebben schrijvers als Swire opgemerkt dat er met de aankondiging van de Avg een “second wave of privacy for the Internet age” is begonnen. De aanleiding voor die hernieuwde aandacht voor privacyvraagstukken zijn volgens Swire recente ingrijpende technologische veranderingen. ‘Sociale’ netwerken zijn in korte tijd gegroeid van nul tot een miljard gebruikers. Mobiele apparaten zoals smartphones en tablets zijn alomtegenwoordig en roepen de vraag op hoe locatiegegevens moeten worden behandeld. En ‘online behavioral advertising’, denk aan het gebruik van ‘cookies’, heeft zowel in Europa als in de VS al geleid tot speciale regelgeving, om tegemoet te komen aan gesignaleerde privacybezwaren.

Deze ontwikkelingen vragen om een nieuwe positiebepaling van betrokkenen en verantwoordelijken, van burgers ten opzichte van overheden en van consumenten in hun relatie tot bedrijven. De EU-commissie kiest met de Avg voor de emancipatie van de betrokkene. Het sociologische begrip ‘empowerment’ is volgens sommigen rechtstreeks van toepassing op de Avg. In deze visie is de positie van betrokkenen gemarginaliseerd door de technologische en commerciële ontwikkelingen en geeft de Avg instrumenten om het grondrecht op privacy te verdedigen en terug te winnen. Het ‘recht om vergeten te worden’ en de verplichting voor verantwoordelijken om te voorzien in dataportabiliteit zijn voorbeelden van de ‘empowerment’ van de betrokkene.

Het ingrijpende karakter van de Avg: de boetes

Kenmerkend voor de Avg, naast de empowerment van de betrokkene, is dat de gevolgen van de Avg ingrijpend zijn. Veel van de nieuwe regels wijken af van de huidige en er gelden hoge boetebepalingen bij overtreding. Nieuwe – in Nederland al bekende - onderwerpen die in de Avg worden geïntroduceerd zijn de meldplicht bij datalekken, het privacy impact assessment (PIA) en de verplichting om privacybeleid te formuleren. Privacy by design and by default’ was ook al een principe van gegevensbescherming, maar de Avg maakt het tot een expliciete verplichting om privacybeschermende maatregelen in informatiesystemen in te bouwen, zodat gewaarborgd wordt dat niet meer gegevens dan noodzakelijk worden verwerkt, op een manier die zo min mogelijk inbreuk maakt op de privacy.

En dan de boetes. Ik noem enkele overtredingen waarvoor een boete van € 10 miljoen (of 2% van de wereldwijde jaaromzet) kan worden opgelegd door de toezichthouder: als er geen beschrijvingen van de verwerkingen zijn vastgelegd in een register of als er geen passende maatregelen voor

informatiebeveiliging zijn genomen, of als het 'privacy by design and default' principe niet is toegepast. Dezelfde boete geldt wanneer de verantwoordelijke niet voldoet aan de meldplicht datalekken of de plicht om een privacy impact assessment te houden. In dezelfde categorie valt het niet aanwijzen van een functionaris gegevensbescherming waar deze verplicht is: een boete van maximaal € 10 miljoen, of 2% van de wereldwijde jaaromzet. Boetes van maximaal € 20 miljoen of 4% van de wereldwijde jaaromzet kunnen bijvoorbeeld worden opgelegd indien de basisbeginselen niet worden gerespecteerd met inbegrip van de voorwaarden voor toestemming; rechten van betrokkenen niet worden ingewilligd; gegevens onrechtmatig worden verstrekt aan een derde land; of een bevel van de AP niet wordt nageleefd.

Met dergelijke hoge boetes wordt gegevensbescherming een onderwerp voor de Raad van Bestuur. Het gaat hier namelijk om sancties die, in termen van de accountant, een risico van 'materieel belang' opleveren. Bij de controle van de jaarrekening zal de accountant hiernaar vragen. Op grond van de Nederlandse corporate governancecode is de Raad van Bestuur verantwoordelijk voor het risicobeheersingssysteem. De Raad van Bestuur rapporteert daarover aan de Raad van Commissarissen. Privacy zal voortaan onderdeel moeten worden van het risicobeheersingssysteem, want bestuurders en toezichthouders moeten in hun jaarverslag of in hun in-control-statement een beschrijving geven van de risico's die zijn verbonden aan de bedrijfsvoering. Zo is privacy een 'board-issue' geworden. De FG speelt daarin een belangrijke, vooral toezichthoudende, rol.

De FG in de context van de Avg

De rol van de FG wordt sterk bepaald door de hiervoor besproken aspecten van de Avg: het ingrijpende karakter van de verordening en de empowerment van het individu. Enerzijds ziet de FG toe op het privacybeleid van de organisatie. Is dat beleid in overeenstemming met de Avg en wordt het correct uitgevoerd? Het toezicht op de compliance geeft de functie van FG een verantwoordelijk karakter, zeker wanneer we daarbij de hoogte van de boetes in aanmerking nemen. Anderzijds is de FG degene die ervoor zorgt dat betrokkene hun rechten kunnen uitoefenen zoals het recht op informatie over de verwerking en de identiteit van de verantwoordelijke, de toegang tot de eigen persoonsgegevens, en de rectificatie en het wissen van gegevens. De FG is dus instrumenteel voor de 'empowerment' van de betrokkene. Maar wie zorgt ervoor dat de FG zijn taak goed kan uitoefenen? Voordat we deze vraag beantwoorden gaan we te rade in de Avg. Wat zegt de Avg over de FG?

De Avg over de FG

De taken en bevoegdheden van de FG vinden we in Hoofdstuk IV, Afdeling 4 van de Avg. Artikel 37 behandelt de aanwijzing van de FG. Artikel 38 gaat over de positie van de FG en artikel 39 behandelt de taken van de FG. Lid 5 van Artikel 37 luidt, kortweg weergegeven, als volgt.

De FG wordt door de voor de verwerking verantwoordelijke 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 FG-taken te vervullen.

Andere bepalingen voor de aanstelling van een FG zijn dat eventuele overige beroepstaken geen belangenconflict op mogen leveren, en dat de FG een zekere ontslagbescherming heeft: de FG mag geen nadeel ondervinden of ontslagen worden als gevolg van de uitoefening van zijn taken. De FG hoeft niet in dienst te zijn bij de verantwoordelijke, maar kan ook ingehuurd worden.

Over de positie van de FG zegt artikel 38 van de Avg het volgende.

1. De verantwoordelijke zorgt ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
2. De verantwoordelijke zorgt ervoor dat de FG zijn plichten en taken onafhankelijk vervult en geen instructies ontvangt met betrekking tot de uitoefening van de functie. De FG brengt rechtstreeks verslag uit aan de leiding van de verantwoordelijke.
3. Betrokkenen kunnen de FG kunnen verzoeken ‘om de uitoefening van de rechten van de verordening’. Bedoeld zijn de rechten die op grond van de verordening toekomen aan betrokkenen. Hier zien we de rol van de FG als instrument bij de ‘empowerment’ van de betrokkene aan de dag treden.
4. De verantwoordelijke waarborgt dat de FG geen instructies krijgt over de uitvoering van zijn taken. De FG zal niet worden ontslagen en zal geen nadeel ondervinden door de uitoefening van zijn taken.

De FG heeft een bijzondere toezichtrol van de FG. Hij vervult zijn taak onafhankelijk en krijgt geen instructies. De rechtstreekse rapportage aan de Raad van Bestuur is in overeenstemming met de toezichthoudende taak. De rol van de FG lijkt in dit opzicht op die van de controller. Een verbindende factor tussen beide functionarissen is het onderwerp risicomanagement. Voor het profiel van de FG betekent het dat de FG inhoudelijk deskundig moet zijn op het gebied van risicomanagement. Bovendien moet hij of zij gesprekspartner (kunnen) zijn van bestuurders en toezichthouders. Dat houdt

ook in dat de FG onwelgevallige boodschappen zodanig weloverwogen en overtuigend moet kunnen overbrengen dat de Raad van Bestuur in actie komt, om door de FG gesignaleerde non-compliance te corrigeren.

Als taken van de FG noemt artikel 39 achtereenvolgens, kortweg weergegeven,

a) Het informeren en adviseren van verantwoordelijke en diens medewerkers over diens verplichtingen;
b) Het toezien op de naleving van de Avg en het privacybeleid van de organisatie, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
c) Het desgevraagd adviseren over uitvoering van de PIA (gegevensbeschermingseffectbeoordeling) en het toezien op de uitvoering;
d) Samenwerken met de toezichthoudende autoriteit, d.w.z. de AP;
e) Het optreden als contactpunt voor de AP inzake aangelegenheden in verband met de verwerking en het op eigen initiatief in voorkomend geval raadplegen van de AP.

De Avg legt hiermee de FG een breed scala aan taken op waarvan de aard varieert van praktisch uitvoerend tot strategisch en waarvan de inhoud betrekking heeft op onderwerpen variërend van informatiebeveiliging, administratieve organisatie, gegevensbeveiliging, audits, privacy by design en default, bewustmaking, opleidingen, PIA's en datalekken. De hoeveelheid en variëteit van de onderwerpen en de mate van verantwoordelijkheid doen een groot beroep op deskundigheid en vaardigheden van de FG. De hoge boetes bij overtredingen hebben tot gevolg dat de FG een grote verantwoordelijkheid draagt. De Raad van Bestuur moet erop kunnen vertrouwen dat de FG de organisatie behoedt voor boetes en overige risico's met betrekking tot de gegevensbescherming.

Met een dergelijk takenpakket is het noodzakelijk dat de FG de scope en reikwijdte van zijn werkzaamheden en verantwoordelijkheden goed in kaart brengt. Daarover is overeenstemming nodig met de verantwoordelijke, zodat men elkaar niet voor verrassingen stelt. Concreet zal dat bijvoorbeeld betekenen dat er duidelijkheid moet bestaan over de omvang van de 'corporate family'. Welke entiteiten horen tot de 'groep van ondernemingen' ex artikel 37 lid 2 Avg? De FG moet dat weten om de eigen verantwoordelijkheid te kunnen begrenzen. Van de relevante verbonden partijen moet de FG immers de verwerkingen documenteren en vragen van betrokkenen beantwoorden. Daarbij zal de FG aan de verantwoordelijke moeten aangeven wat er nodig is om de functie goed te vervullen. Hij of zij

heeft overzicht nodig om tot voldoende inzicht te komen en de verantwoordelijke goed te adviseren. De verantwoordelijke op zijn beurt moet voorzieningen voor een goede taakvervulling treffen.

Bij die randvoorwaarden en voorzieningen hoort dat de FG ondersteund wordt bij de uitoefening van zijn taak. Dat houdt in dat er in ieder geval ruimte moet zijn voor kennisonderhoud en kennisbevordering. Generaliserend kun je zeggen dat huidige FG's veelal een juridische of een ICT-achtergrond hebben. De Avg verwacht dat beide deskundigheden in de FG verenigd zijn, zodat de FG in ieder geval een gesprekspartner is op beide terreinen. Daarnaast verlangt de Avg kennis van gegevensbeveiliging, audits, risicomanagement en good governance. Dat zijn nieuwe aandachtsgebieden voor de meeste privacy professionals en dat zal dus ook voor de huidige FG's opleiding en training vergen.

Eerder is de vraag opgeworpen wie er voor de empowerment van de FG zorgt. Tot op zekere hoogte is het de verantwoordelijke die, zoals eerder vermeld, een goede taakvervulling mogelijk moet maken, door middel van opleiding, personeel en apparatuur. Daarnaast moet de FG terug kunnen vallen op een netwerk van vakgenoten en externe ondersteuning. De unieke positie binnen een organisatie en de rol als toezichthouder verhinderen dat de FG daar zijn klankbord zoekt. Voor de uitwisseling van ervaring, intervisie en onderlinge kennisbevordering is een netwerk van FG's nodig.

Wat staat een verantwoordelijke te doen?

De voorbereiding op de Avg vergt betrokkenheid van professionals als informatiebeveiligers, juristen, controllers, IT-auditors, de externe accountant, maar ook van bestuurders en interne toezichthouders. Het ontwikkelen van privacybeleid volgens de Avg kost tijd. Verantwoordelijken moeten daarom tijdig beginnen met het vaststellen van de nulsituatie. Wat is de stand van de informatiebeveiliging, is er een FG of moet er een aangesteld worden, is er privacybeleid, is privacy onderdeel van risicomanagement en de planning- en controlcyclus? Een FG moet geselecteerd worden en aangesteld, privacybeleid moet ontwikkeld worden en er moet een geïntegreerde 'baseline' opgesteld worden waar de organisatie aan moet voldoen wat betreft privacy en informatiebeveiliging. Privacy impact analyses moeten uitgevoerd worden op de verwerkingen van persoonsgegevens en de resultaten moeten worden gebruikt om 'privacy by design' in te bouwen in informatiesystemen. Verder moeten de betrokken professionals worden opgeleid. En voor datalekken moeten draaiboeken gemaakt worden om te zorgen dat het lek tijdig en gecontroleerd aan de toezichthouder kan worden gemeld.

Wat doet Duthler Associates?

Duthler Associates heeft vanuit een jarenlange ervaring met het onderwerp privacy en gegevensbescherming een dienstverleningsaanbod samengesteld dat inspeelt op de behoeften van organisaties en FG's in de aanloop naar het van toepassing zijn van de Avg. Duthler Associates verzorgt met strategische partners de werving en selectie van FG's waarin naast de kenniscomponent ook rekening gehouden wordt met gedrag en vaardigheden. Eenmaal geselecteerd wordt een passende opleiding op maat gemaakt, rekening houdend met eerder verworven competenties volgt de kandidaat-FG geselecteerde modules of de gehele 'leergang FG'. Aan de leergang is een certificaat verbonden dat recht geeft op inschrijving in het FG-register van Duthler Associates. Het FG-register is voor organisaties die op zoek zijn naar een FG te raadplegen. Om de inschrijving als FG te behouden moet een programma van permanente educatie gevolgd worden. Daarnaast organiseert Duthler Associates op basis van het register FG-communities waar FG's elkaar ontmoeten.

Tenslotte

De Europese privacyverordening stelt burgers beter in staat om hun rechten als betrokkene uit te oefenen (empowerment). De FG staat betrokkenen terzijde om hun rechten te effectueren. Verantwoordelijken zullen aan de toegenomen verplichtingen van de Europese privacyverordening moeten voldoen op straffe van hoge boetes. Om als Raad van Bestuur en Raad van Commissarissen 'in control' te blijven van de risico's voor de organisatie moeten verantwoordelijken zich terdege voorbereiden op de Europese privacyverordening. De functionaris gegevensbescherming is daarbij een onmisbare factor: als kwartiermaker, adviseur, risicomanager, compliance officer en toezichthouder.

Ook voor organisaties waarvoor de aanstelling van een FG geen verplichting is, verdient het aanbeveling zorgvuldig te overwegen om een FG aan te stellen. Een FG is de onafhankelijke spin in het web op het gebied van de bescherming van persoonsgegevens en is daardoor een onmisbare factor in het risicomanagement van elke organisatie en een belangrijk instrument om te kunnen voldoen aan de gehele privacyverordening. Daarom: op zoek naar een FG-schaap met meer dan vijf poten.

** Mr. Philip Coté MBA is jurist en werkzaam als adviseur bij Duthler Associates. Hij is gespecialiseerd in recht en beleid en vraagstukken van goed bestuur. Hij is auteur van de Handreiking voor examencommissies van de Vereniging Hogescholen en adviseert Hogescholen onder meer over gegevensbescherming, onderwijs- en examenregelingen, publiek/privaat-vraagstukken en auteursrecht. Daarnaast treedt hij op als trainer van examencommissies.*