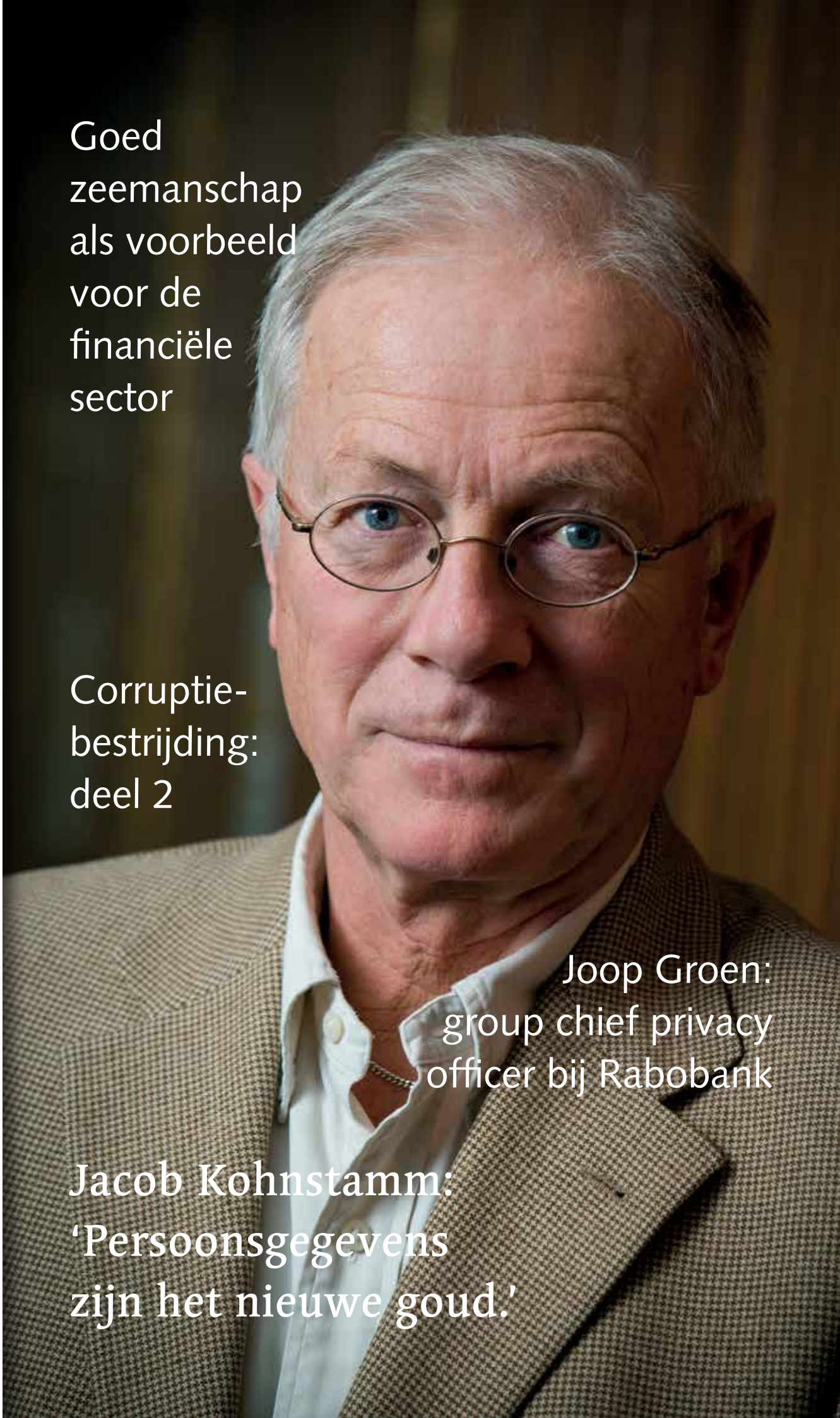
de Compliance Officer
nummer 20, december 2015



Goed zeemanschap als voorbeeld voor de financiële sector

Corruptie-bestrijding: deel 2

Joop Groen: group chief privacy officer bij Rabobank

Jacob Kohnstamm: 'Persoonsgegevens zijn het nieuwe goud.'

Nederlands compliance Instituut

## Colofon

De Compliance Officer is het vakblad voor compliance officers en andere betrokkenen bij het compliance-proces. De doelgroep bestaat uit compliance officers, bestuurders, toezichthouders, secretarissen van de vennootschap en bedrijfsjuristen die betrokken zijn bij het uitvoeren van compliancetaken.

**Redactie:**
Sharon Karsten (bureauredactie) en Cora Wielenga (eindredactie)
Tel 088 99 88 100 E-mail: redactie@complianceofficer.nl
**Aan deze editie werkten verder mee:** Petrosjan Damen, Hans Ludo van Mierlo, Joost Montens, Roderick Noordhoek, Bart Peters, Geert Vermeulen
**Fotografie:** Wilco van Dijen
**Vormgeving:** Tangram Studio
**Druk:** Platform P, Rotterdam
**Uitgever:** Nederlands Compliance Instituut, Postbus 5111, Capelle aan den IJssel
**Advertenties:** Diane Bakker
Tel 088 99 88 100 E-mail: bakker@compliance-instituut.nl

Nieuwsfeiten, ingezonden artikelen en personeelsmutaties kunt u per e-mail doorgeven aan redactie@complianceofficer.nl.

Het abonnement is gratis voor de doelgroep. Abonnees buiten de doelgroep: € 50 (bij 4 edities).

Oplage 3.100 exemplaren
ISSN 1878-7991

**www.complianceofficer.nl**

# Inhoud

# Afscheid...

Een aantal lezers van De Compliance Officer heeft het wellicht al vernomen, maar ik heb besloten om het Nederlands Compliance Instituut na veertien jaar te gaan verlaten.

Daar zal ik zo wat meer over vertellen, maar ik wil op deze plaats van de gelegenheid gebruik maken om een korte 'trip down memory lane' te maken en even terug te kijken op ruim twintig jaar compliance en veertien jaar NCI. Met een flinke portie understatement kun je zeggen dat compliance behoorlijk veranderd is sinds 1995. Toen pasten alle compliance officers in Nederland nog in een flinke vergaderzaal. Het voorkomen van het gebruik van voorwetenschap was hun core business en buiten de bancaire sector waren er nog nauwelijks compliance officers. Beetje bij beetje ontdekten deze compliance officers uit het stenen tijdperk dat compliance niet alleen bij banken toegevoegde waarde kon hebben en dat er ook andere aandachtsgebieden bestonden die relevant waren: witwassen, integere bedrijfsvoering, zorgplicht, terrorismefinanciering, klokkenluidersregeling etc., etc. En nog steeds is compliance in ontwikkeling, compliance officers houden zich tegenwoordig bijvoorbeeld ook bezig met privacy en mededinging.

Ook andere sectoren dan de financiële wereld zijn inmiddels bezig de meerwaarde van compliance te ontdekken, zoals de zorgsector en de woningbouwsector, en ik durf de voorspelling wel aan dat die trend zich nog wel enige tijd zal doorzetten.

Het NCI heeft sinds de oprichting kunnen inspelen op de groei van compliance, zowel in producten en diensten als in de klantenkring. Ik ben blij dat ik met een gerust hart weg kan. Het NCI heeft een ervaren directie, enthousiaste en professionele compliance officers, een effectief en servicegericht supportteam, een mooi palet aan diensten en opleidingen en een indrukwekkende klantenkring. Garantie dus voor kwaliteit en toewijding in de diensten die zij aan klanten biedt.

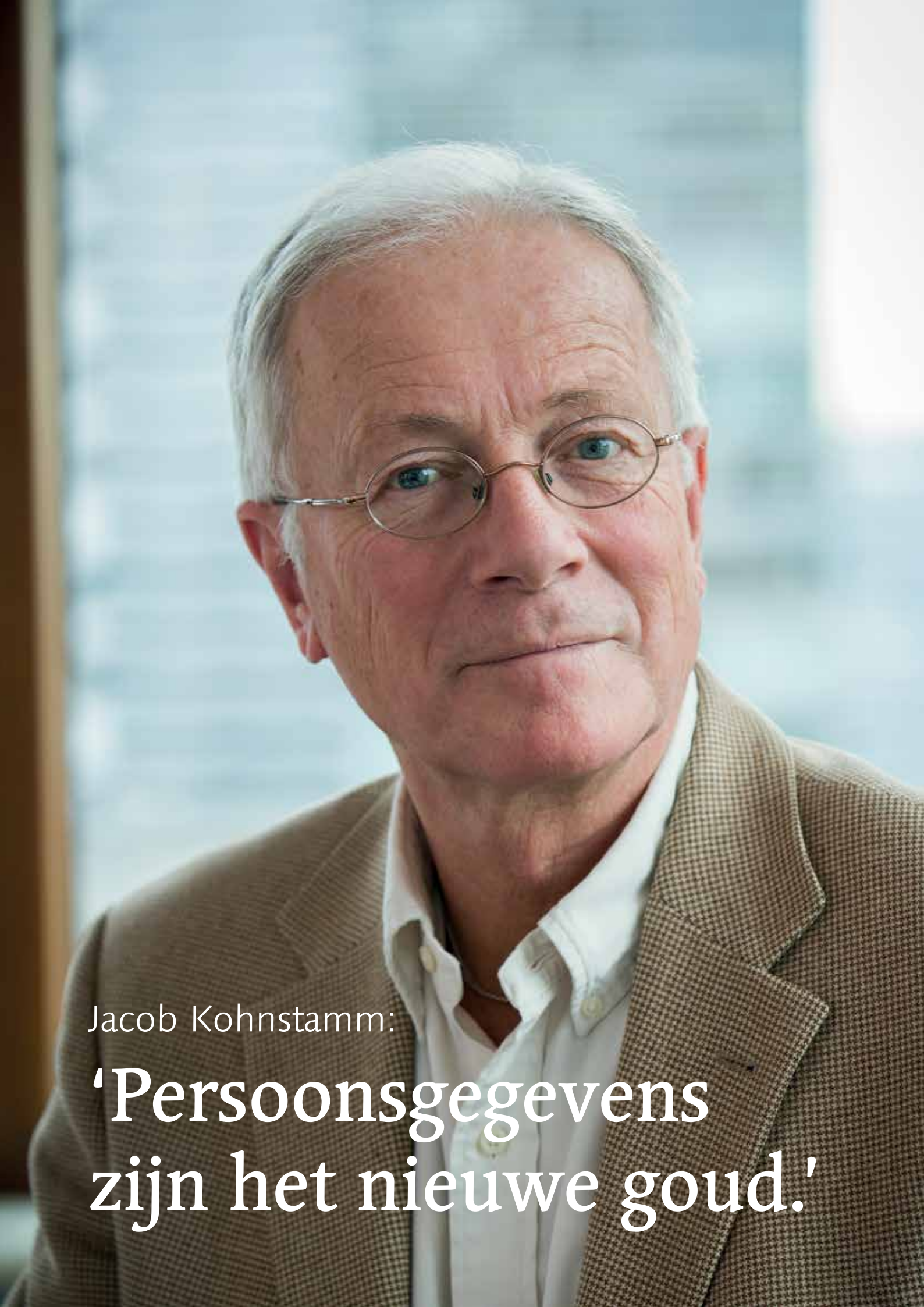
Zoals ik al zei: ik verlaat binnenkort het NCI. Niet omdat ik het niet meer naar mijn zin had, integendeel, maar omdat ik met mijn gezin een 'nieuwe uitdaging' aan ga. Dat klinkt misschien als een cliché, maar een emigratie naar Nieuw Zeeland is zeker een uitdaging. Wij vervullen hiermee onze langgekoesterde wens om meer van de wereld te zien en een nieuw bestaan op te bouwen in een land met veel ruimte en rust.

Dat betekent dat veel geregeld moet worden in Nieuw Zeeland, maar zeker ook hier in Nederland, thuis en bij het NCI. Dat gaat uiteraard niet van de ene op de andere dag, en er is inmiddels achter de schermen veel gedaan om mijn werkzaamheden en klanten binnenkort definitief over te kunnen dragen. We hebben ons team van compliance officers uitgebreid om op die manier onze klanten eenzelfde service te kunnen blijven bieden. Eind december rond ik mijn werkzaamheden af, zodat wij begin januari met een one way ticket en een container vol huisraad de reis kunnen aanvaarden.

Tot nu toe heb ik al veel fijne reacties gehad op mijn toekomstplannen. Ik wil iedereen bedanken voor het meeleven en de gelukwensen en ik wil op mijn beurt iedereen, collega's, klanten, collega compliance professionals en andere relaties veel geluk en succes wensen. En als je Down Under bent: aarzel niet om langs te komen.

Kia Ora!

Bart Peters



Jacob Kohnstamm:

# ‘Persoonsgegevens zijn het nieuwe goud.’

In het kader van het thema 'privacy' mocht het College Bescherming Persoonsgegevens eigenlijk niet ontbreken in deze editie van De Compliance Officer. Dat de voorzitter van het college, *Jacob Kohnstamm*, in deze drukke tijd ingaat op de uitnodiging voor een interview, is best bijzonder. Begin november is het zover en schuift Sharon Karsten aan voor een gesprek over – hoe kan het ook anders – privacy.

**Het nieuwe jaar staat bijna voor de deur. Wat kunnen we in 2016 van het CBP verwachten?** "Van het CBP niets… Wij gaan namelijk vanaf januari 2016 als Autoriteit Persoonsgegevens door het leven. Behalve een nieuwe naam krijgen we ook nieuwe taken: de meldplicht datalekken en de boetebevoegdheid. Zeker de eerste maanden zal hier veel aandacht naar uitgaan."

**Waarom verwacht u dat hier de meeste aandacht naar zal uitgaan?** "Eigenlijk omdat we niet weten wat we precies moeten verwachten van de meldplicht datalekken. Er staat nu een definitie in de wet in welke gevallen organisaties zouden moeten melden, maar die is betrekkelijk vaag. Dit zou ertoe kunnen leiden dat iedereen die een niet-relevant lek heeft, straks denkt 'Ik meld het maar, better safe than sorry'. We zijn bang dat we daardoor zullen worden overspoeld met meldingen. We hebben om dit te voorkomen inmiddels beleidsregels opgesteld die helpen bij het bepalen wanneer je een datalek zou moeten melden. Ook hebben we een mooi systeem in ontwikkeling waarbij melden eenvoudig gaat en waarbij de meldingen voor een belangrijk deel automatisch worden gefilterd. Na deze filtering bekijken we welke overgebleven meldingen we voor kennisgeving aannemen en welke we verder gaan behandelen. Het is even opletten dat de meldplicht altijd twee elementen bevat: melding aan de toezichthouder en melding aan de consument indien de kans groot is dat hij last krijgt van het datalek. Het CBP fungeert dus vooral als filter. Verder zijn we bezig met de voorbereiding op de boetebevoegdheid."

**Wat gaan we van de nieuwe boetebevoegdheid merken?** "We kunnen direct een rode kaart uitdelen, in plaats van eerst een gele kaart waarbij een organisatie de kans krijgt om zijn leven te beteren. We kennen nu alleen nog maar de last onder dwangsom. Dat is wat ik steeds – om in voetbaljargon te spreken – een gele kaart heb genoemd. Hierbij krijgt een organisatie eerst de tijd om de overtreding te herstellen voordat het de dwangsom moet betalen. De boetebevoegdheid geldt als rode kaart waarbij je meteen het veld uit moet en dus direct een boete moet betalen. Als je de principes van de wet weloverwogen negeert, dan kunnen we een flinke boete opleggen. Het effect van de boetebevoegdheid is hopelijk dat er een sterke preventieve werking van uitgaat. Persoonsgegevens zijn het nieuwe goud. Dat moet je goed beveiligen. Ga je daarmee de fout in, dan kan je plotseling erg veel geld kwijt zijn."

**Naar wie zullen de boetegelden toevloeien?** "Boetes vloeien direct in de staatskas. Wij verrijken onszelf niet, daarmee zouden we een verkeerd signaal afgeven."

**Hoe hebben jullie je op de boetebevoegdheid en de meldplicht datalekken voorbereid?** "Onze mensen hebben een cursus boetebevoegdheid gevolgd en ook de collegeleden bespreken met deskundigen de voetangels en klemmen die je bij het inzetten van de bestuurlijke boetebevoegdheid kunt tegenkomen. Een aantal collega's uit het Markttoezichthoudersberaad zijn eerder teruggefloten door de rechter voor het niet correct hanteren van de boetebevoegdheid. Door vooraf goed alle mogelijke scenario's in kaart te brengen en deze te bespreken, proberen we dat bij de Autoriteit Persoonsgegevens te voorkomen. Voor wat betreft de meldplicht: we hebben samen met het ministerie geprobeerd een inschatting te maken van de hoeveelheid tijd die de meldplicht datalekken ons zal gaan kosten. We zijn er niet uitgekomen. Daarom hebben we een monitorfunctie afgesproken. Deze houdt in dat we tijdelijk extra mensen kunnen inhuren wanneer we merken dat de werkbelasting door het aantal meldingen te groot wordt."

> Het onzichtbare zichtbaar maken, is essentieel voor de privacy-bewustwording

**De meldplicht datalekken en de boetebevoegdheid zijn slechts twee onderwerpen waar het CBP zich op richt. Waar werken jullie nog meer aan?** "Aan het begin van ieder jaar maken we bekend waar onze prioriteiten voor dat jaar liggen, op welke thema's. Dit jaar waren dat onder meer bijzondere persoonsgegevens zoals medische gegevens; de verwerking van persoonsgegevens binnen de arbeidsverhouding; en tot slot profilering, het indelen van personen in bepaalde categorieën door het verzamelen en analyseren van data. Een belangrijk deel van deze thema's zal naar verwachting ook volgend jaar terugkomen."

**Per 1 januari aanstaande wordt de naam van het CBP gewijzigd naar het Autoriteit Persoonsgegevens. Wat is de reden achter deze naamswijziging?** "De naamswijziging naar Autoriteit Persoonsgegevens, dat is toch wel een beetje het toefje op de taart. Het is eigenlijk een heel natuurlijke ontwikkeling, gelet op de komende boetebevoegdheid. Met de boetebevoegdheid ben je ook geen college meer, maar eerder een autoriteit. College vond ik al langer niet passend, het klinkt afstandelijk. Sommige mensen spreken liever over de term waakhond, maar ook dat vind ik geen prettige kreet. Autoriteit is veel passender."

**Wijzigt met de naamswijziging ook iets in jullie toezichtvorm? Gaan jullie bijvoorbeeld on site visits of themaonderzoeken uitvoeren zoals DNB en AFM?** "We blijven toezicht houden zoals we dat altijd al hebben gedaan. Het CBP heeft zo'n vijfenzeventig fte, de AFM en DNB hebben ieder honderden medewerkers. Wij kunnen geen on site visits of themaonderzoeken uitvoeren op de manier waarop AFM of DNB dat doen, gewoonweg omdat we daar de capaciteit niet voor hebben. We voeren wel OTP's uit, onderzoeken ter plaatse. Zo ook toevallig vandaag. Bij een OTP gaan onze medewerkers – al dan niet aangekondigd – bij een organisatie langs. Bij een onderzoek werken we volgens een trechter. We kijken eerst of er mogelijk sprake is van een ernstige overtreding van de Wet bescherming persoonsgegevens. Daarna bekijken we of het een overtreding van structurele aard zou kunnen zijn, daarna of door de overtreding heel veel mensen potentieel problemen zouden kunnen krijgen en tot slot bekijken we of we met onze bevoegdheid een einde aan de overtreding kunnen maken. Een mooi voorbeeld hiervan is het onderzoek bij Nike, dat recent in het nieuws was.
Dit is een groot onderzoek geweest waarbij diezelfde trechter is gehanteerd. Bij Nike was sprake van ernstige, structurele overtredingen, waarvan veel mensen last zouden kunnen hebben en waaraan wij een einde kunnen maken."

**DNB en AFM schenken steeds meer aandacht aan organisatiecultuur en aan gedrag. In hoeverre kijkt het CBP ook naar het gedrag en de cultuur bij organisaties?** "Wij hebben een jaar geleden de koers ingezet op handhaven en daar blijven we ons ook op concentreren. Daarmee wijken we af van de toezichtstrategie van DNB of AFM. Door onze koers consequent te blijven varen – en door de beschikbare jurisprudentie – is het voor de mensen helder wat we doen en waarom we dat doen. Wanneer je maar een capaciteit hebt van vijfenzeventig fte, dan is deze aanpak het meest effectief. Het veranderen van en toezicht houden op cultuur en gedrag kost mankracht en geld. Bovendien heb je medewerking nodig van de sectoren waarop je toezicht houdt. Wij moeten er bij veel organisaties nog voor zorgen dat bij de sectoren het onderwerp privacy goed tussen de oren komt. In de eerste jaren van ons bestaan was er vooral behoefte aan voorlichting en guidance; we ontvingen zes- à zevenduizend verzoeken per jaar van advocaten, bedrijven, overheidsinstellingen et cetera. Dat vonden we logisch, want het was nieuw. Anno 2015 wordt iedereen toch wel geacht de regels te kennen. Nu handhaven we dan ook meer en zijn we minder bezig met guidance. Ik zou wensen dat we meer mensen hadden. Dan zouden we zaken anders kunnen organiseren, bijvoorbeeld door ook meer guidance te geven en meer met mensen in gesprek te gaan. We doen het overigens wel, maar op heel kleine schaal."

**Door alle ontwikkelingen zou je verwachten dat meer mensen inzetten juist noodzaak is. Wat zijn de verwachtingen naar de toekomst?** "Persoonsgegevens zijn het nieuwe goud. In die zin ben ik wel jaloers op DNB. Zij hebben het goud letterlijk in hun kluis liggen en hebben voldoende middelen om het te beschermen. Het goud waar wij toezicht op houden is niet alleen onzichtbaar maar hangt daarenboven ergens in de cloud, is overal en ergens. Om dat goud adequaat te beschermen hebben we meer mensen nodig."

**In hoeverre vindt u de functie van privacy officer en compliance officer verenigbaar?** "Dat hangt van de omvang van de organisatie af. Hoe kleiner de organisatie, hoe meer functies zullen worden gecombineerd. Dat is op zich prima. In de Verenigde Staten heb je veel privacy officers die binnen de compliance-afdeling werkzaam zijn of heb je privacy officers die tevens compliance officers zijn. Ik noem bewust de VS, want zij lopen samen met Duitsland voorop in de functie privacy officer; het is daar al veel meer een begrip. Voor mij is over het algemeen het belangrijkste dat een privacy officer een grote mate van onafhankelijkheid moet hebben, met een directe lijn naar de CEO. De privacy officer moet – indien het geen gecombineerde functie is – zeker niet onder de verantwoordelijkheid van de compliance officer vallen, maar moet naast de compliance officer staan; het moeten twee onafhankelijke functies zijn met elk hun eigen escalatiemogelijkheid."

**In uw speech van vorig jaar oktober (Nationale Denktank Expertforum) pleitte u voor een stevig maatschappelijk debat over big data. Wordt het debat inmiddels stevig (genoeg) gevoerd?** "Nee, de discussie wordt nog niet stevig genoeg gevoerd wat mij betreft. Het grote punt voor ons als toezichthouders, maar zeker ook voor het publiek, is dat wat met jouw data gebeurt onzichtbaar is. Juist het onzichtbare zichtbaar maken is essentieel voor de privacybewustwording. Dit is essentieel voor het vertrouwen van mensen in organisaties, producten en diensten. Het belangrijkste doel van de Wet bescherming persoonsgegevens is eigenlijk 'surprise minimization'. Daarmee bedoel ik dat persoonsgegevens die voor het ene doel worden verzameld, niet opeens in een geheel andere context worden gebruikt voor een geheel ander doel.
Het is bijvoorbeeld niet wenselijk dat aan de balie van het gemeentehuis een onbekende beambte je ineens de vraag stelt hoe het met je drugsverslaafde zoon gaat terwijl je er bent om je rollatoraanvraag in te dienen. Dergelijke vertrouwelijke informatie hoort niet bij elkaar te komen. Bij big data weet je helemaal niet meer wat er met jouw data gebeurt. Er wordt op grote schaal data gekoppeld en er worden allerlei ingewikkelde algoritmes op los gelaten, die geen sterveling snapt. Vervolgens word je op basis van de uitkomsten van het algoritme behandeld. Dit lijkt mij geen goede ontwikkeling en ik vind dat we daar echt nog veel te weinig over praten.
Wat ik wel een goede ontwikkeling vind, is dat de regering aan de Wetenschappelijke Raad voor het Regeringsbeleid heeft gevraagd een notitie op te stellen over big data. De hoop is dat deze notitie begin volgend jaar verschijnt en dat dit een zwengel geeft aan de big data-discussie, ook in politieke zin."

**Wat betekent privacy voor u persoonlijk?**
"Ik probeer voorzichtig te zijn. Ik heb bijna vijfentwintig jaar als politicus gewerkt en er is veel over mij bekend. In die zin woon ik in een glazen huis. Dat vind ik niet vervelend, het hoort erbij. Ik doe niet aan Facebook en WhatsApp. En ik zoek via privacyvriendelijke zoekmachines als DuckDuckGo en Ixquick. Privacy loopt eigenlijk als een rode draad door mijn leven. Als student heb ik geweigerd mee te werken aan de laatste volkstelling, omdat ik het ongepast vond – ik riskeerde daarmee een boete van ƒ 400,- wat toen ongeveer mijn maandinkomen vertegenwoordigde – en ik ben als staatssecretaris betrokken geweest bij de indiening van de Wet bescherming persoonsgegevens. Al met al heb ik destijds met grote overtuiging gesolliciteerd op deze functie."

> De naamswijziging naar Autoriteit Persoonsgegevens, dat is toch wel het toefje op de taart

**Welk advies zou u aan de lezers mee willen geven?**
"We hebben net de internationale privacyconferentie achter ons liggen. Daar heeft Daan Roosegaarde een openingsspeech gehouden. Hij vertelde dat er bij nieuwe ideeën altijd drie reacties zijn die ergerniswekkend zijn. De eerste is: 'Ja maar'. De tweede is: 'Het mag niet'. De derde is: 'Dat is niet nieuw, dat hadden we zelf ook wel kunnen verzinnen'. Ik denk dat privacy officers ook 'Nee het mag niet' moeten kunnen zeggen, maar dat ze vooral verleidelijk moeten zijn; dat ze iemand dusdanig moeten kunnen verleiden dat hij zijn plannen uitvoert zonder in strijd te komen met de Wet bescherming persoonsgegevens. Dus niet alleen nee zeggen, maar écht verleiden om het goede te doen."

# Corruptiebestrijding in de praktijk – deel twee

## Het third party due diligence-proces

Geert Vermeulen

**In het vorige nummer van De Compliance Officer heb ik een artikel geschreven over de verdenkingen van corruptie rond de FIFA. Sinds die tijd is de wereldvoetbalbond niet meer uit het nieuws geweest. De ontwikkelingen blijven zich opvolgen en het net rond Blatter en de zijnen lijkt zich verder te sluiten. Inmiddels hebben diverse banken het verzoek gekregen om medewerking te verlenen aan het onderzoek naar verdachte, aan de FIFA-bestuurders gerelateerde, geldstromen op grond van de anti-witwaswetgeving. Ook is er commotie ontstaan over de toewijzing van het WK voetbal in 2006 aan Duitsland en heeft er een inval plaatsgevonden door de autoriteiten bij de Duitse voetbalbond. De ethische commissie van de FIFA heeft een aantal bestuurders, waaronder de heren Blatter en Platini, voorlopig op non-actief gesteld, hangende een onderzoek naar verdachte betalingen. Wellicht meer hierover in een volgende DCO.**

**Waarom is third party due diligence belangrijk?**
Het vorige artikel heb ik afgesloten met de oproep aan compliance officers in Nederland om due diligence uit te voeren op derde partijen. In het artikel werd aangehaald dat Nike in de jaren 90 een groot bedrag aan sport-marketingbedrijf Traffic heeft betaald om een sponsordeal met de Braziliaanse voetbalbond in de wacht te slepen. Traffic heeft hoogstwaarschijnlijk (een deel van) dit bedrag doorbetaald aan functionarissen van de Braziliaanse voetbalbond, waaronder de voorzitter van de bond.

Verdachte betalingen aan derde partijen zijn wel vaker in het nieuws en kunnen enorme boetes tot gevolg hebben. Enige tijd geleden is Ballast Nedam bijvoorbeeld een schikking van € 17 miljoen overeengekomen met het Openbaar Ministerie wegens het betalen van steekpenningen aan buitenlandse tussenpersonen om opdrachten binnen te slepen. SBM Offshore heeft zelfs een schikking van US$ 240 miljoen getroffen met het OM wegens verdachte betalingen aan derde partijen. Al de tien grootste schikkingen op grond van de FCPA, de Amerikaanse anti-corruptiewet, draaien rond betalingen aan derde partijen. Op het moment van schrijven is Vimpelcom – één van 's werelds grootste telecom-bedrijven, waarvan het hoofdkantoor is gevestigd in Amsterdam – in het nieuws omdat het betalingen verricht zou hebben aan Takilant Ltd – een vehikel waarachter de dochter van de president van Oezbekistan schuil gaat – om een telefoonlicentie in Oezbekistan te verkrijgen. Vimpelcom heeft inmiddels een voorziening van US$ 900 miljoen getroffen in het kader van het onderzoek naar deze betaling en staat volgens Reuters op het punt voor US$ 775 miljoen te schikken met de SEC. De voormalige CEO van het bedrijf, een Noor, is gearresteerd door de Noorse autoriteiten en de CFO van Vimpelcom, Henk van Dalen, heeft zijn functie als commissaris bij de Rabobank en de Brabantse Ontwikkelings Maatschappij tijdelijk neergelegd in afwachting van de uitkomsten van het onderzoek.

Waar third party due diligence de belangrijkste beheers-maatregel is om corruptie te voorkomen, levert het soms

ook 'bijvangst' op. Third party due diligence kan bijvoorbeeld ook helpen bij het bestrijden van fraude en andere onethische praktijken.

Maar hoe doe je due diligence op derde partijen? In dit artikel geef ik een aanzet daartoe.

**ICC Anti-Corruption Third Party Due Diligence guide en overige bronnen**

Het toeval wil dat in de tussentijd de International Chamber of Commerce (ICC) een boek heeft gepubliceerd genaamd 'ICC Anti-Corruption Third Party Due Diligence: A Guide for Small and Medium Size Enterprises'. Een uitstekend boekwerk wat in totaal toch nog zo'n veertig pagina's telt. Het vormt een welkome aanvulling op het eerder verschenen 'Good Practice Guidelines on Conducting Third-Party Due Diligence' van het Partnership Against Corruption Initiative (PACI) van het World Economic Forum (WEF), wat meer geschreven is voor de wat grotere ondernemingen. Voor Nederlandse financiële instellingen is uiteraard het document 'Good Practices Bestrijden Corruptie' van De Nederlandsche Bank van belang. Zelf heb ik ook al eens over third party due diligence gepubliceerd.[1] Uit al deze documenten blijkt dat het third party due diligence proces uiteenvalt in een aantal fases. In dit artikel beschrijf ik de eerste drie fases:

- Identificatie van derde partijen
- Verzamelen van derde partijen
- Bepalen van het risico

**Identificatie van derde partijen**

De eerste stap die gezet moet worden is bepalen wie jouw derde partijen zijn. Dat is voor elke bedrijfstak en zelfs voor elk bedrijf verschillend.

In de Verenigde Staten heeft men het hierbij over 'agents': derde partijen die namens jou optreden en je helpen bij het binnenhalen of behouden van je business. Dit kunnen verkoopagenten, distributeurs en andere tussenpersonen zijn. Maar ook de expediteur die de logistiek regelt, inclusief de afhandeling van het douaneproces in risicovolle landen. Of het advocatenkantoor wat helpt bij het verkrijgen van een vergunning in een land aan de andere kant van de wereld. Of de belastingadviseur die ter plekke helpt bij de belastingaangifte. Of de 'adviseur' die betrokken is bij een verkoopdeal. Of bij een inkoopproces.

Dat laatste lijkt op het eerste gezicht nogal vergezocht. Niet zo lang geleden bleek echter dat bij een tender van de NS voor de aankoop van de sprinters een adviseur betrokken was, die door een medewerker van de Canadese treinenbouwer Bombardier is omgekocht om vertrouwelijke informatie over de tender te verstrekken.[2] In dit geval was er geen sprake van omkoping door de NS maar door Bombardier en naar het zich doet aanzien heeft Bombardier naar aanleiding hiervan haar CEO Benelux ontslagen.[3]

Om dit te voorkomen had de NS meer due diligence kunnen doen op deze adviseur. Niet zozeer om actieve omkoping te voorkomen, maar meer om te voorkomen dat het slachtoffer zou worden van passieve omkoping of fraude. Naar verluidt was dezelfde adviseur ook betrokken bij de aankoop van de Fyra. In de pers is vermeld dat hij daarbij twitterde over de luxereisjes naar de fabriek van AnsaldoBreda in Italië.[4] Een betere due diligence op en monitoring van deze adviseur had wellicht een hoop ellende kunnen voorkomen.

Een ander voorbeeld van derde partijen zijn 'fixers', die bijvoorbeeld door buitenlandse correspondenten van kranten en televisiestations gebruikt worden om te navigeren door verre landen met andere gewoonten. Deze fixers proberen ook te voorkomen dat verslaggevers in al te gevaarlijke situaties belanden en kunnen ervoor zorgen dat zij de juiste mensen kunnen spreken. Bij mediabedrijven is het gebruik van fixers in verre oorden de normaalste zaak van de wereld. Echter, wat 'fixen' zij precies en hoe?

---

1 Zie: *Ondernemen zonder Corruptie, Normenkader, management en praktijkervaringen,* mr. M.J. van Woerden (eindredactie), hoofdstuk 14.

2 Zie: 'Topman van Bombardier kocht informatie over NS', *NRC Handelsblad* 10 juli 2015.

3 Zie wederom: 'Topman van Bombardier kocht informatie over NS', *NRC Handelsblad* 10 juli 2015.

4 Zie: 'NS onderzoekt mogelijke omkoping bij aanschaf nieuwe Sprinter', *het Financieele Dagblad* 25 februari 2015 en 'NS onderzoekt omkoping bij aanbesteding sprinters', *NRC Handelsblad* 25 februari 2015.

In het Verenigd Koninkrijk heeft men het niet over 'agents' maar over 'associated persons': bedrijven en personen die diensten aan jou of namens jou verlenen. Deze term is nog wat breder dan die van agents. Zo worden de eigen medewerkers er ook wel onder geschaard. En alle partijen in het inkoopkanaal.

Een goede manier om je derde partijen op het spoor te komen is een nadere bestudering van de uitgaande betalingen. Wie betaal je allemaal en waarom? Een inventarisatie en categorisering van je uitgaande betalingen levert doorgaans een goed beeld op van je derde partijen. Helaas levert het niet altijd een volledig beeld op. In de financiële sector bijvoorbeeld zou je in ieder geval iedere partij die je een commissie betaalt bij de verkoop van een financieel product in aanmerking moeten nemen voor het uitvoeren van due diligence. Echter, sinds de invoering van het provisieverbod voor bepaalde producten worden sommige tussenpersonen niet meer door de bank of door de verzekeraar betaald. Toch raad ik aan om te onderzoeken welke risico's zich alsnog kunnen voordoen rond deze tussenpersonen. Ook kan het voorkomen dat betalingsstromen expres worden verlegd om het zicht op een betrokken partij te ontnemen.

Een bijzondere categorie derde partijen zijn de bedrijven met wie je een joint venture bent aangegaan. In de olie- en gas industrie is het gebruikelijk dat, indien er een veelbelovende bron in een ontwikkelingsland wordt ontdekt, er een joint venture wordt gevormd tussen een oliebedrijf, die de benodigde technologische kennis en ervaring inbrengt, alsmede het netwerk om de olie of het gas te verkopen, en een staatsbedrijf, waardoor het land waarin de olie of het gas is gevonden er ook wat aan verdient. Echter, wie zitten er precies achter dat staatsbedrijf? En wie zitten in de directie van dat bedrijf? Hoeveel krijgen de bestuurders betaald en wat moeten zij in ruil daarvoor doen? Belanden de opbrengsten van het staatsbedrijf uiteindelijk wel in de staatskas?

In sommige landen bestaat er een wettelijke verplichting voor buitenlandse bedrijven om een joint venture op te richten met een lokaal bedrijf. In het Midden-Oosten, Noord-Afrika, Zimbabwe, in sommige landen die vroeger deel uitmaakten van de Sovjet-Unie en (in het verleden) in China komt dit vaak voor. Vaak wil je dan een partner met kennis van de lokale markt die je behulpzaam is bij het genereren van business. In het Midden-Oosten dient je lokale partner je te introduceren in de lokale ondernemingsnetwerken, anders zul je daar waarschijnlijk geen zaken doen. Maar hoeveel krijgen deze partners betaald voor het werk wat ze doen? Wie zijn zij? Wie zitten er achter deze bedrijven? Hoeveel (politieke) invloed hebben ze precies en waarom?

En stel dat je een minderheidsaandeel hebt in de joint venture, hoe comfortabel ben je dan met de gang van zaken in dit bedrijf? Mag je er bijvoorbeeld een audit uitvoeren?

**Verzamelen van de derde partijen**

De tweede stap is het verzamelen van alle derde partijen in een centrale database. Dit helpt om een beter zicht te krijgen op de aantallen, de risico's en de voortgang. Als compliance officer heb je doorgaans beperkte middelen tot je beschikking. Je moet kiezen aan welke partijen je meer of minder aandacht gaat besteden. Uiteraard wil je de meeste aandacht besteden aan de grootste risico's. Je moet dus inzicht hebben in waar de grootste risico's liggen. Meer hierover in de volgende paragraaf. Ook wil je weten hoe ver je bent met due diligence en wat de (voorlopige) resultaten hiervan zijn. Indien je bedrijf in hoogrisicolanden actief is en met duizenden derde partijen samenwerkt, dan zou het toch wel vreemd zijn als die allemaal goedgekeurd worden. Indien je te maken krijgt met de Amerikaanse autoriteiten, dan zullen die vragen hoeveel partijen er niet goedgekeurd zijn, welke dat zijn en waarom zij niet zijn goedgekeurd. Dit is één van de manieren waarop zij door 'papieren' compliance-programma's proberen heen te prikken.

Indien je als compliance officer meerdere landen coördineert, dan krijg je in dit stadium te maken met de vereisten uit data-privacywetgeving. Er is namelijk een grote kans dat er private personen tussen die derde partijen zitten. De contactpersonen bij en bestuurders van je derde partijen zijn natuurlijk ook natuurlijke personen. Met een beetje geluk heeft de organisatie waarvoor je werkt reeds de beschikking over centrale databestanden en is de overdracht van persoonsgegevens tussen de verschillende landenorganisaties binnen het bedrijf al geregeld, bijvoorbeeld middels 'binding corporate rules'. Mocht dit nog niet geregeld zijn – wat in de praktijk vaak het geval is – dan moet je er rekening mee houden dat binnen de EU persoonsgegevens m.b.t. derde partijen

> Een goede manier om je derde partijen op het spoor te komen is een nadere bestudering van de uitgaande betalingen

niet zonder meer uitgewisseld kunnen worden. En ook mag je niet zonder meer due diligence doen op de betrokken personen. Mogelijk moet daarvoor toestemming worden gevraagd van de betrokkenen en/of van de nationale autoriteiten. Dit zal vaak het geval zijn in landen als Duitsland, Spanje en Frankrijk. In andere landen dienen de betrokken derde partijen vaak ten minste geïnformeerd te worden en de mogelijkheid te worden geboden om bezwaar te maken.

De situatie wordt nog lastiger indien er sprake is van de overdracht van persoonsgegevens buiten de EU. Indien je bedrijf niet werkt onder binding corporate rules, dan moet er gebruik gemaakt worden van standaardcontracten tussen de betrokken entiteiten. In het verleden heb ik regelmatig gebruik gemaakt van het Safe Harbor-protocol bij de overdracht van persoonsgegevens naar de Verenigde Staten. Dit mechanisme voor de overdracht van persoonsgegevens kan sinds de recente uitspraak van het Europese Hof van Justitie niet meer gebruikt worden. Om een en ander verder te compliceren heeft Rusland in september wetgeving ingevoerd die er toe leidt dat persoonsgegevens van Russen in Rusland bewaard moeten worden. Hoe hiermee om te gaan?

Een oplossing kan dan zijn dat het due diligence-proces lokaal wordt uitgevoerd, waarbij de resultaten geanonimiseerd geconsolideerd worden. Mocht de organisatie waarvoor je werkt echter onderzocht worden door de autoriteiten, dan zullen deze autoriteiten niet snel genoegen nemen met geanonimiseerde gegevens. Maar je kan dan in ieder geval alvast beginnen met het due diligence-proces, terwijl je tegelijkertijd werkt aan een oplossing voor de data-privacyproblemen. Desalniettemin dien je jezelf te realiseren dat in een land als China de lokale wetgeving m.b.t. het uitvoeren van achtergrondonderzoek bijzonder lastig is. En je moet lokaal ook over voldoende kennis en kunde en betrouwbare medewerkers beschikken om het due diligence-proces lokaal uit te kunnen voeren.

Zodra je meer inzicht hebt in de hoeveelheid derde partijen wordt het tijd om ze te differentiëren naar de mate van risico.

**Bepalen van het risico**

Aangezien je als compliance officer niet over ongelimiteerde middelen beschikt, zul je de meeste aandacht willen besteden aan de meest riskante derde partijen. Daarnaast wil je de reguliere processen in je organisatie niet meer vertragen dan noodzakelijk. De diverse brondocumenten (zie paragraaf 2) noemen de volgende risicofactoren:

- landenrisico;
- bedrijfstakrisico;
- type relatie;
- omvang van de transactie(s);
- wel/geen interactie met publieke sector.

*Landenrisico*

In sommige landen bestaat er een groter risico op corruptie dan in andere landen. Elk jaar publiceert Transparency International de Corruption Perception Index (TI CPI). Dit is de meest gebruikte indicator om aan te geven hoe corrupt een land is. Er is echter ook de nodige kritiek op de index. Er wordt namelijk een poging gedaan om een perceptie van corruptie te meten. De wijze waarop de index tot stand komt is wellicht niet geheel wetenschappelijk verantwoord; het is vooralsnog de beste indicator die beschikbaar is. Althans, onlangs heeft TRACE een index gepubliceerd, die wat beter aansluit bij mijn eigen ervaringen in de diverse landen.[5] Maar vooralsnog wordt meestal de TI CPI gebruikt.

Overigens is het niet verstandig om volledig blind te varen op de reputatie van een land. In het algemeen wordt

5 Zie: www.traceinternational.org/trace-matrix. Landen als Qatar, India, China en Bangladesh zijn volgende Transparency International minder corrupt dan volgens TRACE. Volgens TI is Frankrijk corrupter dan België. Volgens TRACE is dit andersom. Volgens TI zijn Zimbabwe en Noord-Korea corrupter dan Nigeria. Volgens TRACE is dit andersom.

Nederland bijvoorbeeld gezien als een land waar relatief weinig corruptie voorkomt. Dat lijkt me ook terecht. Maar het betekent niet dat er in Nederland geen corruptie voorkomt. Inmiddels is bijvoorbeeld wel bekend dat diverse banken, bij de verkoop van rentederivaten aan woningcorporaties, stevige commissies betaalden aan FIFA Finance, de adviseur van een aantal woningcorporaties, die overigens niets te maken heeft met de gelijknamige voetbalbond. Uit het boek 'De bekentenis' blijkt dat een deel van deze commissies door FIFA Finance werd doorbetaald aan de financieel directeuren van bijvoorbeeld Vestia en Havensteder, die deze financiële instrumenten aankochten. Of denk bijvoorbeeld aan het Rotterdamse havenschandaal, waar onlangs ook een boek over is verschenen. De laatste jaren is ook een groeiend aantal Nederlandse politici in opspraak gekomen wegens corruptie. Ook in Nederland loont het de moeite om due diligence te doen op derde partijen.

*Bedrijfstakrisico*
In sommige bedrijfstakken is het corruptierisico groter dan in andere bedrijfstakken. De ICC-guide noemt bijvoorbeeld de bouw, de vastgoedsector, nutsbedrijven, de olie- en gasindustrie, mijnbouw, telecommunicatie, de farmaceutische industrie, de logistieke sector, de luchtvaart, de defensie-industrie en (opmerkelijk genoeg) de financiële sector. Dit komt overeen met mijn eigen ervaringen.

*Type relatie*
Sommige type relaties zijn riskanter dan andere. Mijns inziens is er bijvoorbeeld weinig risico bij het gebruik van een distributeur van relatief goedkope consumentengoederen. Ik kan me voorstellen dat Unilever en Procter & Gamble vanuit een anti-corruptieperspectief relatief weinig zorgen hebben over de verkoop van hun producten door Albert Heijn en Jumbo in Nederland. Dat ligt anders wanneer een handelsagent en/of consultant zich zou melden bij een baggeraar voor een maritiem project in Indonesië. Bij de inschatting van het risico is hierbij het landenrisico, bedrijfstakrisico, type relatie en de omvang van de transactie van belang.

*Omvang van de transactie(s)*
Relevant is ook hoeveel de derde partij betaald krijgt, zowel per transactie als in totaal. Wat is de kans dat een deel van dat geld gebruikt wordt om iemand om te kopen? Als je bijvoorbeeld als verzekeraar verzekeringen verkoopt aan particulieren via een supermarkt, waar de supermarkt een paar euro per verzekering aan overhoudt, dan is de kans dat die paar euro gebruikt wordt om de consument om te kopen nihil. Dat ligt anders als er een financieel adviseur betrokken is bij de verkoop van renteswaps aan een woningbouwcorporatie, waarbij de adviseur een commissie van enkele tonnen ontvangt.

> Weinig corruptie betekent niet dat er geen corruptie voorkomt

*Interactie met de publieke sector*
Hoewel omkoping in de private sector in veruit de meeste landen verboden is, is het risico op vervolging en de hoogte van de straf aanzienlijk hoger bij omkoping van ambtenaren of andere personen die werkzaam zijn in de publieke sector. Daarom dient interactie met de publieke sector ook te worden gezien als een risicofactor.

Als je uiteindelijk al je derde partijen hebt verzameld en hebt onderverdeeld in risicocategorieën, hoe moet je dan verder? Meer hierover in de volgende DCO.

# Pizza privacy matters


Hongerig na een lange reis, pakte ik de eerste avond in Amerika enthousiast de huistelefoon om pizza te bestellen. Aan de andere kant van de lijn vroeg de medewerkster naar mijn telefoonnummer om de bestelling te kunnen plaatsen. Ik had geen idee wat mijn nummer was. Het stond nergens genoteerd en we waren net aangekomen in ons tijdelijke huis. Ik vroeg haar of ze dit niet toevallig op haar computerscherm kon zien. Hierop antwoordde ze dat ze inderdaad mijn telefoonnummer kon zien, maar ze mocht – om privacyredenen – dit nummer niet overnemen. Ik moest het haar zelf vertellen, anders mocht ze de bestelling niet plaatsen.

Wat betreft privacy vraag ik me af wat de fundamentele verschillen zijn tussen Nederland en Amerika. En ik kan u alvast verklappen dat aangaande privacy ik tegenstrijdige signalen oppik. Als ik hier vraag of men privacy belangrijk vindt, is de reactie: "Ja, heel belangrijk." Dat is steevast het antwoord, ongeacht welke wet of regel het betreft. Amerikanen[1] zeggen al snel dat een regel belangrijk is. Hier hoef ik bijvoorbeeld ook niet uit te leggen wat een compliance officer doet. Iedereen weet dat.
Maar dat strookt niet met mijn ervaringen als nieuwkomer in de Amerikaanse maatschappij. Ik heb het dan niet over de gewichtige zaken die Edward Snowden onthulde. Nee, ik doel dan op de 'robocalls' en 'autodialers'. Een verschijnsel wat ikzelf niet ken in Nederland. Computers die willekeurig telefoonnumers bellen. Als je opneemt, wordt er een bericht afgespeeld of je wordt ongevraagd doorverbonden met een medewerker. Wekelijks krijg ik dergelijke telefoontjes. Van politieke partijen en vakbonden tot aan telemarketeers en oplichters.

Wellicht verklaart de Fudge Factor-theorie[2] mijn gepercipieerde tegenstrijdigheid. Iedere maatschappij is in gelijke mate eerlijk. Echter, iedere maatschappij maakt op andere terreinen verschil tussen hun wettelijke normen en wat men sociaal werkelijk aanvaardbaar vindt. Bijvoorbeeld als het gaat om betalen van belastingen, vergunningaanvragen of alcohol in het verkeer. En ik vermoed dat op het gebied van privacy Amerikanen juist meer dulden dan hun wet toestaat.

Voor mij is de kern van privacy de bescherming van mijn persoonlijke levenssfeer. Elke ongevraagde benadering via de telefoon zie ik als een aantasting van mijn privacy. Ik zit er niet op te wachten en ik heb er niet om gevraagd. Zoiets. Bovendien acht ik mijn recht op privacy bijna even hoog als mijn recht op vrije meningsuiting, om maar wat te noemen. Schouderophalend grinniken mijn Amerikaanse collega's om mijn verontwaardiging over de robocalls. Het landelijke bel-me-niet-register biedt soelaas, maar niet helemaal. Politieke partijen zijn bijvoorbeeld toegestane uitzonderingen.

In de Economist las ik dat Amerikanen privacy meer beschouwen als een soort consumentenrecht. Zelf ben ik er nog niet uit waar het fundamentele verschil zit.[3]
Die eerste avond wist ik de pizzamedewerkster niet te overtuigen dat mijn privacy echt niet in het gedrang was. Die pizza kreeg ik dus niet, wel een portie ongevraagde telefoontjes.

Groetjes,
Joost

*Joost Montens werkt voor AstraZeneca, een innovatief biofarmaceutisch bedrijf. Sinds februari 2015 woont en werkt hij in de Verenigde Staten. In deze column bericht hij over zijn compliance-ervaringen en bevindingen.*

1 Vergeef me de overdreven simplificatie. Het is hetzelfde als een uitspraak over 'de' Europeaan, van de Oeral tot aan IJsland.

2 Lees of bekijk het werk van Dan Ariely, The Honest Truth About Dishonesty (danariely.com)

3 Voor belangstellenden, een grondige vergelijking tussen EU en US: www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf?_sm_au_=iHH4sPrNLVZTr78j

## Speakers' Corner: Petrosjan Damen en Hans Ludo van Mierlo

# 'Goed Vakmanschap' als kernbegrip voor iedereen in financiële sector

Veel medewerkers in de financiële sector verkeren in een ongemakkelijke spagaat. Hun eigen professionele inzicht lijkt steeds meer ondergeschikt te raken aan richtlijnen van toezichthouders en aan ondersteunende systemen. De steeds grotere focus op het naleven van regels staat diametraal tegenover die andere ontwikkeling die in de financiële sector is ingezet na de financiële crisis: de focus op de klant.

In de bankierseed, die alle bankmedewerkers inmiddels hebben afgelegd, beloven zij dat ze 'een zorgvuldige afweging maken tussen de belangen van partijen die bij de onderneming betrokken zijn, in het bijzonder die van de klanten en de maatschappij'. Met de eed wordt dus niet alleen het klantbelang centraal gesteld, maar ook een beroep gedaan op de deskundigheid en het morele kompas van iedere individuele medewerker.

Het hinken op twee gedachten, enerzijds meer nadruk op externe regels en systemen en anderzijds een beroep op het eigen professionele en morele inzicht van de individuele medewerker, zorgt ervoor dat veel bankmedewerkers zich erg ongemakkelijk voelen. Deze schijnbare tegenstelling tussen extrinsieke en intrinsieke sturing maakt dat professionals niet meer weten wat nu echt prioriteit heeft: het goed bedienen van de klant of een uitgebreide verantwoording voor elk advies in het dossier van de klant? Bij deze worstelling staan twee spanningsvelden centraal.

**Spanningsveld**

Een eerste spanningsveld gaat over de vraag hoe beslissingen worden genomen door financiële dienstverleners. Vertrouwt de professional volledig op de externe regels of blijft hij ook zelf nadenken. Dat zelf nadenken wordt de laatste tijd stevig ontmoedigd. Steeds vaker proberen de wetgever en toezichthouders te bepalen hoe een financieel professional in de praktijk dient te handelen. Daar komt nog eens bij, dat veel IT-systemen een kritiekloze naleving van regels afdwingen in de procesgang. Ook als hij dat echt wil, dan nog heeft de professional geen of weinig ruimte om naar eigen inzicht af te wijken van de externe stuurmiddelen.

**Sta-in-de-weg**

Een tweede spanningsveld heeft betrekking op de vraag op welk detailniveau een goede beslissing genomen moet worden. De wetten en richtlijnen die de overheid en toezichthouders aan de financiële sector hebben meegegeven zijn zo opgesteld dat ze generiek toepasbaar zijn. Ze kijken naar situaties op een algemeen niveau. Op hoog abstractieniveau kloppen ze. Op detailniveau, op het niveau van de adviseur en de klant, zijn ze soms een regelrechte sta-in-de-weg voor een goede oplossing. Klanten willen specifieke oplossingen voor specifieke situaties. Voor betrokken bankmedewerkers is het juist een uitdaging om in specifieke gevallen met specifieke oplossingen te komen. Daarvoor heb je immers al die opleidingen gedaan. Financiële dienstverlening op detailniveau, daar kun je

# Goed zeemanschap als voorbeeld voor de financiële sector

je als professional in onderscheiden.
Het ongenoegen binnen de financiële sector over het werken met geboeide handen neemt met de dag toe. De financiële sector wil zich revancheren na het gezichtsverlies door de financiële crisis en recente schandalen rond inadequate producten. Ze ervaart de vele en ogenschijnlijk tegenstrijdige opdrachten waar ze vandaag aan moet voldoen eerder als een belemmering dan als een steun in de rug.

**Gezond verstand**

Er is wel degelijk een goede uitweg uit de ongemakkelijke spagaat waarin veel financiële dienstverleners zeggen te verkeren. Daarvoor verwijzen we graag naar het concept van 'goed zeemanschap'. Dit is een officieel begrip dat is vastgelegd in het Binnenvaart Politie Regelement. Het reglement zegt met zoveel woorden, dat een schipper van de gegeven regels moet afwijken indien de omstandigheden dat vereisen: 'De schipper moet in het belang van de veiligheid of de goede orde van de scheepvaart, voor zover dit door de bijzondere omstandigheden waarin het schip zich bevindt is geboden, volgens goed zeemanschap afwijken van de bepalingen van dit reglement.'

Het lijkt in eerste instantie nogal een tegenstrijdig principe: een generieke regel die stelt dat je moet afwijken van de regels indien de specifieke situatie dat vereist. Het is echter een hele logische manier om de beslissingsbevoegdheid te leggen waar die hoort. Alleen de schipper ter plekke kan in een concrete situatie beoordelen wat er op dat moment op die plek onder die omstandigheden dient te gebeuren. Natuurlijk zijn en blijven de regels voor een schipper een zeer belangrijk extern stuurmiddel. Maar dezelfde regels verplichten hem ook zijn gezond verstand te gebruiken tijdens zijn werk en zijn gedrag in verschillende situaties daar op aan te passen.

**'Goed vakmanschap'**

Het concept van goed zeemanschap kan iedereen die bij de financiële sector betrokken is – dus zowel wetgever, toezichthouders, adviseurs, maar ook klanten en media – helpen goed zicht te krijgen op de persoonlijke vrijheid van iedere professional binnen de sector. Wij pleiten daarom voor het introduceren van het begrip 'Goed vakmanschap' in de financiële sector. Dit begrip kan dienen als een flexibel kompas. Het begrip geeft aan dat een professional steeds een optimum dient te zoeken tussen de externe kaders en zijn eigen professionale inschatting die het belang van een individuele klant centraal stelt. Dit concept biedt de professional niet alleen ruimte, maar dwingt hem ook steeds zelf na te blijven denken. Het principe van 'goed vakmanschap' zorgt voor de synthese tussen de generieke regels en de specifieke toepassing daarvan in concrete gevallen.
Goede financiële dienstverlening is de afgelopen jaren steeds meer een synoniem geworden voor geen foute financiële dienstverlening. Het vervaardigen van een goed klantendossier was eerder gericht op zelfverdediging dan op het klantbelang. Daarmee breng je de creativiteit en het zelfvertrouwen in de sector en het plezier in het werk niet terug. De klant centraal stellen vraagt niet om 'afvinken', maar om inleven en meedenken.

Een pleidooi voor meer vrije ruimte voor professionals, betekent niet dat we er ook voor pleiten dat individuele medewerkers zich niet aan de regels houden. Wij willen dat individuele medewerkers zich aangemoedigd weten om zelf professioneel te blijven meedenken. Zodra zij op situaties stuiten waarbij regels of systemen het klantbelang onnodig tegenwerken dan dienen zij ergens aan de bel te kunnen trekken. Sterker nog, ze zouden aan die bel moeten trekken. Dat zijn ze aan hun klanten en hun vakmanschap verplicht. Regels en systemen zijn immers slechts hulpmiddelen en op zich niet heilig. In het belang van de klant moet daar dus van afgeweken kunnen worden. Ministers en burgmeesters kennen een 'discretionaire bevoegdheid' om in bijzondere gevallen van wettelijke regels afwijkende beslissingen te nemen. Wij pleiten ervoor, dat ook financiële professionals zo'n mogelijkheid krijgen.

**Randvoorwaarden**

Het afwijken van regels ten behoeve van de klant kan nooit een doel op zichzelf zijn. Het is ook niet onze bedoeling een nieuw artikel in de wet op te nemen, die ruimte zou kunnen bieden voor nieuwe uitwassen. Om het concept van 'Goed vakmanschap' te laten werken hoeven slechts enkele randvoorwaarden ingevuld te worden. Zo moet elke bewuste afwijking van de regels in het belang van de klant professioneel gesignaleerd, beargumenteerd en geregistreerd worden. Op die manier kunnen interne en externe toezichthouders zicht houden op de professionaliteit en integriteit binnen de organisatie. Is er sprake van systematische afwijking van de regels dan is er kennelijk iets aan de hand.

Het kan wijzen op de behoefte aan betere uitleg van de regels, aan betere scholing of de noodzaak de regels of de IT-programma's aan te passen.

**Reflectiekamer**
De zoektocht naar de hardheid van de regels is een weg, die iedere professional binnen de organisatie moet gaan. Je moet natuurlijk wel eerst de regels kennen en begrijpen voordat die je in een specifiek geval ter discussie stelt. We pleiten er daarom ook voor binnen financiële instellingen een zogenaamde 'reflectiekamer' in te stellen. We denken hierbij een select groepje senioren die – op eigen initiatief of op verzoek van collega's – actuele en eventueel aankomende kwesties doornemen om daaruit lessen te trekken. De reflectiekamer lijkt daarin misschien wel wat op een commissie ethiek, die sommige grote instellingen al kennen en die zich uitspreekt over specifieke ethische en maatschappelijke kwesties.

De introductie van het begrip 'Goed vakmanschap' in de financiële sector verdient brede steun. Natuurlijk moet de sector zelf er allereerst in willen geloven en er voor willen gaan. Daarnaast is de oprechte steun nodig van politiek, toezichthouders, consumentenorganisaties, onderwijs en de financiële pers. Niemand is gebaat bij een aangeschoten financiële sector zonder zelfvertrouwen. Iedereen is gebaat bij een financiële sector, waarin zelfbewuste professionals op basis van hun professionaliteit met trots doen wat ze met hun beroepseed beloofd hebben. Zo voorkomen we dat we samen met open ogen opnieuw een financiële schipbreuk leiden.

*Petrosjan Damen is zelfstandig organisatieadviseur en promotieonderzoeker bij Nyenrode Business Universiteit. Hij doet onderzoek naar het effect van stuurmechanismen op het gedrag van besluitvormers in de financiële sector.*

*Hans Ludo van Mierlo is bestuurdersadviseur, oud-bankier, publicist en geestelijk vader van de bankierseed. Hij schreef o.m. het boek 'Gepast en ongepast geld' en 'Bankiers zweren bij geld'.*

> Maatwerk vraagt om uitzonderingen op de regels

## Klanten helpen met geboeide handen

*Alle financiële adviseurs kunnen voorbeelden geven van situaties waarin van regels en IT-systemen ingaan tegen het belang van de klant.*

**I. Beleidswijziging overlijdensverzekering**
Een klant met een overlijdensverzekering is terminaal ziek. Hij wil een deel van zijn uitkering voor overlijden ontvangen om de laatste paar maanden van zijn leven nog iets met zijn kinderen te kunnen doen, maar volgens de regels wordt er niet uitgekeerd voor overlijden.
*Oplossing:* Nadat een medewerker diep in deze kwestie is gedoken, is in deze specifieke situatie het verzoek van de klant mogelijk gemaakt.
*Stand van zaken:* De verzekeraar heeft dit inmiddels in meer gevallen mogelijk gemaakt.

**II. Persoonlijke inschatting uitgeschakeld**
Twee enthousiaste jonge artsen in opleiding met prima carrièreperspectief vragen een hypotheek aan voor een huis dat volgens de algemene regels net buiten hun financiële bereik ligt.
*Oplossing:* De bank praat met de twee jonge mensen over hun toekomstverwachtingen en is op grond daarvan bereid de hypotheek toch te verstrekken. De jonge artsen wonen plezierig in hun huis en kunnen de hypotheek gemakkelijk aflossen.
*Stand van zaken:* De bank werd door toezichthouder AFM berispt. Alle banken houden zich nu nog strakker aan de rigide regels, waardoor ook succesvolle starters minder gemakkelijk een lening krijgen en de professionaliteit van de bankmedewerker (persoonlijke inschatting) er minder toe doet.

**III. Geen hypotheek voor miljonair**
Een oud-ondernemer in ruste met een groot vermogen vraagt een hypotheek van enkele tonnen op zijn huis van meer dan een miljoen euro. Daarmee wil hij in Amsterdam een huis voor zijn studerende dochter kopen. De hypotheek wordt hem geweigerd omdat hij geen vast inkomen heeft.
*Oplossing:* Er wordt geen oplossing gevonden.
*Stand van zaken:* Klant boos. Bankadviseur teleurgesteld.

**Conclusie van de betrokken adviseurs:**
- Er is niks mis met de regels, maar wel met de interne bedrijfscultuur bij veel instellingen en bij de toezichthouder.
- Waar angst regeert worden de regels heilig verklaard, waar betrokkenheid regeert worden de regels met wijsheid toegepast.

# Terms and conditions may apply

Roderick Noordhoek


**Hoewel al twee jaar oud, is de documentaire 'Terms and conditions may apply' nog steeds actueel. Wie meer te weten wil komen over de gevolgen van privacybeleid bij ondernemingen en privacywetgeving vanuit de overheiddie raad ik van harte aan deze film eens te bekijken**

De documentaire start aan het begin van een nieuw privacytijdperk; het tijdperk na de inwerkingtreding van de USA Patriot Act (inmiddels vervangen door de Freedom Act). Deze wet zorgde ervoor dat de Amerikaanse overheid alle data van vermeende terroristen kan monitoren. Belangrijk hierbij is dat monitoren van data alleen is toegestaan wanneer er sprake is van 'vermeende terroristen' en dat dit bedoeld is ter voorkoming van aanslagen. Althans, dat was de opzet.

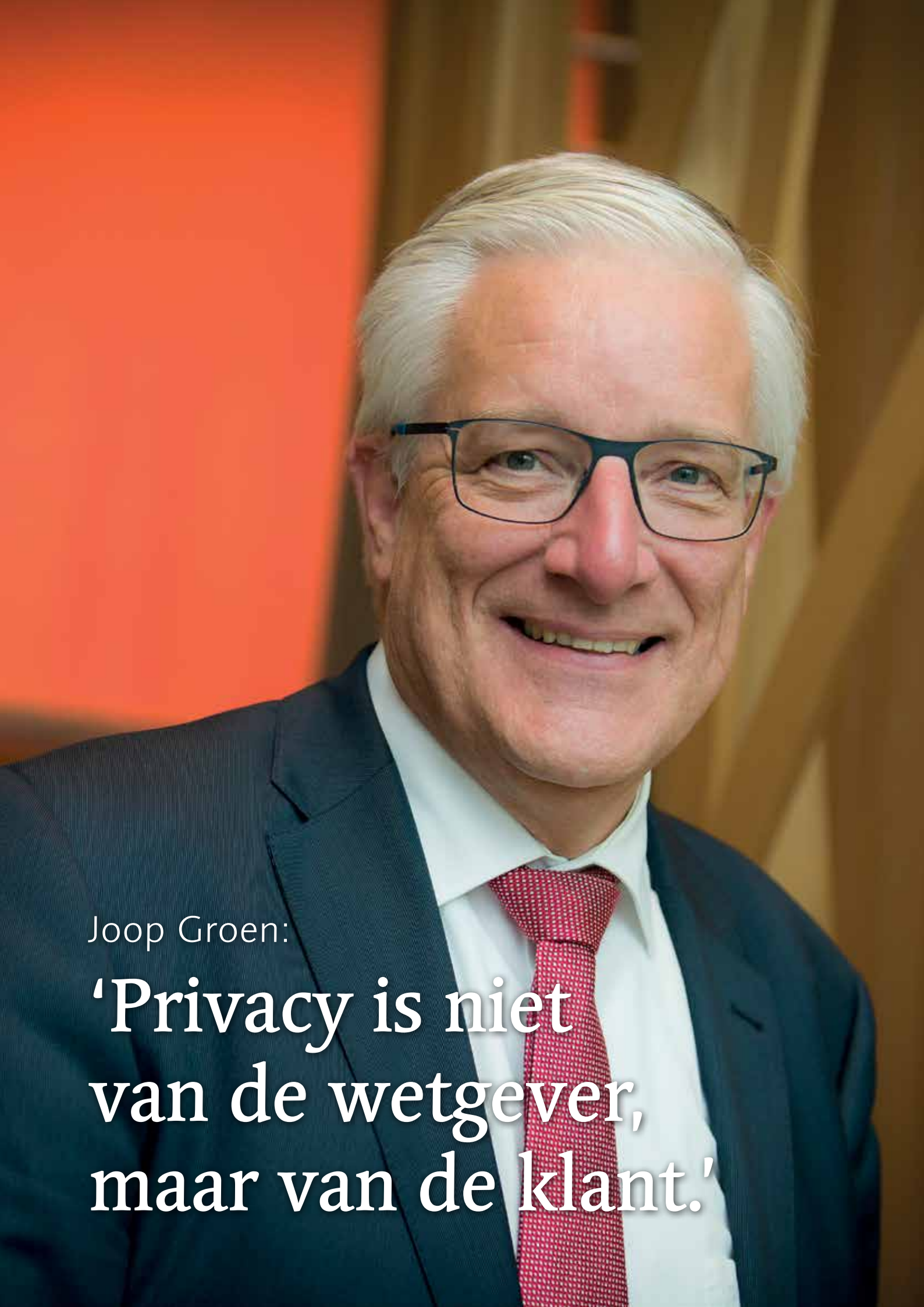
Volgens de documentaire creëerde de USA Patriot Act ook een bijeffect. Het opende de deuren voor ondernemingen om steeds meer persoonlijke data vast te leggen en om deze voor lange tijd te bewaren. In eerste instantie ter voorkoming van terrorisme, maar in tweede instantie als geheel nieuw verdienmodel.

Ondernemingen gingen deze informatie namelijk gebruiken voor gerichte advertenties. Zo wist een grote supermarktketen bijvoorbeeld eerder dat een tienermeisje zwanger was dan haar eigen vader. Dit bleek uit haar zoekgedrag op de website, waarna het thuiswonende meisje persoonsgerichte advertenties kreeg thuisgestuurd voor luiers en babykleding.

Een tweede bijeffect is de verkoop van deze data aan derden. Het accepteren van een online-privacybeleid werd een standaard handeling; men ging klakkeloos akkoord met de privacyvoorwaarden, zonder de lappen tekst gelezen te hebben. Dit gaf ondernemingen de ruimte om in hun privacybeleid op te nemen dat opgeslagen data eigendom werd van de onderneming en mocht worden doorverkocht aan derden. En zelfs wanneer gegevens expliciet werden beschermd tegen verkoop aan derden bleek doorverkoop toch mogelijk, bijvoorbeeld in het geval van een faillissement. De gevolgen hiervan worden blootgelegd in de documentaire.

Met de recente aanslagen in Parijs en de verhoogde dreiging van terrorisme in verschillende Europese landen zullen overheden – net als de Verenigde Staten – steeds meer toegang willen tot data die ondernemingen opslaan. Het implementeren van een Europese wet die vergelijkbaar is aan de USA Patriot Act, als reactie op de dreiging van terreur in Europa, is niet ondenkbaar en wellicht wenselijk. Natuurlijk zien wij allemaal graag dat terroristische aanslagen worden voorkomen en het gebruik van data is daarbij een zeer belangrijk instrument. Het is echter belangrijk om een lijn te trekken tussen het gebruik van data voor deze doeleinden, en de manier waarop ondernemingen het gebruiken om een digitaal profiel van ons te schetsen, hier een persoonlijkheid aan te verbinden en zonder dat wij het merken hierdoor onze keuzevrijheid beperken. Een gevoelige, maar zeer waardevolle lijn.

Terms and conditions may apply legt deze lijn goed bloot en geeft ons te denken of wij echt niets te verbergen hebben. En misschien nog wel belangrijker: of wij willen dat ondernemingen een online profiel creëren dat wellicht is gebaseerd op onvolledige data, zonder context, omgezet in onjuiste informatie.



Joop Groen:

# ‘Privacy is niet van de wetgever, maar van de klant.'

Toen Friesland Bank werd geïntegreerd in de Rabobank werd *Joop Groen* – toen nog chief information security officer bij Friesland Bank – de functie van group chief privacy officer aangeboden. Een mooie uitdaging voor Joop, die omwille van zijn nieuwe functie in de leer ging aan de Tilburg Law School om alles te weten te komen over privacyrecht en de Wbp. Sharon Karsten praat met Joop Groen over zijn functie, over uitdagingen en dilemma's, met als rode draad: privacy.

**Wat houdt de functie group chief privacy officer precies in?** "Kort gezegd houd ik toezicht op de naleving van de privacyregelgeving voor de groepsonderdelen. Niet alleen op Rabobank binnen Nederland, maar ook op alle entiteiten buiten Nederland en de dochterondernemingen Obvion, De Lage Landen en Rabo Vastgoedgroep. Binnen die entiteiten zijn compliance officers werkzaam die de rol van privacy officer vervullen. Privacy is een thema dat prima past binnen compliance. Desondanks is de Wet bescherming persoonsgegevens (Wbp) – in verhouding tot de andere twee pijlers van compliance, de Wet op het financieel toezicht (Wft) en de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) – anders. De Wft en de Wwft focussen op integer handelen en de zorgplicht. De Wbp ziet meer toe op het juist en proportioneel gebruiken van persoonsgegevens. De Wft/Wwft en de Wbp staan dan soms ook op gespannen voet met elkaar: waar ligt bijvoorbeeld de grens tussen CDD en privacy? In het bedrijf houd ik hier toezicht op, op basis van functionele rapportagelijnen en op allerlei geledingen binnen het bedrijf."

**Heeft de nieuwe privacy verordening veel veranderingen teweeg gebracht?** "Ja. In Europa hebben we de regel dat persoonsgegevens niet buiten de landsgrenzen mogen worden uitgevoerd, mits het land waaraan je de gegevens wilt verstrekken, voldoet aan de eisen van Europese Commissie. Zoals de eis dat het betreffende land voldoet aan adequate gegevensbeveiliging. De Rabobank opereert over de hele wereld en daardoor hebben we te maken met adequate en niet-adequate landen. Dat zou betekenen dat voor elke 'cross border transfer' een apart contract zou moeten worden afgesloten. Dat is onbegonnen werk. Daar heeft de Europese Unie een oplossing voor bedacht, de 'binding corporate rules (BCR's)' als groepsbreed beleid voor de bescherming van persoonsgegevens. Het Rabobank-beleid geeft ruimte om binnen de groep gegevens uit te wisselen, ongeacht of de entiteit zich nu in een adequaat of in een niet-adequaat land bevindt. In 2011 zijn we gestart met het opstellen van de Rabobank BCR's. In 2014 zijn ze bindend verklaard voor de hele Rabobank-groep en zijn we gestart met de implementatie. In het implementatieprogramma kijken we al met een scheef oog naar de nieuwe Europese Verordening om zoveel mogelijk aspecten in de huidige implementatie van de BCR's mee te nemen."

**Hoe is deze implementatie wereldwijd verlopen?** "De BCR's zijn vastgelegd in twee privacycodes: een voor het klantdomein en een voor het medewerkerdomein. Wereldwijd hebben onze entiteiten een self assessment uitgevoerd tegen deze privacycodes. Op basis van deze self assessment heeft elk onderdeel een implementatieplan opgesteld om aan de eisen van de privacycodes te voldoen. Elk land is daarbij gefaciliteerd met een juridische analyse van de verschillen tussen de lokale regelgeving en de BCR's. De beleidslijn binnen het bedrijf is: 'Rabo-law prevails'. Als de lokale wet minder streng is dan de Rabo-wet dan volg je de Rabo-wet. Als de lokale wet strenger is, dan volg je de Rabo-wet én de lokale regels. Per land zijn deze verschillen vastgelegd in een 'local addendum' op de privacycodes. Deze aanvullingen op de privacycodes actualiseren we in principe eens per jaar. We houden niet alleen lokaal, maar ook centraal de wereldwijde wet- en regelgeving in de gaten. Vanuit de centrale organisatie attenderen we lokale entiteiten op tussentijdse wijzigingen met betrekking op het addendum, en vragen we terugkoppeling over de implementatie van deze wijzigingen binnen de lokale organisatie."

**Waarom is privacy een taak van de compliance officer en is er niet gekozen voor een aparte privacy officer?** "De keuze om er geen aparte functie van te maken is begonnen met het vraagstuk of privacy

## Bescherming van de persoonlijke levenssfeer begint met respect

onderdeel moest gaan uitmaken van IT-security of van compliance. Privacy is meer dan IT-security maar kan daar niet zonder. Er was al een sterke compliancefunctie aanwezig aan de business-zijde en is het een logische keuze om privacy daar onderdeel van uit te laten maken."

**Wat maakt jouw werk interessant?** "Geen dag is hetzelfde en geen casus gelijk. Bij privacy gaat het steeds meer over de ethische vraag erachter; over het wel of niet verzamelen en hergebruiken van data. In principe gebruiken we data alleen voor het doel waarvoor we het hebben gekregen, maar die doelvraag is erg breed. De onbalans tussen enerzijds de Wft/Wwft en de Wbp anderzijds zorgt regelmatig voor dilemma's. Dergelijke dilemma's belanden op mijn bureau, en geen een is hetzelfde. Dat maakt het boeiend."

**Waar komen privacydilemma's vandaan, hoe gaan jullie ermee om?** "Dilemma's komen uit de hele compliance-organisatie. Zowel aan de voorkant waar de klantinteractie plaatsvindt als op terreinen van innovatie en marketing. We proberen generieke antwoorden te geven op verschillende privacycasussen, maar ik merk vanuit de praktijk dat iedere casus dusdanig specifiek is dat er vaak geen generiek antwoord te geven is. Het is daarom belangrijk veel tijd en energie te steken in bewustwording en de medewerkers te leren welke afwegingen er moeten worden gemaakt. In Europa is de bescherming van de persoonlijke levenssfeer een basisrecht. Dan moeten we niet beginnen met de vraag 'Voldoen we aan de wet?', maar moeten we onszelf de vraag stellen 'Voldoen we aan het standaard-beginsel dat de klant in alles wat wij doen beschermd wordt in zijn persoonlijke levenssfeer?' Als je vanuit die invalshoek de casuïstiek bekijkt, dan is het vinden van een antwoord aan de ene kant makkelijk omdat je de klant centraal stelt, maar aan de andere kant zorgt het ook voor dilemma's. Want wat gaat er nu voor? Commercie, zorgplicht, ethiek?"

**Wat prevaleert, ethiek of wetgeving?** "Ik ben geneigd te zeggen ethiek. Als voorbeeld neem ik de meldplicht datalekken. Instellingen die niet onder financieel toezicht vallen, hoeven de klant niet te informeren als er een datalek is geweest. Het is de vraag in hoeverre dat transparant is. Ik adviseer altijd om in zo'n situatie eerlijk het gesprek met de klant aan te gaan. Leg uit wat er mis is gegaan en bied je verontschuldigingen aan. Dat is beter dan te redeneren: 'het staat niet in de wet , dus ik hoef het niet te doen.' De Rabobank is een coöperatieve bank die zich profileert als een bank die zich anders gedraagt dan andere banken. Dat moeten we op alle vlakken laten zien. Transparant zijn over wat er fout is gegaan, maar ook over wat we met de klantgegevens doen. In al je doen en handelen laten zien dat je echt om de klant geeft."

**De Rabobank neemt vier kernwaarden als uitgangspunt: respect, integriteit, professionaliteit en duurzaamheid. Hoe verhouden de kernwaarden zich tot het onderwerp privacy?** "Die matchen daar volledig mee. Als het gaat om de bescherming van de persoonlijke levenssfeer van de klant of medewerker, dan begint dat met respect. Integer zijn – zeggen wat je doet en doen wat je zegt – transparant zijn, professioneel handelen; het zijn ook de kernwaarden als het gaat om privacy."

**En duurzaamheid? Die ontbreekt nog in het rijtje.** "Duurzaamheid betekent ook nemen van verantwoordelijkheid. Verantwoordelijkheid nemen houdt ook in transparant zijn in hetgeen je doet met de persoonsgegevens van klanten en waar nodig de klant betrekken in de keuze om persoonsgegevens verder te verwerken."

**Tegen welke privacy obstakels lopen jullie aan?** "Het belangrijkste obstakel is de soms schijnbare disbalans tussen de primaire wetten die gelden voor een bancaire instelling. In Nederland is dat de disbalans tussen de Wft/Wwft en de Wbp; die spreken elkaar op sommige punten tegen. Maar ook in Europa en daarbuiten gelden soms per land verschillende regels. Onze medewerkers moeten dagelijks afwegen welke eis prevaleert en dat zijn moeilijke dilemma's.
Een ander obstakel is de relatief zware administratieve last om privacycompliant te zijn. Je merkt dat, daar waar we juist proberen over te stappen van rule-based naar principle-based, de Europese privacywetgever daar geen boodschap aan heeft. Die stopt ons weer terug in het keurslijf van regels en administratieve last."

**Waar ligt de grootste uitdaging?** "Ik denk dat de grootste uitdaging ligt in het gebruiken van klantgegevens in nieuwe business. We hebben heel veel data tot onze beschikking. Deze data kun je met nieuwe technieken, zoals Advanced Data Analytics, gebruiken om je processen te verbeteren, beter risicobeheer te voeren, de klant beter te bedienen, maar ook om nieuwe producten te ontwikkelen. Ik denk écht dat daar de grootste uitdaging ligt; ervoor

zorgen dat de nieuwe businessmodellen, die zullen zijn gebaseerd op innovatie en data, privacycompliant zijn en blijven én zorgen dat ze in het belang van de klant zijn."

**Wordt big data onderdeel van het nieuwe business-model?** "Ik denk het wel. Je kunt al heel veel bankzaken online regelen. Die online, virtuele wereld: zo gaat de bank van de toekomst er ook uitzien. Hoe kunnen we er nu voor zorgen dat je toch nog bij onze bank blijft komen, ook online? We zullen het voor jou interessant moeten maken en dat kan door het inzetten van beschikbare data. Waarbij het ene uiterste is dat wij beslissen wat goed voor je is en waarbij het andere uiterste is dat jij zelf beslist wat goed voor je is. In het midden ligt een soort gezamenlijk model. Een model waarin wij transparant zijn in wat we hebben, wat we willen en wat we kunnen, en waarin jij als klant kunt zeggen of je dat wilt of niet."

**De bank kan hierbij een proactieve houding aannemen en de klant heel gerichte voorstellen doen, maar komt de privacy dan niet in het geding?** "De innovatie en marketing-afdelingen van de bank zijn inderdaad dagelijks bezig om te kijken welke technologie en andere werkwijze we kunnen inzetten om de klant beter te bedienen. Vanuit privacy moet je zorgen dat je heel alert blijft op allerlei innovatieve ideeën die hier bedacht worden. Het is de kunst om vanaf het eerste moment dat het idee ontstaat, al aan te haken en het gesprek aan te gaan. We

> De grootste uitdaging: het gebruiken van klantgegevens in nieuwe business

hebben bijvoorbeeld binnen de bank een business data committee, waarin de vragen of ideeën die binnen de bank ontstaan en met klantdata van doen hebben, worden besproken. Mijn rol binnen het committee is om te luisteren naar alle belanghebbenden en om – met oog voor alle belangen – een afweging te maken of iets wel of niet verantwoord is v.w.b. privacy. Ik ben als chief privacy officer onafhankelijk en kan gevraagd en ongevraagd adviseren en escaleren. Ik kan dus altijd zeggen: 'We doen iets waarvan ik vind dat het niet of anders zou moeten.' Maar het beste is om vroegtijdig met de mensen in gesprek te gaan en te blijven, en hen te wijzen op de privacyrisico's en de alternatieven."

**Wat betekent privacy voor jou persoonlijk?** "Eigenlijk niets anders dan datgene wat ik dagelijks belijd over hoe wij met onze klanten omgaan. Mijn privacy is ook mij zeer heilig. Het is voor mij als mens belangrijk, maar tegelijkertijd vind ik het 'mens zijn' ook belangrijk. Daar bedoel ik mee dat ik sommige persoonlijke dingen echt wel deel met mensen, maar dat ik dat wel heel bewust doe. Net als onze klanten wil ik ook beschermd worden in mijn eigen persoonlijke levenssfeer. Ik ben als Joop Groen, als group chief privacy officer of als wie dan ook, niet anders. Privacy – en dus hoe je omgaat met de persoonlijke levenssfeer van iemand anders – maakt wat mij betreft deel uit van iemands integriteit."

**Maar de definitie van integriteit is niet voor iedereen gelijk.** "In de essentie is integriteit voor iedereen hetzelfde. Omdat de basisingrediënten 'respectvol met elkaar omgaan' en 'transparant zijn' zijn."

**Juist die basisingrediënten zijn toch niet voor iedereen hetzelfde?** "Maar komt dat niet voort uit het feit dat mensen hun eigen regels bedenken? Ik krijg regelmatig de vraag of iets wel of niet mag van 'privacy'. Dan stel ik standaard de tegenvragen: 'Wie is 'privacy'? Ben ik dat? Of is dat de klant of je collega?' Ik houd ze een spiegel voor, vraag ze om zich te verplaatsen in de klant of collega. En stel ze de vraag: 'Wat denk je zelf?' Het antwoord volgt dan al snel. Ik herken wel wat je zegt hoor, ieder heeft zijn eigen integriteit. Alleen wordt ernaar gekeken als: integriteit is van 'compliance', compliance is van 'compliance' en privacy is van 'privacy'. Terwijl het allemaal in jezelf zou moeten zitten en vanuit jezelf zou moeten komen. We zijn in een maatschappij terecht gekomen waarin we dat min of meer zijn kwijtgeraakt."

**Hoe kunnen we die intrinsieke motivatie dan weer terugbrengen?** "Transparantie, transparantie, transparantie. Laten zien waar je voor staat. Laten zien wat je doet. Op elk niveau in de organisatie. Als het over integriteit gaat, laat zien dat rangen en standen geen rol meer spelen. Dat je altijd mag laten horen wat jouw waarden en normen zijn. Dat is voor mij een ideaalbeeld. Zo zou de wereld eruit moeten zien."

**Tot slot: welk advies zou je aan de compliance officer meegeven?** "Privacy is niet van gisteren, privacy is van morgen. Privacy is ook niet van de wetgever maar van de klant. Wees voorbereid op wat de maatschappij of de burger morgen van je vraagt."

**Chances never build to last**
**I better run**
**and chase**
**And I will find more**
*Songtekst HEAVN –*
*Finding out more*

## Bart, bedankt voor alles. We wensen jou en je gezin veel succes en geluk toe in Nieuw Zeeland!

Albert, Arjan, Bernadette, Cora, Danieke, Diana, Diane, Geert, Hanne, Jordi, Lisan, Marit, Martin, Musa, Roderick, Ruud, Sharon, Susan.

# Compliance opleiding: Themamiddag Breaking Corporate Silence

**In samenwerking met de Nyenrode Business Universiteit organiseren wij de themamiddag 'Breaking Corporate Silence' voor complianceprofessionals, HR-professionals, toezichthouders en bestuurders die formele en informele communicatieprocessen willen waarnemen en die ervoor willen zorgen dat transparantie en eerlijkheid worden gewaarborgd in hun organisatie.**

Het programma bestaat uit twee dagdelen waarvan het tweede dagdeel optioneel is.

Tijdens het eerste dagdeel leert u 'corporate silence' te definiëren en in de organisationele context te plaatsen, wordt u geïnspireerd door praktijkvoorbeelden van een tegenspreker en het adviespunt klokkenluiders. De middag wordt vervolgens afgesloten met een discussie over de praktijk en de rol van compliance.

Het tweede dagdeel zorgt voor verdieping op de thema's van de eerste middag.

Datum eerste dagdeel: 22 maart 2016
Datum van de tweede dagdeel: 7 april 2016

*Voor meer informatie kunt u terecht bij Roderick Noordhoek via noordhoek@compliance-instituut.nl of via ons telefoonnummer 088 - 99 88 100.*

*Wilt u zich inschrijven voor deze themamiddag? Dat kan via onze website www.compliance-instituut.nl*

| | |
|---|---|
| **5 januari** | LCP Competentietraining |
| **6,7 januari** | LCP Module 2 - groep 1 |
| **12 januari** | LCP Module 4 - groep 5 (dag 1) |
| **13, 14 januari** | LCP Module 2, extra groep |
| **14 januari** | Masterclass Soft Controls (dag 3) |
| **26 januari** | LCT Module 4 |
| **26, 27 en 28 januari** | LCP Module 3 - groep 1 |
| | |
| **1, 2, 3 februari** | LCP Module 3, extra groep |
| **9 februari** | LCP Competentietraining - groep 1 |
| **9 februari** | LCP Module 4 - groep 5 (dag 2) |
| **16, 17 februari** | LCT Module 5 |
| **17 februari** | LCP Module 4 - groep 1 (dag 1) |
| **17, 18 februari** | LCP Module 5 - groep 5 |
| | |
| **1 maart** | Introductie Compliance |
| **1 maart** | Masterclass Soft Controls (dag 1) |
| **3 maart** | Compliance & integriteit woningcorporaties |
| **10 maart** | Toezichtsrecht niet-juristen |
| **15, 16 maart** | LCT Module 2 |
| **16, 17 maart** | LCP Module 2 - groep 2 |
| **24 maart** | LBW Module 2 |
| **29, 30 maart** | LCT Module 3 |
| **31 maart** | LBW Module 3 |
| **31 maart** | LCOZ Module 1 |
| | |
| **5 april** | LCT Module 4 |
| **5 april** | LCP Module 4 - groep 1 (dag 2) |
| **5 april** | Masterclass Soft Controls (dag 2) |
| **7 april** | LCOZ Module 2 |
| **7 april** | Themamiddag Breaking Corporate Silence - verdiepingsdagdeel |
| **12 april** | LCOZ Module 3 |
| **12 april** | Opleiding Privacy Officer |
| **12, 13 april** | LCT Module 5 |
| **14 april** | LBW Module 4 |
| **19, 20 april** | LCP Module 5 - groep 1 |
| **19, 20, 21 april** | LCP Module 3 - groep 2 |
| **21 april** | LCOZ Module 4 |

LBW: Leergang Bestrijding witwassen & terrorismefinanciering
LCC: Leergang Corporate Compliance
LCO: Leergang Compliance Officer
LCOZ: Leergang Compliance Officer in de Zorg
LCP: Leergang Compliance Professional
LCT: Leergang Compliance Trust

# Wij wensen u een goed 2016 toe

Nederlands compliance Instituut

Leading in compliance