Privacywet en privacyfunctionaris

Val ik in de prijzen?

Privacywet en privacyfunctionaris: val ik in de prijzen?

Waarover gaat deze brochure en voor wie is zij bestemd?
Heeft de privacywetgeving belangrijke gevolgen voor mijn organisatie? Brengen aard en activiteiten van onze organisatie grotere risico's met zich mee? Is de bescherming van persoonsgegevens voor ons een wezenlijke factor? Moet ik iemand aanstellen als aanspreekpunt, of om toezicht te houden? Voor het management van een organisatie zijn dit vaak lastige vragen. Deze brochure biedt richting bij het beantwoorden van deze vragen.

Hieronder wordt eerst kort omschreven waarom aandacht voor gegevensbescherming in een organisatie belangrijk is en wat een functionaris voor de gegevensbescherming is en doet. Om snel voor uw organisatie de gevolgen te kunnen inschatten is een praktische vragenlijst opgenomen. Daarna worden de belangrijkste wettelijke regels voor het registreren en gebruiken van persoonsgegevens beschreven en wordt ingegaan op de risico's van het niet-naleven van deze regels. Tot slot wordt stilgestaan bij het toezicht op de naleving van de regels, en de meerwaarde van het aanstellen van een eigen functionaris.

Inhoud

Privacywet en privacyfunctionaris: val ik in de prijzen?
Nederlands genootschap van functionarissen voor de gegevensbescherming

Waarom aandacht voor gegevensbescherming?
Organisaties, ondernemers, consumenten en overheden kunnen er niet omheen. Om deel te nemen aan het maatschappelijk verkeer is het noodzakelijk dat persoonsgegevens worden geregistreerd en gebruikt. Zo heeft een bank persoonsgegevens nodig om geldrekeningen te kunnen beheren, een verzekeringsmaatschappij om een polisadministratie bij te kunnen houden, een vereniging om contributies te kunnen innen, een arts om een goede behandeling voor te kunnen stellen, en een gemeente om een rijbewijs te kunnen afgeven. Het is belangrijk dat dergelijke gegevens op een zorgvuldige wijze worden verwerkt. Dat bepaalt immers het vertrouwen in de organisatie en de kwaliteit van zijn dienstverlening.

Wat is en doet een functionaris voor de gegevensbescherming (FG)?
Er zijn wettelijke regels van toepassing op het registreren en gebruik van persoonsgegevens. De belangrijkste is de Wet bescherming persoonsgegevens (Wbp). Een *functionaris voor de gegevensbescherming*[1], ook wel privacyfunctionaris genoemd, houdt toezicht op de naleving van die regels. Zo'n functionaris wordt aangesteld door het management van een organisatie en kan naast een toezicht- ook een adviesfunctie hebben. Op die manier wordt bevorderd dat persoonsgegevens zorgvuldig worden geregistreerd en gebruikt. Anders gezegd, het aanstellen van een privacyfunctionaris helpt om risico's rondom de verwerking van persoonsgegevens inzichtelijk te maken en om ongelukken te voorkomen[2].

Het "privacyprofiel" van uw organisatie
De risico's die gepaard gaan met de verwerking van persoonsgegevens, de wettelijke eisen die daaraan gesteld worden en de consequenties daarvan, kunnen per branche en per organisatie verschillen. Weet u wat het privacyprofiel is van úw organisatie?
Aan de hand van de vragen in deze brochure kunt u eenvoudig bepalen of de privacywetgeving voor uw organisatie belangrijke gevolgen heeft. De "vragenlijst" hieronder bestaat uit een aantal stellingen die risicoverhogende kenmerken van uw organisatie kunnen zijn. Door de van toepassing zijnde vakjes aan te kruisen krijgt u voor uw organisatie een (totaal)beeld van de risico's die er zijn bij de registratie en het gebruik van persoonsgegevens. U kunt hiermee snel inzicht krijgen waar het zwaartepunt moet liggen van uw privacybeleid, en of het zinvol is om een privacyfunctionaris aan te stellen.

[1] Zie voor nadere uitleg onder het kopje: Toezichthouder(s). De termen functionaris voor de gegevensbescherming en privacyfunctionaris worden in deze brochure naast elkaar gebruikt.
[2] Zie voor de beschrijving van de meerwaarde van de FG het kader achter in deze brochure.

Zijn onderstaande stellingen van toepassing op uw organisatie? Kruis achter elke stelling een vakje aan.	*Niet van toepassing*	*Een beetje van toepassing*	*Van toepassing*
Activiteiten van de organisatie 1. De kernactiviteiten van de organisatie (als geheel) zijn gericht op de registratie en het gebruik van persoonsgegevens; *(zie de toelichting op blz. 5)*	groen	oranje	rood
2. Uw organisatie verzamelt en/of gebruikt persoonsgegevens ten behoeve van derden;	groen	oranje	rood
3. Er geldt een hogere maatschappelijke gevoeligheid dan gemiddeld voor non-compliance of privacyincidenten; *(let op de geldende regels of opvattingen, de aard van de activiteiten of de producten, of de doelgroep van de organisatie)*	groen	oranje	rood
Verkrijging van de gegevens 4. Gegevens worden geregistreerd en gebruikt op grond van eigen waarneming zonder dat betrokkenen daarvan op de hoogte zijn;	groen	oranje	rood *j
5. Betrokkenen zijn *(juridisch of feitelijk)* verplicht om hun gegevens af te staan en/of door uw organisatie te laten verwerken;	groen	oranje	rood *j
Hoeveelheid gegevens 6. De databases van uw organisatie bevatten persoonsgegevens over heel veel personen; *(< 1000= groen, 1000 – 50.000= oranje, > 50.000= rood. Het gaat hierbij om zowel werknemers als klanten)*	groen	oranje	rood
Aard van de gegevens 7. Uw organisatie verzamelt en/of gebruikt regelmatig gegevens over het privéleven van mensen, gegevens over kinderen, financiële gegevens, gegevens die worden gebruikt ter beoordeling van personen, of gegevens over inwoners van andere lidstaten van de Europese Unie, de Verenigde Staten, Canada, Zwitserland, Noorwegen, IJsland, Liechtenstein, New Jersey, Guernsey, Isle of Man, Australië, Nieuw-Zeeland, of Japan; *(dit zijn gegevens met een verhoogde (privacy)gevoeligheid of met een verhoogd juridisch risico)*	groen	oranje	rood
8. Uw organisatie verzamelt en/of gebruikt gegevens met een *hoge* (privacy)gevoeligheid waaronder gegevens over godsdienst of levensovertuiging, ras of etniciteit, politieke gezindheid, lichamelijke of geestelijke gezondheid, seksuele leven, vakbondslidmaatschap, gegevens over strafbaar gedrag, gegevens over onrechtmatig of hinderlijk gedrag in verband met een door de rechter opgelegd verbod, of BSN-nummers;	groen	oranje	rood
Complexiteit van gebruik en registratie van gegevens **9.** Er is behalve de algemene privacywet, ook bijzondere (sectorale) wet- of regelgeving van toepassing op de registratie en/of het gebruik van persoonsgegevens; *(bijvoorbeeld specifieke wetten, besluiten, gedragscodes)*	groen	oranje	rood *j
10. Er worden voor veel verschillende doeleinden gegevens geregistreerd en gebruikt of er zijn veel verschillende bestanden in de organisatie aanwezig, er zijn veel gebruikers/beheerders of er vinden veel uitwisselingen plaats met andere delen van de organisatie, of met derden zoals dienstverleners;	groen	oranje	rood *j
Verstrekking aan derden 11. Aan meer dan 10 (overheids)instanties worden gegevens verstrekt, of er worden gegevens verstrekt aan één of meer buitenlandse autoriteiten;	groen	oranje	rood *j
12. Er worden geregeld gegevens verstrekt aan een of meer derden die gevestigd zijn in landen buiten de EU;	groen	oranje	rood *j
Vragen over gegevensgebruik **13.** In uw organisatie rijzen vaak vragen over wat er wel of niet mag met persoonsgegevens;	groen	oranje	rood *j
14. Er is behoefte aan 1 verantwoordelijk aanspreekpunt voor vragen over de registratie en het gebruik van persoonsgegevens;	groen	oranje	rood *j
Complexiteit van de organisatie. 15. De organisatie heeft een complexe organisatiestructuur met veel verschillende afdelingen, meerdere divisies of vestigingen, of zij is gevestigd in meerdere landen;	groen	oranje	rood
Ambitie 16. Uw organisatie hecht grote waarde aan naleving van wet- en regelgeving, aan maatschappelijk zorgvuldig optreden of aan kwaliteit op het gebied van de informatievoorziening. Het is van wezenlijk belang dat uw organisatie vertrouwen geniet op het gebied van rechtmatigheid, zorgvuldigheid en kwaliteit, in het bijzonder wat betreft de verwerking van persoonsgegevens.	groen	oranje	rood

Score. Vul in op de stippellijnen:	*geen risico*	*middelhoog risico*	*hoog risico*
	aantal groen:	aant. oranje:	aantal rood:
invullen:	…	…	…
	x 0 punten =	x 1 punt =	x 2 punten =
ingevuld aantal x aantal punten:	0	…	…
optellen:		**TOTAAL:**	…

Het resultaat: valt uw organisatie "in de prijzen?"
Door het aantal punten, en het aantal rode vakjes dat u in de vragenlijst heeft aangekruist op te tellen, kunt u het privacyprofiel van uw organisatie bepalen:

Resultaat	
13 punten of minder of er zijn 0-1 rode vakjes zichtbaar	**Uw organisatie heeft geen bovengemiddeld privacyrisico. U heeft de mogelijkheid een FG aan te stellen**
13 - 19 punten of er zijn 1-3 rode vakjes zichtbaar	**Privacy is een onmiskenbare risicofactor in uw organisatie. Het verdient aanbeveling een FG aan te stellen**
meer dan 19 punten of er zijn 4 of meer rode vakjes zichtbaar	**Privacywetgeving vormt een wezenlijk aandachtsgebied en risico. Het wordt sterk aanbevolen om voor de organisatie een FG aan te stellen**

Het resultaat uit de test en de invulling van de FG-functie

Mocht uw organisatie besluiten tot het aanstellen van een FG, dan dient te worden nagedacht over kenniseisen en functieprofiel. Het NGFG heeft hierover meer informatie beschikbaar. De vragenlijst geeft op bepaalde punten echter al een indicatie. De vuistregel is: hoe hoger de score uit de vragenlijst, hoe groter het belang voor de organisatie bij bescherming van gegevens. De hoogte van score kan in verband daarmee ook betekenis hebben voor de capaciteit die nodig is voor de uitoefening van de taken van de FG.

5 groene vakjes of minder: de FG-taken maken substantieel deel uit van de capaciteit van 1 fulltimer.

De situatie binnen een organisatie kan een bepaalde invalshoek, een bepaalde achtergrond van de FG vereisen. Zo kan de achtergrond van de FG bijvoorbeeld zijn: IT-specialist, onderzoeker, beveiliger of jurist. Uiteraard dient hij of zij wel aan de wettelijke vereisten te voldoen, en kennis van de privacywetgeving te hebben. De vragenlijst maakt de juridische invalshoek globaal meetbaar. Een hoge score bij bepaalde risico's wil zeggen dat voor uw FG het zwaartepunt zal liggen op de specifieke juridische werkzaamheden, zoals de behandeling van vragen over wetstoepassing. Het gaat bij een hoog risicoprofiel dan niet zelden om lastige kwesties, zoals over de relatie tussen verschillende wetten en het afwegen van belangen. Er is dan reden om de juridische kennis goed te borgen. In de vragenlijst zijn daarom vragen opgenomen die zijn gemarkeerd met een "j".

3 of meer keer een "*J": het zwaartepunt zal liggen op de juridische invalshoek.

Toelichting bij de vragenlijst

Doel en inhoud van de vragenlijst
De vragen in de lijst zijn er op gericht om er achter te komen of er sprake is van een “hoog risicoprofiel” bij een organisatie, in welk geval maatregelen zoals zoals het aanstellen van een FG op zijn plaats zijn. De vragen in de lijst gaan dus niet over de vraag of de privacywetgeving überhaupt wel van toepassing is. Dat is reeds het geval als er sprake is van het verwerken van persoonsgegevens*. De vragen in de lijst zijn gebaseerd op de normen uit wet- en regelgeving, richtlijnen van het Cbp en ervaringen uit de professionele praktijk.

Voorbeeld
Een voorbeeld: de Wbp is van toepassing op persoonsgegevens die worden verwerkt voor intern beheer en bedrijfsvoering van de organisatie (zoals de “eigen” personeels- en salarisadministratie), maar ook op persoonsgegevens die worden verwerkt voor de kernactiviteiten. In het tweede geval is er meestal een hoger risico voor de organisatie. Dat is zeker het geval als de kernactiviteiten direct verband houden met het gebruik van persoonsgegevens (zie vraag 1). De organisatie heeft dan een betrekkelijk groot belang bij het rechtmatig en zorgvuldig gebruik van de gegevens.

Door wie wordt de vragenlijst ingevuld?
Voor het invullen van de vragenlijst kan het nodig zijn verschillende deskundigen te raadplegen. Denk in het bijzonder aan deskundigen op het gebied van de primaire bedrijfsprocessen, de gegevensverwerking, als aan de hogere manager en de bedrijfsjurist. Voor grote, complexe organisaties (zoals multinationals en grote overheidsorganisaties) is het beter om de vragenlijst per business unit, divisie, directie of dienst in te vullen. De resultaten hebben dan betrekking op dat dienst- of bedrijfsonderdeel. De privacyfunctie moet namelijk worden afgestemd op de structuur en grootte van de organisatie. Het is dan van belang te weten bij welke organisatieonderdelen accenten moeten worden gelegd. Er zullen in grote, complexe organisaties vaak één of meer decentrale privacyfunctionarissen nodig zijn.

**Welke gegevens vallen onder “persoonsgegevens”?*
Persoonsgegevens zijn alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon. De meest sprekende voorbeelden zijn naam, adres of geslacht. Maar ook andere gegevens vallen onder de definitie van persoonsgegeven. Bijvoorbeeld gegevens die een waardering over iemand geven, zoals het resultaat van een onderzoek. Zelfs gegevens over ondernemingen of organisaties, of gegevens over voorwerpen of objecten, kunnen wel persoonsgegevens zijn. Dat is het geval als zij mede bepalend zijn voor de wijze waarop iemand in het maatschappelijk verkeer wordt beoordeeld of behandeld. Als u dan een verband kunt leggen tussen het gegeven en een bepaalde natuurlijke persoon, is er sprake van een persoonsgegeven.

De privacywetgeving

Waar moet u aan voldoen? De Wbp bevat algemene normen voor het gebruik van persoonsgegevens die door iedere organisatie zelf moeten worden uitgewerkt. De belangrijkste vuistregels zijn de volgende.

1. Doelbinding
Persoonsgegevens mogen slechts voor bepaalde en gerechtvaardigde doeleinden worden verzameld en niet worden verwerkt voor doeleinden die daarmee onverenigbaar zijn.

2. Rechtmatige grondslag
Voor elk gebruik van persoonsgegevens moet een rechtmatige grondslag in de wet te vinden zijn. Deze grondslagen zijn: ondubbelzinnige toestemming van de betrokkene of noodzakelijk voor de uitvoering van een overeenkomst, nakoming van een wettelijke plicht, de bescherming van een vitaal belang, de uitvoering van een publiekrechtelijke taak dan wel een gerechtvaardigd belang van de organisatie of van de betrokkene.

3. Kwaliteit
De persoonsgegevens moeten zoveel mogelijk juist, nauwkeurig, toereikend en ter zake dienend zijn. Er mogen niet meer gegevens worden verwerkt dan noodzakelijk is voor het doel van de verwerking. De opgeslagen gegevens mogen niet langer bewaard worden dan noodzakelijk is.

4. Transparantie of openheid
De persoon van wie persoonsgegevens worden verwerkt moet kunnen overzien door wie en voor welke doeleinden zijn gegevens worden verwerkt. Hij moet actief geïnformeerd worden door de organisatie. Daarnaast moet de organisatie de gegevensverwerking in veel gevallen melden bij het College bescherming persoonsgegevens (Cbp). Als alternatief kan de melding worden gedaan bij de eigen FG, die binnen de organisatie is aangesteld.

5. Beveiliging
Naast deze meldingsplicht heeft de organisatie een beveiligingsplicht. De organisatie moet ter beveiliging van de persoonsgegevens, passende technische en organisatorische maatregelen treffen.

6. Rechten
De personen van wie persoonsgegevens worden verwerkt hebben verder het recht om kennis te nemen van de opgenomen gegevens, het zogenaamde inzagerecht. In voorkomende gevallen hebben zij tevens het recht de opgenomen gegevens te laten verbeteren of te laten verwijderen.

7. Buitenlands gegevensverkeer
Verstrekking van gegevens naar landen buiten de EU is alleen toegestaan als dat land een passend niveau van bescherming heeft.

Naast de Wbp zijn er overigens ook internationale privacyregels waar steeds meer organisaties mee te maken krijgen. Bijvoorbeeld wanneer zij hun activiteiten uitbreiden met een webwinkel.

Zelfregulering
De wet gaat uit van zelfregulering. Een organisatie moet zelf aan de slag gaan met de uitvoering van de Wbp. Een niet geringe opgave. Gelukkig zijn er hulpmiddelen beschikbaar. Zo heeft het Ministerie van Justitie een handleiding ontwikkeld met tekst en uitleg. Deze handleiding en andere informatie en hulpmiddelen zijn ook te downloaden via de website van het Cbp. In sommige branches zijn gedragscodes ontwikkeld. In deze gedragscodes zijn de regels van de wet al nader uitgewerkt voor de desbetreffende branche.

Wat moet een organisatie doen?
De organisatie moet op grond van de Wbp de volgende verplichtingen nakomen:

- Nagaan welke verwerkingen er zijn;
- Vaststellen of deze rechtmatig plaatsvinden. Dat betreft bij voorbeeld de noodzaak, de kwaliteit en de doelbinding;
- Nagaan of de verwerkingen moeten worden gemeld bij het Cbp of zijn vrijgesteld van de meldingsplicht;
- De opgeslagen gegevens niet langer bewaren dan noodzakelijk is;
- Passende beveiligingsmaatregelen treffen;
- Informatie verstrekken aan de betrokkenen, en hun rechten, zoals het recht op inzage, correctie of verzet, op verzoek effectueren;
- Periodiek nagaan of de melding dan wel de afspraken die zijn gemaakt nog steeds geldig zijn of moeten worden aangepast.

Welke risico's zijn er verbonden aan het overtreden van de regels?
Het onzorgvuldig omgaan met, of onjuist gebruik van persoonsgegevens door een organisatie kan leiden tot schade. Schade in de vorm van imagoschade door het verlies van vertrouwen in de organisatie, en het verlies van klanten of potentiële klanten. Schade door afbreuk aan "goed werkgeverschap" ten opzichte van de werknemers. Het Cbp kan bestuursdwang uitoefenen of een boete opleggen. Er kunnen ook strafrechtelijke sancties volgen.

De rol van de FG bij de inbedding van de privacywetgeving
Het is van belang dat de privacywet in een organisatie wordt geïmplementeerd. Dit betekent concreet dat een organisatie in ieder geval de wettelijke verplichtingen nakomt en maatregelen treft om de rechten van betrokkenen te kunnen effectueren. Dit betreft in de regel een directe verantwoordelijkheid van de leiding van de organisatie, de bestuurlijke top. Een succesvolle implementatie is in feite onmogelijk zonder *commitment* van de top. Een evenwichtig privacybeleid, dat ook wordt onderhouden, kan zeer behulpzaam zijn bij het implementatieproces. Het privacybeleid wordt eveneens vastgesteld door de leiding van de organisatie.

Als het privacybeleid is vastgesteld, kan een organisatie met behulp van een systeem van monitoring, evaluaties en privacy-audits nagaan in hoeverre het privacybeleid effectief is. Door middel van een jaarlijkse zelfevaluatie aan de hand van een vragenformulier toetst de organisatie zelf of aan de normen van gegevensbescherming en privacy wordt voldaan. Bij een privacy-audit wordt de toetsing uitgevoerd door een onafhankelijke auditor. In de eerste plaats toetst de auditor of de organisatie adequaat is ingericht om te kunnen voldoen aan de wet. Vervolgens beoordeelt hij alle procedures en getroffen maatregelen op hun werking. De privacy-audit is een essentieel onderdeel binnen het systeem van toezicht en beheer. De FG kan een belangrijke rol vervullen bij het initiëren en uitvoeren van de privacy-audits en het uitbrengen van het uiteindelijke advies aan de verantwoordelijke.

Toezichthouder(s)

Het Cbp houdt toezicht op de naleving van de Wbp. Het Cbp doet onderzoek, heeft een openbaar register van meldingen van gegevensverwerkingen en kan handhavend optreden door bestuursdwang toe te passen. Bij dat laatste kan worden gedacht aan het in beslag nemen van administraties in geval van vermoedens van privacyschendingen. Ook kan het Cbp dwangsommen en boetes opleggen. Het Cbp draagt met zijn toezicht bij aan de ontwikkeling van een juiste invulling van het normenkader van de Wbp.

De Wbp biedt ook de mogelijkheid om een *interne* toezichthouder aan te stellen. Afhankelijk van de aard en de omvang van de gegevensverwerkingen en de risico's op onzorgvuldig gebruik van persoonsgegevens, kan het verstandig zijn om specifieke (juridische) kennis in huis te halen, en het toezicht op de gegevensverwerkingen toe te vertrouwen aan een eigen functionaris. Deze functionaris wordt doorgaans *functionaris voor de gegevensbescherming, privacy officer, privacyfunctionaris,* of *compliance officer* genoemd. In alle gevallen is er sprake van een medewerker die bijdraagt aan het managen van de privacyrisico's, en die als spin in het web binnen een onderneming kan optreden als in- en extern aanspreekpunt op het gebied van verwerkingen van persoonsgegevens.

Het inrichten van de privacyfunctie, en het aanstellen van een functionaris moet echter wel voldoen aan bepaalde minimumeisen. Wil de functionaris effectief kunnen functioneren, dan moeten eisen worden gesteld aan zijn betrouwbaarheid en deskundigheid, maar ook aan zijn "armslag" of positie binnen de organisatie. Het gaat er om of de functionaris voldoende invloed kan uitoefenen. Hij of zij wordt immers aangesteld vanuit het besef dat een daadwerkelijke bescherming van persoonsgegevens de grootste meerwaarde voor de organisatie heeft. Van intern toezicht door een FG in de zin van de wet is alleen sprake als voldaan wordt aan de in de wet gestelde eisen rond de onafhankelijkheid van de FG.

Behalve aan afzonderlijke organisaties geeft de wet ook aan brancheorganisaties, waarbij verschillende bedrijven of organisaties zijn aangesloten, de mogelijkheid om een functionaris voor de gegevensbescherming te benoemen. De bevoegdheden van de FG strekken zich in dat geval uit over de verwerkingen van al de aangesloten bedrijven, instellingen of organisaties.

NGFG
NEDERLANDS GENOOTSCHAP
FUNCTIONARISSEN GEGEVENSBESCHERMING

Meerwaarde van de FG

Wat is de meerwaarde van een FG?

- De functionaris voor de gegevensbescherming (FG) is een wettelijk erkende toezichthouder, maar maakt ook deel uit van de organisatie van de verantwoordelijke die hem heeft benoemd. Daardoor is hij goed in staat kwesties op het gebied van “zijn” verantwoordelijke te beoordelen en mee te denken over passende oplossingen.
- Het Cbp stelt zich terughoudend op ten aanzien van organisaties waar een FG toeziet op de naleving van de bescherming van persoonsgegevens. De FG’s worden opgenomen in het openbare register van functionarissen voor de gegevensbescherming.
- De FG is een vast aanspreekpunt met een stevige adviesfunctie naar de verantwoordelijke - dat is in de regel de directeur of raad van bestuur - in zaken over (de verbetering van) het gebruik van persoonsgegevens. De FG kan ook optreden als onafhankelijke bemiddelaar en/of klachtenbehandelaar. Dit hoeft dan niet buiten de deur te gebeuren, wat voor beide partijen voordelen kan bieden.
- Het aanstellen van een FG is een passende maatregel wanneer serieuze waarborgen vereist zijn bij het registreren en gebruiken van persoonsgegevens. De FG beschikt over mogelijkheden om de organisatie op effectieve wijze te helpen bij het streven naar het rechtmatig en zorgvuldig gebruiken van de persoonsgegevens. De FG kan het daarvoor noodzakelijke privacybewustzijn binnen de organisatie bevorderen en in stand houden. Met de uitoefening van zijn taken en bevoegdheden werkt de FG mee aan de borging van de kwaliteit van de gegevensverwerking, en aan de zorgvuldigheid en de betrouwbaarheid van zijn organisatie.

Kortom, het op een juiste wijze verwerken van persoonsgegevens zal met een FG meer betekenis krijgen in het kader van *compliance* en “behoorlijk bestuur” van een organisatie, maar ook als kwaliteitsaspect, als een *asset* dat kan bijdragen aan een positief kwaliteitsimago. En daar zal in principe bij elke organisatie aandacht voor zijn.

Ga voor meer informatie naar de website www.ngfg.nl. Hier treft u nog meer hulpmiddelen aan voor het inrichten en ondersteunen van de FG-functie, zoals het informatieblad over de taken van de FG. Ook vindt u daar meer informatie over de activiteiten van het NGFG in het kader van de kwaliteitsbevordering voor de beroepsgroep van FG’s.