de Compliance Officer
nummer 24, december 2016

Interview: Don Ginsel
Het is tijd voor een ander paradigma

Compliancethema
Zakelijk gebruik van WhatsApp

FINTECH

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: Cor Jan Dasselaar, Hans Kooij, Ruud van der Mast, Joost Montens, Roderick Noordhoek, Björn Schuitemaker, Jan Willem Taams, Arno Voerman, Cora Wielenga.
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 3.200 exemplaren
ISSN 1878-7991

www.complianceofficer.nl

Inhoud

FinTech-dromen

Ondanks onze intentie om u altijd de laatste stand van zaken mee te geven in ons tijdschrift, durf ik daar zeker met dit thema niets over te beloven. Met FinTech als thema is het haast ondoenlijk om volledig up-to-date te zijn. De ontwikkelingen gaan zo snel dat je maar even met je ogen hoeft te knipperen en er alweer nieuwe ontwikkelingen zijn. Dat heeft ons er niet van weerhouden om toch een themanummer te maken met FinTech in de hoofdrol. We vinden het belangrijk, omdat we denken dat FinTech een onderwerp is om als compliance officers goed bij stil te staan. We doelen dan overigens niet alleen op de hippe start-ups in de financiële sector, maar op alle technische innovatie in de financiële sector. Dus ook de technische innovatie bij de financiële organisaties die al meer dan honderd jaar bestaan scharen wij onder FinTech.

Voor compliance officers is FinTech zowel een droom als een nachtmerrie. Een droom vanwege de vele mogelijkheden die het biedt om organisaties te helpen om integriteit en compliance beter te waarborgen. FinTech kan een nachtmerrie worden op compliancegebied wanneer we ons niet voldoende verdiepen in alle (on)mogelijkheden.

Om als compliance officer te kunnen profiteren van de 'FinTech-droom' en je organisatie te behoeden voor de 'FinTech-nachtmerrie', moet je als compliance officer weten wat er speelt op het terrein van FinTech. Een belangrijke les die ik zelf op het gebied van FinTech heb geleerd, is dat de ontwikkelingen zo snel gaan, dat het niet voldoende is om alleen naar de huidige situatie te kijken; de aanstaande innovaties moet je net zozeer meenemen in je (compliance)plannen.

Ik geloof dat als je als compliance officer goed wilt reageren op FinTech – of beter nog, daarop wilt anticiperen – dat je ook moet innoveren. Experimenteren met en door compliance. Dat klinkt voor u wellicht als 'contradictio in terminis'. Menig compliance officer is zeer waarschijnlijk voorzichtig van aard. Experimenteren klinkt als gevaarlijk en daardoor haast als een tegenstelling voor compliance. Het goed omgaan met FinTech als compliance officer vraagt wat mij betreft om een experimentele aanpak. Wij zijn daarom in navolging van de Engelse en Nederlandse toezichthouder gestart met een 'sandbox'. Waar de toezichthouders een sandbox begonnen zijn om te experimenteren met FinTech-oplossingen in een verlicht vergunningsregime, richten wij ons op de innovatie van het compliancevak ten aanzien van FinTech in de sandbox. We gaan daarbij onderzoekend te werk. Hoe kunnen we gebruik maken van de 'FinTech-droom'. Hoe kunnen we de 'FinTech-nachtmerrie' voorkomen?

Hoe zal het met de FinTech-ontwikkelingen gaan? Vanzelfsprekend weten we dat niet. Wat we wel weten is dat mensen de neiging hebben om de ontwikkelingen op korte termijn te overschatten en op langere termijn te onderschatten. Dus over een jaar of vijf zijn wellicht een deel van onze FinTech-dromen waar geworden en over vijftien jaar kunnen we ons niet meer voorstellen wat voor gedachtes we in 2016 nog over FinTech hadden. Onze huidige scenario's verbleken dan bij de realiteit van 2025.

Dit tijdschrift is dan wellicht vandaag of morgen niet meer actueel, maar biedt een mooie start om als compliance officer kennis te maken met de (on)mogelijkheden van FinTech. En daarnaast kan dit een mooi bewaarexemplaar worden. Het is wellicht amusant om in 2026 onze in 2016 bedachte scenario's terug te lezen. Ik denk daarbij aan het bekende filmpje van Hans Bromet over het gebruik van mobiele telefoons in 1999: de geïnterviewden konden zich allemaal het nut van een mobieltje niet voorstellen. Dit leidde tot prachtige quotes zoals *"Ik heb een gewone telefoon, waarvoor moet ik een mobiel hebben?"* en *"Ik heb al een antwoordapparaat, thuis ben ik altijd al bereikbaar"*. Wat een tegenstelling met hoe we nu onze telefoons beleven.

Ik wens u voor 2017 mooie 'FinTech-dromen' toe.
Cora Wielenga

Don Ginsel:

‘Het is tijd voor een ander paradigma.’

Op de Zuidas, te midden van de gevestigde (financiële) orde, spreekt Roderick Noordhoek met *Don Ginsel,* oprichter van Holland FinTech. Don staat inmiddels bekend als hét aanspreekpunt voor start-ups, wetgevers en toezichthouders waar het gaat over FinTech in Nederland en daarbuiten. Ook de bestaande financiële partijen zitten graag met Don aan tafel. Op de website staat te lezen wat Holland FinTech doet: het koppelen van inzichten, ondernemingskansen, technologie, kapitaal, regulering en talent. Het forum van Ginsel en consorten heeft inmiddels meer dan 250 leden. Don ontwikkelde zijn fascinatie voor FinTech door het samenvoegen van zijn eerdere ervaringen. Hij studeerde civiele techniek, werkte bij de ABN Amro en investeerde vanuit een venture capital-onderneming in CleanTech (duurzame, technologische oplossingen).

Hoe is Holland FinTech ontstaan? "Toen ik bezig was mijn verschillende achtergronden van finance, business en technologie aan elkaar te koppelen, zag ik de FinTech-trend aankomen vanuit de US en de UK. Met een plan in de hand om ook in Europa een platform voor FinTech te creëren, sloten IBM, Van Doorne, Innopay en KPMG zich snel bij ons aan.

Vervolgens zijn we gaan kijken hoe we het platform het beste konden vormgeven. We wilden direct het hele 'ecosysteem' een boost geven; ons niet beperken tot de activiteiten van een 'business incubator' of 'accelerator', maar wel die elementen erin verwerken (ter verduidelijking: een business incubator biedt een start-up een geïntegreerd pakket aan diensten, met als doel het bedrijf snel te kunnen laten groeien). Uiteindelijk is dus besloten een organisatie op te zetten met als uitgangspunt dat iedereen zich hier welkom voelt, maar wel onafhankelijk is. Onze taak is om deelnemende partijen met elkaar in contact te brengen en voor hen te kijken wat er op FinTech-gebied gebeurt in de wereld."

Hoe weet je dat je kijkt naar blijvende ontwikkelingen? De levensvatbaarheid van veel start-ups of ontstane netwerken zijn niet altijd even groot. "We hebben ervoor gekozen om daar geen oordeel over te vellen. We investeren ook niet in de aangesloten partijen. Daarnaast is de levensvatbaarheid ook heel lastig te voorspellen. Met behulp van één grote klant kan een start-up opeens een succesverhaal zijn, zonder dat je dat zag aankomen. Vaak zie je dat er bij twijfel niet wordt geïnvesteerd. Valt de start-up vervolgens om, dan zegt bijvoorbeeld een bank: 'Toch maar goed dat we dat niet gedaan hebben.' Maar eigenlijk werkt het andersom; met die investering had het juist een succes kunnen worden. Het idee van 'opportunity costs' moet door investeerders ook goed worden begrepen. We helpen de deelnemers door het voorleggen van mogelijke oplossingen. Hoe er vervolgens wordt samengewerkt, daar proberen we niet in te sturen.

Daarbij hebben we ook te maken met 'hypes'. Een hype is moeilijk te vertalen naar de reële waarde van een technologische ontwikkeling. Het is niets anders dan de perceptie van mensen. Veel belangrijker hierbij is de onderliggende 'waarheid'; daarin zien we dat innovatie van alle tijden is. FinTech, als het gebruik van technologie in financiele diensten, is dan ook niet nieuw, maar zit qua ontwikkeling in een stroomversnelling. Momenteel speelt de vraag of bijvoorbeeld de hype blockchain kan voldoen aan alle verwachtingen. Het kan nog best lang duren voordat die technologie alledaagse oplossingen levert. Als de hype straks over is, betekent dat niet dat blockchain waardeloos is geworden. Daarom is het beter om je

> Onze taak is om deelnemende partijen met elkaar in contact te brengen en voor hen te kijken wat er op FinTech-gebied gebeurt in de wereld

oog te houden op toepasbare oplossingen. Als experts zeggen dat iets potentie heeft, dan blijven wij de ontwikkeling volgen."

Er wordt weleens gesteld dat veel FinTech-ontwikkelingen oude wijn in nieuwe zakken is. Is er dan wel sprake van innovatie? "Wat innovatie betreft hebben wij een brede definitie. Elke verbetering die ontstaat door het koppelen van iemand met een probleem aan iemand met een (technologische)oplossing is een innovatie. Verbeteringen binnen de bestaande processen in de financiële sector zijn niet altijd zichtbaar; het zijn geïntegreerde oplossingen. Hierdoor lijkt er – onterecht – niet veel te veranderen. Tegelijkertijd zijn er ook partijen die als zeer innovatief worden gezien, omdat hun oplossing jaren voor de markt uit loopt. Dat zijn de oplossingen die moeilijk marktaandeel kunnen veroveren, omdat de voorkeur vaak uitgaat naar bewezen technologieën die nu veel aandacht krijgen."

Het gaat er bij innovatie toch uiteindelijk om dat de transactiekosten worden verlaagd? "Ja, maar dat moet wel in de brede zin van het woord worden uitgelegd. Zo zie je dat bij betaalinstellingen niet veel meer valt te reduceren op de transactiekosten. Tegelijkertijd wordt er wel veel geïnnoveerd door deze instellingen. Dit heeft te maken met gebruikersgemak, wat je ook kunt zien als transactiekosten: hoeveel knoppen moet ik indrukken voordat mijn transactie is verricht?"

DNB komt voor de toekomst van de financiële sector met drie scenario's 1. de disruptie van start-ups; 2. de overname van start-ups door bestaande partijen; en 3. het toetreden van grote tech-bedrijven als Google en Facebook (BigTech's). Wat zie jij als meest aannemelijk scenario? "Volgens mij moet je ze niet los van elkaar zien. Alle scenario's vinden al in meer of mindere mate plaats. Bekijk ze als kenmerken van de totale markt, waarbij wellicht één scenario dominant kan worden. Je ziet voor derde partijen dat het steeds makkelijker wordt om toe te treden in de financiële value chain, zowel aan de voorkant als aan de achterkant. Als je kijkt naar PSD2 (nieuwe payments-wetgeving vanuit Europa, geldig vanaf 2018) zie je dat start-ups en BigTech's aan een gereguleerde partij gaan 'hangen'. Dat komt doordat banken toegang moeten geven tot accountinformatie en 'payment initiation'. Daarbij kunnen derde partijen betalingen verrichten zonder dat zij gereguleerd zijn als bank, maar onder een lichter regime vallen. Een al bestaand voorbeeld is Apple Pay, waarbij Apple meevaart op de vergunning van de creditcardmaatschappij en zo data verzamelt waarmee zij meer mogen dan die gereguleerde bank."

Hoe kunnen we een stap maken om die scenario's te laten werken? "Het is tijd voor een ander paradigma. Vanaf mijn studie heb ik altijd het idee gehad dat je een landschap kan creëren zoals je het wilt hebben. Dat is heeft mijn 'natuurlijke en menselijke kijk' op de wereld gevormd. Wat mij bij elke organisatie met meer dan pakweg honderd man fascineert, is hoe zo'n onderneming 'in control' kan zijn, ook richting haar stakeholders. Hoe weet de bestuurder nou dat hij/zij in control is over alles wat er gebeurt? Als je het mij vraagt kan dat niet en dit werd door de crisis ook niet ontkracht. Tot op heden ben ik er ook niet van overtuigd dat de traditionele bedrijfsmodellen hier toe in staat zijn."

Wat is dan het nieuwe paradigma? "Ik ben overtuigd van het holacracy-model. Dit model veronderstelt dat elk individu zijn eigen mandaat houdt om te doen wat voor hem/haar het beste is vanuit de rol die hij of zij heeft. Uiteraard wel met bepaalde grenzen. Elke handeling die een individu verricht, is daarbij volledig autonoom bepaald en dient het hogere doel van het collectief. Hierbij is dus geen toestemming nodig van een leidinggevende, tenzij dat vooraf is bepaald. Het hogere doel hoeft daarbij ook

niet bekend te zijn. Zie het als de organen in een lichaam of de mensen in een stad. Zij werken samen zonder dat ze het weten. Het feit dat wij dit interview nu kunnen houden, wordt door heel veel mensen gefaciliteerd, zonder dat zij dat zelf weten, maar vanuit hun rol leveren zij toegevoegde waarde. Een top-down organisatie vertoont in zo'n geval gebreken. Zodra er een baas moet zijn die dit moet organiseren, krijg je direct het 'in control' probleem."

Past holacracy wel bij de financiële industrie? "Het zal nog wel even duren voordat een dergelijk systeem in de financiële sector wordt ingevoerd. Op dit moment zitten de bestaande spelers vast aan het 'in control'-denken en is dat ook de manier waarop de toezichthouder toezicht houdt. Daar komt bij dat het integriteitrisico niet altijd te ondervangen is met duidelijke regels.

Dat zou zich in dit systeem vanzelf moeten oplossen. Als de spelregels in organisatie duidelijk zijn en dit ervoor zorgt dat er volledige transparantie is, kan iedereen zich eraan houden en elkaar erop wijzen. Dan hoeft het ook niet meer de compliance officer te zijn die toezicht houdt op de naleving van deze regels. Op deze manier kan de business hierin zelf de juiste afwegingen maken. Ze kennen dan de risico's en de winst die aan elk besluit gekoppeld is, én die 'risk and reward' zitten dan ook bij het individu zelf, terwijl deze nu ontkoppeld zijn. Dat is ook een van de boodschappen die Luyendijk in zijn boek meegeeft en kan een oplossing zijn voor het 'agency' probleem (informatie-asymmetrie)."

Wat voor compliancerisico´s zie jij ontstaan door FinTech? "Alle nieuwe partijen die aanhaken op de financiële supply chain staan onder beperkter of soms geen toezicht, terwijl zij soms meer infomatie hebben dan een bank. Ook kunnen zij, door bijvoorbeeld PSD2, handelingen verrichten die normaal gesproken alleen middels goedkeuring van de bank werden verricht. De klant krijg bij PSD2 meer controle en gemak, maar potentieel loop je ook meer risico. Ook is het bijna niet mogelijk om 'in control' te zijn als gereguleerde instelling. Dat is mijns inziens al onmogelijk als je onderneming meer dan honderd fte's heeft, laat staan als je als bank 'in control' moet zijn van de hele supply chain.
De huidige regulering wijst eigenlijk de banken aan als de hoeders van het financiële systeem. Als je nu kijkt naar hoe al die niet-gereguleerde partijen zich vestigen in de supply chain en daarmee ook een deel van de omzet opstrijken, moet je jezelf afvragen of de bank straks nog wel de partij is met de meeste macht. Of is dat de partij die de meeste data heeft…"

Is het wel goed dat er dan een bankvergunning-light is? "Volgens mij is dat dus geen probleem. Sterker nog, het is goed dat nieuwe partijen kunnen toetreden. Daarbij moeten we dus ook niet meer kijken naar de banken als de aangewezen partij om de verantwoordelijkheid te nemen. Alle partijen die in die supply chain zitten zouden eigenlijk onder een vorm van toezicht moeten staan. Alleen dan kan je de stabiliteit in de sector waarborgen. Dat is ook mijn punt met holacracy."

Waarom denk je dat de toezichthouder dan toch vooral naar die bank kijkt? "De toezichthouder maakt graag gebruik van het feit dat banken groot zijn, kapitaal hebben en vooral een reputatie hebben die ze alles waard is. De toezichthouder ontleent met name aan dat laatste veel comfort. Ze kan dreigen met het feit dat zij de reputatie van de bank kan schaden. Die 'stok' ontbreekt bij veel kleinere partijen. Voorheen kwam de toezichthouder daar ook mee weg. Toen transactiedata digitaal beschikbaar werd, is er heel snel een strak regime opgetuigd voor de bescherming ervan. Inmiddels is er veel data digitaal verkrijgbaar, maar de bescherming ervan is belegd bij andere regimes. Als ik al mijn contracten bijvoorbeeld in de cloud zet bij Google, dan zit daar de informatie die wat zegt over de manier waarop ik geld verdien. Alleen de uitkomst hiervan staat op mijn bankrekening. De bescherming van die informatie vind ik tenminste even belangrijk als de bescherming van mijn bankgegevens. Daar wringt de schoen, want wat dat betreft is er geen 'level playing field'. Naarmate de omzet meer en meer wordt uitgesmeerd over de keten, moet je jezelf afvragen of er wel voldoende draagvlak is voor de wijze van toezicht zoals dat nu is opgezet."

Moeten alle toezichthouders dan met elkaar gaan integreren? "Dat hoeft niet per se, maar als je de hele keten van financiële dienstverlening bekijkt: wie heeft welke rol, waar zitten welke risico's en hoe spreken we de juiste partijen op de juiste risico's aan? Nu zie je dat er wordt gezegd: de bank heeft de vergunning, dus die regelt het maar. Dat kan gewoon niet, maar tegelijkertijd denk ik ook niet dat de toezichthouders op dit moment andere

> Als experts zeggen dat iets potentie heeft, dan blijven wij de ontwikkeling volgen

mogelijkheden hebben. Deze moeten ze snel gaan ontwikkelen. Overigens moet er überhaupt meer bewustzijn ontwikkeld worden bij financiële instellingen over het feit dat zij onderdeel zijn van een supply chain. De enige die zich hiervan echt bewust zijn zitten binnen de IT. Zij begrijpen hoe informatiestromen lopen en waar je in de gehele keten toezicht op moet houden."

Wat betekent dit dan voor het toezicht? "Volgens mij gaat het straks veel meer over digitale monitoring. Zorgen dat bepaalde dingen geregeld zijn, is niet alleen maar een handtekening onder een 'in control statement'. Het gaat om het inbouwen van geautomatiseerde checks and balances in de gehele informatiestroom. Overigens is technologie daarbij niet heilig. Het is ook belangrijk dat er mensen bij betrokken zijn die op basis van hun intuïtie kijken naar de uitkomst. De automatisering en intuïtie moet je dan zien als twee parallelle rekenstappen die uiteindelijk weer bij elkaar komen. Intuïtie moet daarbij worden ingebouwd in het systeem en door de hele keten. Het toezicht wordt straks zo ingeregeld dat het gehele proces blootgelegd wordt en dan moet blijken of je als financiële instelling, samen met je ketenpartners, dat proces goed hebt ingeregeld."

Dat inbedden van intuïtie in de processen, hoe zie je dat voor je? "Neem als voorbeeld het robo-advies: een professional moest voorheen al zijn overwegingen vastleggen om zo verslag te kunnen doen van het adviesproces. Straks wordt dit overgenomen door een robot. Dat scheelt veel administratie voor die professional, maar maakt hem niet onnodig. Hij wordt juist veel beter ingezet, omdat hij als mens met zijn intuïtie vooraf een inschatting maakt en kan kijken of het uiteindelijke robo-advies in zijn ogen redelijk is. Je haalt zo veel meer waarde uit die persoon. Daarbij is er voorlopig ook nog steeds behoefte aan intermenselijke contact, wanneer je bijvoorbeeld een krediet gaat aanvragen."

Leuk om te horen; iemand die zich focust op technologie en die een lans breekt voor het gebruiken van intuïtie in de oordeelsvorming als controlemechanisme. "Vergeet niet dat die intuïtie niet menselijk hoeft te zijn. We zien nu dat dit ook te programmeren is. Artificial intelligence (AI) kan ook worden ingezet voor monitoring. Straks is het wellicht mogelijk dat AI het gehele proces monitort; dat het een signaal geeft bij afwijkingen van de parameters die door de mens, met behulp van zijn intuïtie, zijn ingegeven. Dit zorgt er ook voor dat het proces veel transparanter is. Dat geeft dan weer belangrijke informatie voor compliance. Zij kunnen zien of bij elk moment in het proces van besluitvorming voldoende informatie aanwezig was om een integere afweging te kunnen maken en of de spelregels hierbij zijn gevolgd. Je hoeft dan niet meer vanuit het resultaat terug te redeneren. Als dat proces goed is ingeregeld kan je ook de verantwoordelijkheid voor integere besluitvorming terugleggen bij de juiste persoon. Het gevolg is wel dat alles vastgelegd wordt en zichtbaar is. Wanneer de afweging zorgt voor een actie die ethisch gezien in een grijs gebied zit, is dit ook zichtbaar voor de toezichthouder. Het is dus uiterst belangrijk dat als je kiest voor een afwijking op de regels, je dit zo zorgvuldig mogelijk vastlegt. Het lastige hierbij is dat je misschien niet alle context in kaart kan brengen. Daarbij kunnen medewerkers risico avers reageren op zo'n hoge mate van controle. Ik merk ook dat dit nu al geldt voor sommige compliance officers. Zij reageren met over-compliant gedrag."

Hoe ziet de compliance officer er überhaupt uit als wat we besproken hebben praktijk wordt? "De compliance officer moet een combinatie van competenties in huis hebben. Hij moet voldoende kennis hebben van IT en tegelijkertijd ook zijn intuïtie kunnen inzetten vanuit een monitorende rol. Ook moet hij goed met de business kunnen overleggen en hen de informatie kunnen verstrekken die zij nodig hebben bij de risk and reward-afweging. Dat maakt overigens dat je compliance kan meenemen in het totale riskmodel, waarbij de grootste uitdaging is dat ook vanuit compliance de reward gevoed wordt. Je ziet vaak dat bij een risk and reward-afweging de reward kwantitatief gemaakt kan worden, terwijl de risk kwalitatief van aard is. Compliance moet dan als een van de interne stakeholders helpen in het maken van een gelijkwaardige, gebalanceerde afweging middels die rol van informatieverstrekker."

Lang verhaal kort

Compliance officers beschikken over een reeks middelen[1] die medewerkers helpt het belang van hun bedrijf voorop te stellen in hun beslissingen. Hiertoe investeren bedrijven meer en meer in computertoepassingen. Dit betreft veelal computersoftware die uit een hoop data mogelijke overtredingen door medewerkers identificeert. Hieruit volgt een rapportage waarna compliance officers aan de slag gaan om deze mogelijke overtredingen te onderzoeken. Een enkele keer is het daadwerkelijk raak. Zelf herinner ik me voornamelijk veel 'false positives'.

Echter, de laatste ontwikkeling betreft software die niet zozeer achteraf overtredingen identificeert, maar al vooraf aangeeft of een medewerker de fout in lijkt te gaan. Onder het mom: voorkomen is beter dan genezen. Zelf ben ik niet heel bekend met deze 'cognitive computing technologies', maar uit belangstelling volg ik dergelijke berichten op de voet. In de tussentijd begin ik me op een ander terrein te bekwamen, te weten; ouderwetse retorica. Oftewel: de kunst van het verhaal.

Eén van de kenmerken die ik Amerikanen toedicht, is dat zij retorisch hun mannetje staan. Of het gaat om discussie, debat, speech of andere vorm van voordracht; het valt mij op dat Amerikanen op dit vlak sterk uit de hoek komen. Ik herinner me een situatie dat ik tijdens de koffiepauze op een congress tegen mijn Spaanse collega zei: *"Er klopt geen hout van wat die Amerikaan op het podium zojuist vertelde, maar het klonk wél goed"*. Met mijn komst naar de VS had ik me dan ook voorgenomen om me op dit terrein verder te ontwikkelen.

Afgelopen zomer volgde ik daartoe een korte cursus. Recent heb ik de eerste voorzichtige stappen gezet om de theorie in de compliancepraktijk te gebruiken. In plaats van een droge opsomming over regels, startte ik laatst een training door te vertellen hoe de film 'Pretty Woman' en de 9/11-terreuraanslagen ervoor gezorgd hebben dat ik samen met hen in die trainingsruimte terecht ben gekomen.[2] Ik kan je vertellen: het lijkt aan te slaan. Je brengt daarmee meteen een heel andere dynamiek teweeg. In weze is het niets nieuws of opzienbarend. De mens gebruikt de vertelkunst al duizenden jaren om kennis en ervaringen te delen. Ondanks alle moderne technologie blijft vertelkunst een krachtig middel. Ga maar na. Hoe vaak ben je de powerpoint presentatie van zojuist al vergeten, maar kan je de film van twintig jaar geleden nog wel helder voor de geest halen?

Als geen ander verwelkom ik nieuwe technologie, maar laten we niet vergeten dat er ook nog oude technieken bestaan die wij, compliance officers, kunnen gebruiken in ons dagelijks werk.

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 Bij AstraZeneca noemen wij deze de 'Great 8': Organisation & Culture, Risk management, Standard Setting, Training & Communication, Control Activities, Auditing & Monitoring, Investigation & Remediation en Reporting.

2 Deze zin bevat alleen al een reeks aan verteltechnieken zoals focalisatie, thematiek, personages en cliffhanger.

PSD2 - de herziene richtlijn betaaldiensten

Arno Voerman

Eind 2015 is de herziene richtlijn betaaldiensten vastgesteld (PSD2).[1] Deze richtlijn moet uiterlijk 13 januari 2018 in de nationale rechtstelsels van de EU-lidstaten zijn geïmplementeerd. Veelbesproken is de regulering van 'payment initiation' en 'account information services'. Belangrijk is ook dat banken verplicht zijn aanbieders van deze betaaldiensten toegang tot betaalrekeningen te bieden. Er zijn echter ook andere belangrijke wijzigingen.

De PSD

In 2009 is de 'payment services directive (PSD)' in de Wet op het financieel toezicht (Wft) en het Burgerlijk Wetboek (BW) geïmplementeerd. Het verlenen van betaaldiensten is toen een gereguleerde activiteit geworden. Een nieuwe categorie vergunninghouders werd geïntroduceerd, namelijk de betaalinstellingen. Volgens het register van DNB zijn er op dit moment negenendertig Nederlandse betaalinstellingen. Daarnaast zijn er zevenenzeventig Nederlandse betaaldienstverleners op basis van een vrijstelling actief.

De betaaldiensten zijn beschreven in de bijlage bij de PSD. Het gaat daarbij onder meer om het aanbieden van betaalrekeningen, het uitvoeren van betaalopdrachten en geldtransfers. Wanneer in de uitoefening van een beroep of bedrijf betaaldiensten worden verleend, is in beginsel een vergunning als betaalinstelling vereist. Er zijn echter uitzonderingen. Zo hebben banken geen aparte vergunning als betaalinstelling nodig. Ook bepaalde vormen van dienstverlening zijn uitgezonderd. Het gaat dan bijvoorbeeld om ondernemingen die technische diensten aan banken en/of betaalinstellingen verlenen. Voorwaarde is dan wel dat zij op geen enkel moment in het bezit komen van of controle hebben over cliëntgelden.

De PSD voorziet verder in eisen voor de informatie die betaaldienstverleners aan hun cliënten moeten verschaffen. Ook bevat het regels met betrekking tot de rechten en plichten van gebruikers van betaaldiensten.

Aanleiding voor herziening PSD

Sinds de totstandkoming van de PSD is er op technologisch vlak veel gebeurd. Denk bijvoorbeeld aan de opkomst van mobiel betalen en betaal-apps. FinTech-ondernemingen introduceerden diensten zoals 'payment initiation' en 'account information'. Onder de PSD zijn beide diensten echter niet gereguleerd. Onder meer om ervoor te zorgen dat bestaande en nieuwe spelers onder gelijke voorwaarden hun activiteiten kunnen verrichten, achtte de Europese Commissie modernisering van de PSD noodzakelijk. In de snelle toename van elektronisch en mobiel betalen zag de Europese Commissie verder aanleiding zwaardere veiligheidseisen voor het betalingsverkeer te introduceren.

Implementatie in Wft en BW

PSD2 zal – als gezegd – uiterlijk 13 januari 2018 in het Nederlandse recht moeten zijn geïmplementeerd.[2] De consultatieversie voor de betreffende implementatiewet is op 18 november 2016 gepubliceerd. Uit het document blijkt onder meer van welke lidstaatopties Nederland gebruik wil maken. Na de consultatieronde zal het wetsvoorstel door de Tweede Kamer en Eerste Kamer moeten worden aangenomen.

1 Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt.

2 Te raadplegen via www.internetconsultatie.nl.

Structuur PSD2
De PSD2, die de PSD volledig vervangt, kent dezelfde structuur als de PSD. De titels I en II bevatten de vergunningsvoorwaarden en bepalingen over toezicht. In de titels III en IV staan regels over de (rechts)verhouding tussen de betaaldienstverlener en de gebruiker van betaaldiensten. Zo zijn in titel IV onder meer de aansprakelijkheidsbepalingen opgenomen. Titel IV bevat ook voorschriften ten aanzien van 'strong customer authentication' (sterke cliëntauthenticatie) en 'alternative dispute resolution (ADR)'-procedures. In Titel V wordt onder meer de bevoegdheid van de Commissie geregeld om gedelegeerde handelingen vast te stellen. Titel VI kent slotbepalingen, waaronder bepalingen die betrekking hebben op betaaldienstverleners die op dit moment al betaaldiensten verlenen. Ook bevat het een aantal wijzigingen in andere richtlijnen, waaronder de herziene richtlijn elektronisch geld (EMD2).
Naast de richtlijn zelf zijn ook de zogenoemde 'Regulatory Technical Standards' ofwel technische standaarden van belang. Deze worden door de European Banking Authority (EBA) en de Europese Commissie voor diverse onderwerpen vastgesteld. Inmiddels zijn enkele technische standaarden in concept opgesteld en ter consultatie aan de markt aangeboden. Een technische standaard die veel stof heeft doen opwaaien, is die waarin de eisen voor 'strong customer authentication' worden ingevuld.
In het vervolg van deze bijdrage worden enkele wijzigingen ten opzichte van de PSD kort besproken.

Substance-eis
Om misbruik van het recht van vestiging te voorkomen, bepaalt de PSD2 dat een betaalinstelling die een vergunning in een lidstaat aanvraagt, ten minste een deel van haar betaaldienstverlening in die lidstaat moet verrichten. Deze 'substance-eis' gaat óók gelden voor bestaande betaalinstellingen en vergunninghoudende elektronischgeldinstellingen. Zij zullen uiterlijk 13 juli 2018 aan deze eis, en overigens ook aan alle andere PSD2-vergunningeisen, moeten voldoen. Wanneer zij op die datum niet aan de nieuwe eisen voldoen, wordt het hun verboden nog langer betaaldiensten aan te bieden respectievelijk elektronisch geld uit te geven. Vergunningen zullen worden ingetrokken. Voor ondernemingen die zijn 'uitgeweken' naar landen waarin gemakkelijker een vergunning kon worden verkregen, zal dit serieuze gevolgen hebben.

Gekwalificeerde deelnemingen – verklaring van geen bezwaar nodig
De PSD2 voorziet in een toetsingsregime voor gekwalificeerde deelnemingen. Bij het verkrijgen van een gekwalificeerde deelneming (direct dan wel indirect een aandelen- of zeggenschapsbelang van 10% of meer) of wanneer het belang hoger wordt dan 20, 30 of 50% of wanneer de betaalinstelling een dochteronderneming zou worden, dient een verklaring van geen bezwaar te worden verkregen. Hetzelfde geldt bij afstoting of vermindering van een gekwalificeerd belang. Dit gaat verder dan de huidige betrouwbaarheidstoetsing van (natuurlijke personen achter) aandeelhouders die als mede-beleidsbepaler worden aangemerkt.

Cross-border dienstverlening – bijkantoor of agent
Nieuw ten opzichte van de PSD is dat de lidstaten kunnen bepalen dat de betaalinstellingen die op hun grondgebied werkzaam zijn, maar waarvan het hoofdkantoor zich in een andere lidstaat bevindt, voor informatie- of statistische doeleinden periodiek verslag aan hen moeten uitbrengen over de activiteiten die op hun grondgebied plaatsvinden. Indien deze betaalinstellingen een bijkantoor hebben of via agenten werkzaam zijn, moet deze informatie ook voor het monitoren van de naleving van de regels in de titels III en IV PSD2 kunnen worden gebruikt. Lidstaten kunnen ook bepalen dat deze betaalinstellingen een centraal contactpunt op hun grondgebied moeten aanwijzen. Nederland is voornemens gebruik te maken van deze lidstaatopties, dit met het oog op een zo efficiënt mogelijk toezicht.
De EBA en de Europese Commissie zullen technische standaarden opstellen waarin onder meer wordt vastgelegd welke taken het contactpunt dient te hebben.

Uitbreiding reikwijdte
De PSD2 brengt meer betaaldienstverlening onder toezicht. Hieronder worden enkele voorbeelden genoemd.

Alle valuta's en 'one-leg transactions'
De reikwijdte van de PSD wordt ten eerste uitgebreid door de bepalingen over (i) de transparantie- en informatievereisten en (ii) de rechten en verplichtingen van betaaldienstgebruikers – enkele uitzonderingen daargelaten – ook te laten gelden voor transacties waarbij één van de betaaldienstverleners zich buiten de Europese Economische Ruimte (EER) bevindt (de 'one-leg transactions'). Ook zullen de desbetreffende bepalingen gelden voor transacties in alle officiële valuta's, wederom enkele uitzonderingen daargelaten, wanneer de betrokken betaaldienstverleners zich in de EER bevinden.

Aanscherping bepaalde uitzonderingen
PSD2 voorziet ook in aanscherping van bepaalde huidige uitzonderingen. Zo wordt de uitzondering voor betaaldiensten binnen een 'beperkt netwerk' (de 'limited-network exemption') beperkt. Zo maakt overweging 14 van de PSD2 duidelijk dat het alleen registreren van aangesloten winkels, die een bepaald betaalmiddel accepteren, niet meer voldoende is om als beperkt netwerk te kwalificeren. Nieuw is verder dat dienstverleners die gebruik willen maken van de 'beperkt netwerk'-uitzondering bij een bepaald transactievolume een notificatie moeten sturen aan de toezichthouder. Wanneer de toezichthouder vindt dat geen beroep kan worden gedaan op de uitzondering, zal de toezichthouder dat gemotiveerd moeten beslissen. De notificaties aan de nationale toezichthouders zullen in de registers van de nationale toezichthouders moeten worden opgenomen en zullen door de EBA worden gepubliceerd.
Een voor de praktijk belangrijke wijziging ziet op e-commerce marktplaatsen. Op dergelijke online marktplaatsen wordt vraag en aanbod ten aanzien van producten en diensten bij elkaar gebracht. De meeste marktplaatsen doen echter meer, waaronder ondersteuning van het betaalproces. DNB ziet dergelijke marktplaatsen, zelfs als zij in het bezit komen van cliëntgelden, op dit moment niet als vergunningplichtig omdat hun hoofdactiviteit niet bestaat uit het aanbieden van betaaldiensten. PSD2 geeft in overweging 11 echter aan dat agenten die zowel voor rekening van de betaler als de begunstigde handelen (zoals de hier bedoelde marktplaatsen) slechts uitgezonderd kunnen zijn van de vergunningplicht indien zij op geen enkel moment in het bezit zijn van of controle hebben over cliëntgelden. Belangrijk is verder dat de uitzondering voor technische dienstverleners (waaronder ook aanbieders van IT- en communicatienetwerken) blijft. Zij mogen echter geen betaalinitiatiediensten of rekeninginformatiediensten aanbieden.

Nieuwe betaaldiensten: payment initiation en account information services
Ondernemingen die betaalinitiatie- en rekeninginformatiediensten aanbieden, worden onder het toepassingsgebied van de PSD2 gebracht. Deze ondernemingen moeten een vergunning hebben of geregistreerd zijn. Om dat te bereiken worden de betaalinitiatie- en rekeninginformatiediensten als nieuwe betaaldiensten in de richtlijn opgenomen. De PSD2 maakt onderscheid tussen 'account servicing payment service providers' ofwel rekeninghoudende betaaldienstverleners (lees: banken) en andere betaaldienstverleners.
De betaalinitiatiedienst is een dienst voor het initiëren van betaalopdrachten, op verzoek van de betaaldienstgebruiker, met betrekking tot een betaalrekening die bij een andere betaaldienstverlener wordt aangehouden. De betaaldienstverlener initieert de betaling ten behoeve van de consument, bijvoorbeeld bij online aankopen bij een webwinkel. Sofort is een voorbeeld van een bedrijf dat doet aan betaalinitiatie. De rekeninginformatiedienst is een onlinedienst voor het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen die de betaaldienstgebruiker bij een of meer betaaldienstverleners aanhoudt. In Nederland is het online huishoudboekje van AFAS Personal daar een voorbeeld van.

Access to the Account (XS2A)
Banken zijn onder PSD2 verplicht aanbieders van betaalinitiatie- en rekeninginformatiediensten toegang te bieden tot betaalrekeningen van hun klanten. Banken mogen voor deze toegang niet eisen dat deze aanbieders een overeenkomst met de bank aangaan. Wanneer een rekeninghouder uitdrukkelijk toestemming geeft voor een betaling via een betaalinitiatiedienstverlener, dient de bank mee te werken. Hoewel over de vorm van toegang nog geen duidelijkheid bestaat, is dit onderdeel van de PSD2 vanuit innovatief, maar ook commercieel oogpunt het meest interessant.
De verplichte toegang ofwel 'access to the account' maakt allerlei nieuwe diensten voor consumenten, maar ook voor zakelijke klanten mogelijk. Via een combinatie van betaalinitiatie en rekeninginformatie kan een nieuwe speler bijvoorbeeld een wallet-oplossing bieden, waarin klanten een integraal overzicht kunnen krijgen van de saldi op hun – bij meerdere banken – aangehouden betaalrekeningen met de mogelijkheid ook betaalopdrachten te geven. Overigens is dit niet exclusief voorbehouden aan FinTech-ondernemingen. Ook bestaande banken kunnen deze nieuwe diensten verlenen. Zo heeft ABN AMRO bijvoorbeeld Gradefix geïntroduceerd. Gradefix is een nieuwe dienst die op basis van betalingsverkeergegevens een analyse en risico-inschatting maakt van een klant. Consumenten en MKB-ondernemingen kunnen deze analyse gebruiken om een compleet en persoonlijk inzicht te krijgen in hun financiële situatie. Zij kunnen zelf bepalen of zij dit rapport willen delen met derden, bijvoorbeeld hypotheekverstrekkers. De transactiegegevens moeten nu nog zelf door de klanten voor een analyse worden aangeboden. In de toekomst zal Gradefix dit echter zelf kunnen doen via de mogelijkheid van rekeninginformatiediensten.[3]

3 Persbericht ABN AMRO 22 november 2016, www.abnamro.com/nl/newsroom/persberichten/2016/abn-amro-biedt-met-gradefix-risk-as-a-service.html.

> De PSD2 maakt onderscheid tussen 'account servicing payment service providers' en andere betaal-dienstverleners.

Strong customer authentication

Voor bepaalde handelingen, bijvoorbeeld het initiëren van elektronische betaaltransacties, schrijft PSD2 'strong customer authentication' ofwel sterke cliëntauthenticatie voor.

Sterke cliëntauthenticatie wordt voorgeschreven wanneer de betaler 1) online toegang wil krijgen tot zijn betaalrekening, 2) een elektronische betaling initieert of 3) via een communicatiemiddel op afstand een handeling verricht die een risico op fraude of ander misbruik met zich brengt. Een voorbeeld van deze laatste categorie is het elektronisch ondertekenen van een machtiging voor automatische incasso (een e-mandate).

Sterke cliëntauthenticatie is – volgens PSD2 – een authenticatie met gebruikmaking van twee of meer factoren die worden aangemerkt als 'kennis', 'bezit' en 'inherente eigenschap'. Bij de factor kennis gaat het om iets wat alleen de gebruiker weet, zoals een pincode. De factor bezit ziet op iets wat de gebruiker heeft, bijvoorbeeld een betaalpas of een mobiele telefoon. De factor inherente eigenschap betreft iets wat eigen aan de gebruiker is, zoals een biometrisch kenmerk als een vingerafdruk. In Nederland is sterke cliëntauthenticatie bij internetbankieren al gebruikelijk.
Sterke cliëntauthenticatie conform de PSD2 zal verplicht zijn achttien maanden nadat de desbetreffende technische standaarden zijn vastgesteld. Gelet op het huidige voorbereidingsproces, zal dat niet eerder dan oktober 2018 zijn. Hoewel sterke cliëntauthenticatie het frauderisico beperkt, wordt daarmee het 'check-out proces' ook verzwaard. Met name voor internetwinkels kan dit tot lagere verkopen leiden wanneer klanten ergens in het 'check-out proces' afhaken. Nu geeft PSD2 aan de EBA óók de bevoegdheid om in de technische standaarden uitzonderingen op sterke cliëntauthenticatie toe te staan. In het concept voor de desbetreffende technische standaarden zijn de uitzonderingen echter wel heel erg beperkt geformuleerd. Vanuit de markt is daarop al veel commentaar geleverd. Zelfs het onderhandelingsteam PSD2 van het Europees Parlement heeft in een reactie aan de EBA laten weten dat de uitzonderingen veel te beperkt zijn. Volgens het onderhandelingsteam zou een risk-based analyse voor het al dan niet toepassen van sterke cliëntauthenticatie ook mogelijk moeten zijn. Gelet op de geavanceerde risk-tools die thans al worden toegepast, zou dit voor de praktijk een mooie uitkomst zijn. Het is echter de vraag of een en ander de EBA en de Europese Commissie tot andere gedachten zal brengen.

Compliance aandachtspunten

Vanzelfsprekend zal de naleving van de nieuwe regels onder PSD2 door banken, betaalinstellingen en elektronischgeldinstellingen de nodige compliance-aandacht vergen. Ook zullen (FinTech-)ondernemingen die betaaldiensten verrichten, moeten beoordelen of de PSD2 wellicht (alsnog) leidt tot een vergunningplicht en welke andere consequenties PSD2 voor hen heeft. Deze beoordeling ligt overigens niet alleen op het bord van de betreffende (FinTech-)ondernemingen zelf. In het geval van een samenwerking met bijvoorbeeld een bank, zal de bank ook zelf moeten beoordelen of haar contractpartner een vergunning nodig heeft. Het betreft hier de invulling van de 'poortwachtersfunctie' waar DNB veel waarde aan hecht. Banken en betaalinstellingen zullen daarnaast ook moeten kijken naar hun cliëntenbestand. Zij zijn immers verplicht hun cliënten te kennen en integriteitsrisico's te identificeren en te beheersen. Daaruit volgt dat zij (i) moeten toetsen of cliënten zich bezig houden met vergunningplichtige activiteiten en zo ja, (ii) bij gebreke van een vergunning gepaste actie moeten ondernemen (zoals bijvoorbeeld het staken van de dienstverlening en het opzeggen van de cliëntrelatie). Overigens zal de toezichtrechtelijke beoordeling niet altijd eenvoudig zijn. Veel zal afhangen van de vraag hoe de toezichthouders in de praktijk de PSD2, althans het daarop gebaseerde nationale recht, zullen toepassen. Daarbij is voor Nederland meer guidance door DNB zeker aan te bevelen. De praktijk zal daarbij gediend zijn!

Arno Voerman is advocaat financieel recht bij Van Doorne N.V. te Amsterdam.

FinTech voor starters

Cora Wielenga

In de afgelopen tijd ben ik het onderwerp FinTech gaan verkennen. Ik ben daarbij vaak verrast. Wat ik had bedacht als toekomstmuziek, is op sommige punten nu al werkelijkheid. En wat ik dacht dat niet mogelijk was, is nu in ontwikkeling. FinTech brengt door de snelle ontwikkelingen een hoop leven in de brouwerij. En deze reuring brengt weer een groot aantal kansen en een groot aantal bedreigingen met zich mee. In deze korte bijdrage neem ik u graag mee in mijn eigen ontdekkingsreis in FinTech-land en stip daarbij een aantal kansen en risico's aan vanuit complianceperspectief. Dit artikel is met name geschreven voor die mensen die nog niet veel over FinTech gehoord of gelezen hebben.

Wat is FinTech?

Veelal wordt bij FinTech gedacht aan start-ups in de financiële dienstverlening. Zie ook onderstaande definitie.

> *Financial technology, also known as FinTech, is an economic industry composed of companies that use technology to make financial services more efficient. Financial technology companies are generally startups trying to disintermediate incumbent financial systems and challenge traditional corporations that are less reliant on software.*[1]

Ik geef er inmiddels de voorkeur aan om FinTech breder te zien. Ik sluit daarom liever aan bij de volgende definitie: *recente en toekomstige technische innovatie in de financiële dienstverlening.*[2] Dit betekent dat FinTech zowel een rol speelt bij start-ups, maar evenzeer bij de financiële ondernemingen in de klassieke zin van het woord.

Eigenlijk zou je kunnen zeggen dat alle innovatie die plaatsvindt in de financiële sector onder FinTech wordt geschaard wanneer de innovatie door techniek wordt ondersteund.

Voor klanten zijn er door deze technische innovatie veel verbeteringen mogelijk. Bestaande dienstverlening wordt verbeterd en nieuwe diensten ontstaan. Ook de ACM houdt zich sinds dit jaar bezig met FinTech. Zij zoeken uit in hoeverre FinTech de concurrentie in de financiële sector kan ondersteunen. Dat zou immers uiteindelijk leiden tot meer keuze en betere dienstverlening voor consumenten.

Vanuit complianceperspectief zijn er risico's verbonden aan de nieuwe technologieën. Ik licht een aantal voorbeelden van FinTech toe en benoem daarbij de compliancekansen en -bedreigingen. Ik ben me ervan bewust dat dit slechts het topje van de ijsberg is, maar voor starters in FinTech kan het een aardige introductie zijn.

1 en.wikipedia.org/wiki/Financial_technology, laatst geraadpleegd op 26 oktober 2016.

2 Afgeleid van en.wikipedia.org/wiki/Financial_technology, laatst geraadpleegd op 26 oktober 2016.

Compliancekansen en -bedreigingen op het gebied van FinTech

In deze paragraaf laat ik een aantal technische innovaties de revue passeren. Ik licht ze heel kort toe en maak daarbij een korte vertaalslag naar het compliancevak.

Blockchain

Wellicht het bekendste voorbeeld wanneer we aan FinTech denken, met name door de bekendheid van bitcoins. Blockchain is een decentrale database die een gestaag groeiende lijst met data bijhoudt die beschermd zijn tegen manipulatie. DNB is in navolging van de Bank of England ook bezig met de ontwikkeling van een eigen munt: DNBcoin. Blockchaintechnologie kun je ook gebruiken voor verificatie van de identiteit van klanten. Dit is mogelijk wanneer meerdere entiteiten jouw identiteit bevestigen. Identificatie en verificatie via blockchain is nu nog wat minder bekend, maar kan goed bijdragen in de Wwft-verplichtingen die veel financiële organisaties hebben. Een nadeel aan blockchaintechnologie vind ik, dat niet veel mensen het begrijpen. Hoe kunnen we de compliance-risico's overzien van iets wat we niet kunnen doorgronden?

Biometrie

Biometrie houdt in dat je eigenschappen van mensen kunt meten. Bekende voorbeelden zijn de vingerafdruk of de irisscan. Maar ook het meten van je stem of de manier van lopen valt hieronder. Biometrie kun je gebruiken bij identificatie en verificatie van klanten. Zoals bijvoorbeeld gebeurt bij het vrijgeven van onze smartphones of bij het inchecken op vliegvelden. Daarnaast kun je biometrie inzetten om gedragingen van mensen te meten. Er bestaan systemen die deze gedragingen meten, bijvoorbeeld door het dragen van polsbandjes, meetkastjes of zelfs bepaalde kleding. Hierbij wordt dan vastgelegd met wie mensen praten en op welke manier dat gebeurt. Vervolgens wordt de data geanalyseerd. Bij sportteams heeft dit al tot verbetering van de sportprestaties geleid. Dit is sinds een aantal jaar ook te gebruiken in zakelijke context: aan de hand van de gedragingen van mensen worden team-prestaties verbeterd, besluitvormingsprocessen verbeterd en werkstress verminderd.[3] Daarnaast kan biometrie organisaties helpen om fraude te reduceren. De data die biometrie oplevert, kan geanalyseerd worden en leiden tot red flags die vervolgens weer onderzocht kunnen worden. Toekomstmuziek? Nee hoor, dat kan en gebeurt al. Mooi dat dit kan; je kunt het dus ten goede gebruiken om het gedrag positief te beïnvloeden. Daarnaast kun je het repressief inzetten in het geval van fraudedetectie. Maar ik moet eerlijk bekennen dat ik dit ook spannend vind. Hoe ver willen we gaan? En hoe staat het met onze privacy?

> FinTech speelt een rol bij start-ups, maar evenzeer bij de traditionele financiële ondernemingen

Advanced analytics

Dit is het analyseren van big data om bijvoorbeeld klant-wensen te voorspellen. ABP gebruikt dit bijvoorbeeld in de klantbediening om op basis van bepaalde gebeurtenis-sen bij klanten, zoals een nieuwe baan of een geboorte van een kind, mogelijke klantvragen te voorspellen. Het ABP informeert klanten proactief over hun gewijzigde situatie, zodat klanten beter bediend worden. Doordat klanten eerder en beter worden geïnformeerd, wordt de klanten-service minder gebeld en worden de kosten van de klantenservice naar beneden gebracht. Ook AFM en DNB zijn bezig een slag te maken naar het data-

3 techcrunch.com/2015/02/24/new-firm-combines-wearables-and-data-to-improve-decision-making, laatst geraadpleegd op 26 november 2016.

gedreven toezicht.[4] Organisaties die werken met advanced analytics hebben rekening te houden met de privacyregelgeving wanneer er gewerkt wordt met persoonsgegevens. Op het moment dat de gegevens geanonimiseerd worden verwerkt, worden deze niet meer aangemerkt als persoonsgegevens.

Kunstmatige intelligentie

Kunstmatige intelligentie (ook wel artificial intelligence (AI) genoemd) houdt in dat computers zelf leren. Dit kan positief werken ten aanzien van bijvoorbeeld robo-advies. Hiermee kun je als organisatie voorkomen dat er advies gegeven wordt wanneer dat niet mag. Of kun je beter borgen dat het juiste advies wordt gegeven. Een nadeel van zelflerende computers is dat mensen de computers op een gegeven moment niet meer begrijpen. Er zijn op dit moment al twee computers die hun eigen codetaal hebben ontwikkeld die mensen niet meer kunnen achterhalen.[5] Hoewel ik het vanuit zorgplicht kan begrijpen dat het prettig is om foutloze adviezen te geven, vind ik het vanuit compliance-oogpunt een risico wanneer we niet meer kunnen begrijpen waar we toezicht op houden.

Cloud computing

Oftewel: onze data in de lucht. Dit roept bij mij allerlei beveiligingsrisico's op. Mogelijk doordat ik niet voldoende weet van de (on)mogelijkheden. Ik vind het in ieder geval een spannend idee dat data in de cloud wordt opgeslagen.

Dit valt wellicht nog mee wanneer organisaties hun eigen cloud ontwikkelen, maar bij het gebruik van publieke clouds besef je wellicht niet altijd waar de bedrijfsdata wordt opgeslagen.

BigTech

BigTech's zijn grote technologiebedrijven die toetreden op de markt voor financiële diensten. Door hun bekendheid bij consumenten en technologische voorsprong kunnen zij waarschijnlijk relatief eenvoudig de concurrentie aangaan met bestaande financiële ondernemingen. Volgens een

studie van de AFM is het de verwachting dat BigTech's meerdere financiële diensten aanbieden (o.a. betalen, beleggen, verzekeringen) in plaats van zich op één dienst te richten, zoals gebruikelijk bij start-ups.[6]

Rol van compliance officers

Wat moeten compliance officers nu met deze ontwikkelingen? Volgens mij is het essentieel om te weten hoe ver je eigen organisatie is met technologische innovatie en te weten wat de kansen en risico's zijn die darmee samenhangen. Compliance officers kijken nu mee in de productontwikkeling van financiële organisaties. Los van onze rol in PARP-processen krijgen compliance officers steeds vaker een toetsende rol in de beoordeling van (strategische) veranderingen van de organisatie. FinTech is een snelgroeiend terrein. Als je eigen organisatie actief is in technische innovatie, is het aan de compliancefunctie om hier actief vanaf het begin aan te haken, zodat tijdig eventuele risico's kunnen worden besproken of eventuele voordelen beter benut kunnen worden.

Cora Wielenga is directeur van het Nederlands Compliance Instituut.

4 AFM, *Toezicht in tijden van verandering. Agenda 2016-2018*, januari 2016.

5 www.vn.nl/het-begint-twee-computers-hebben-een-geheimtaal-bedacht, laatst geraadpleegd op 3 november 2016.

6 www.dnb.nl/binaries/Discussiedocument%20AFM-DNB%20Meer%20ruimte%20voor%20innovatie_tcm46-342351.pdf, laatst geraadpleegd op 27 oktober 2016.

Compliance telt mee

In deze rubriek zal ik aangeven waarom de compliancefunctie, na de stresstesten van de Europese Bankenautoriteit (EBA), echt meetelt en dat het de hoogste tijd is de governance bij banken hierop aan te passen.

Stresstesten

Eind juli 2016 publiceerde de EBA de resultaten van de stresstest van Europese systeembanken. Met name de verandering in systematiek van de stresstesten zal voor de compliancefunctie grote gevolgen hebben.
In de stresstest van 29 juli is voor het eerst rekening gehouden met 'operational risks'. Het hoogste kapitaalbeslag is voor credit risk (debiteurenrisico) € 349 miljard of driehonderdzeventig basispunten. Operational risk is met € 105 miljard en honderdtien basispunten het tweede risico, nog voor market risk met € 98 miljard en honderd basispunten.
Binnen het operational risk van € 105 miljard maakt 'conduct risk' € 71 miljard uit. Conduct risk heeft betrekking op mis-selling, marktmanipulatie en witwasdetectie en is daarmee een proxy voor compliance- en integriteitrisico's. Het meenemen van conduct risk in het solvabiliteitsbeslag voor het beheersen van compliancerisico's is van eminent belang.
Aandacht voor, en investeren in, de compliancefunctie is tot nu toe vaak een lastige discussie. Bestuurders zien wel dat het noodzakelijk is, maar een objectief element in de discussie ontbrak tot nu toe.

Governance bij banken

De vraag wie de klant is van de compliancefunctie van banken is van groot belang voor het goed borgen van deze functie. Vrijwel ieder compliance charter leert dat de compliance officer de raad van bestuur gevraagd en ongevraagd van advies moet dienen. Zo beschouwd is de klant van de compliance officer de raad van bestuur. Deze benoemt, beoordeelt en ontslaat de compliance officer. Onze toezichthouders verwachten terecht dat de compliance officer kritisch is ten aanzien van de issues die spelen binnen de bank en dus ook kritisch is naar de raad van bestuur. Kun je daar een goede invulling aan geven als diezelfde raad van bestuur je klant is?

De klant is eerder de raad van commissarissen. Hij baseert zijn toezicht echter mede op interne rapportages die voor de huidige klant van de compliance officer zijn opgesteld. Voor de interne auditfunctie geeft de Bank for International Settlements in haar 'Corporate governance principles for banks (July 2015)' aan, dat zijn rapportages zonder 'management filtering' naar de auditcommissie gestuurd dienen te worden. Hierdoor verschuift de hiërarchische rapportagelijn de facto van de raad van bestuur naar de raad van commissarissen of de auditcommissie, waarmee de onafhankelijke positie van de interne auditor goed geborgd wordt.
In Amerika is een soortgelijke tendens te zien. Een aantal grote namen in de Amerikaanse zakenwereld, waaronder Warren Buffet en Jamie Dimon, publiceerden in juli dit jaar 'Commonsense Corporate Governance Principles'. Hun eerste principe luidt:

"Truly independent corporate boards are vital to effective governance, so no board should be beholden to the CEO or management. Every board should meet regularly without the CEO present, and every board should have active and direct engagement with executives below the CEO level."

Het is de hoogste tijd dit ook zo voor de compliancefunctie in te richten. Laat de raad van commissarissen de compliance officer benoemen, beoordelen en ontslaan en laat de compliance officer rapporteren aan de raad van commissarissen of aan een commissie van de raad van commissarissen.

Cor Jan Dasselaar is governance, risk en compliance consultant en oud voorzitter van de Vereniging Compliance Officers.

Zakelijk gebruik van WhatsApp vanuit privacyperspectief

Hans Kooij

'WhatsApp zet de deur open voor bedrijven' kopte Nu.nl recent.[1] Bedrijven die WhatsApp gebruiken als klantcontactkanaal zullen blij geweest zijn met deze titel. Schijn bedriegt. Wordt WhatsApp zakelijk ingezet, dan is dat een overtreding van de voorwaarden van WhatsApp en de Wet bescherming persoonsgegevens (Wbp). In dit artikel wordt zakelijk gebruik van WhatsApp beoordeeld vanuit privacyperspectief. Conclusie is dat, mits een bedrijf de informatievoorziening richting klanten goed inricht en de juiste waarborgen treft, de privacy-inbreuk gering is.

Gewijzigde voorwaarden WhatsApp maken zakelijk gebruik mogelijk met toestemming van WhatsApp

25 augustus 2016 werkte WhatsApp voor het eerst in vier jaar de voorwaarden en het privacybeleid bij. Wie herinnert zich nog de blog van de CEO van WhatsApp bij de overname door Facebook in 2014: *"[…] het respect voor privacy zit in ons DNA. Wanneer de samenwerking met Facebook had betekend dat we onze waarden zouden moeten wijzigen, hadden we de samenwerking niet aangegaan."*[2]

De recente wijziging is onder andere doorgevoerd om zakelijk gebruik te kunnen introduceren en duidelijker te maken dat WhatsApp onderdeel is van Facebook. WhatsApp is ook data gaan delen met Facebook. In november is WhatsApp daar voor Europese gebruikers mee gestopt na druk vanuit de Europese toezichthouders.

De gewijzigde voorwaarden maken zakelijk gebruik mogelijk, mits een bedrijf daarvoor toestemming krijgt van WhatsApp.[3] Voor zover bekend is een dergelijke toestemming nog niet gegeven. Wel geeft WhatsApp aan te experimenteren met een aantal bedrijven. Veel bedrijven zetten WhatsApp desondanks in vanwege de populariteit en omdat klanten erom vragen, en accepteren daarmee risico's.

Hey there! I am using WhatsApp!

Het in Californië gevestigde WhatsApp Inc. is met meer dan een miljard gebruikers een van de meest populaire berichtendiensten.[4] Veel partijen gebruiken WhatsApp in communicatie met klanten en ook de overheid

1 Nu.nl, 'WhatsApp zet de deur open voor bedrijven, www.nu.nl/apps/4312149/whatsapp-zet-deur-open-bedrijven.html

2 WhatsApp Blog, 'Een aantal zaken rechtzetten', 17 maart 2014, blog.WhatsApp.com/529/Een-aantal-zaken-rechtzetten

3 Voorwaarden en Privacybeleid WhatsApp (taalinstelling: NL), www.whatsapp.com/legal geraadpleegd 23 september 2016. Overal waar WhatsApp verder gequote wordt, betreft dit deze zelfde Voorwaarden en Privacybeleid.

4 WhatsApp blok 'Eén Miljard',1 februari 2016, blog.whatsapp.com/616/E%C3%A9n-miljard?

experimenteert met WhatsApp.[5] Een klant die contact via WhatsApp op prijs stelt, kan een bedrijf toevoegen en wordt daarmee bediend via het door hem gewenste kanaal.

Hey there! Is WhatsApp using me?

"Ons Privacybeleid legt uit hoe we samenwerken om onze Diensten en ons aanbod te verbeteren, zoals het bestrijden van spam, het doen van productsuggesties en het tonen van relevante aanbiedingen en advertenties op Facebook. […] Uw berichten zijn van u en wij kunnen ze niet lezen."

Via WhatsApp worden persoonsgegevens verwerkt. In Nederland is daarop de Wet bescherming persoonsgegevens (Wbp) van toepassing.[6] De Wbp is de implementatie van de Europese Privacyrichtlijn in Nederland en is dwingend recht. Vanuit privacyperspectief is het dan belangrijk om te weten welke persoonsgegevens WhatsApp verwerkt. Begin 2013 publiceerde de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens (AP, destijds nog het CBP), samen met de Canadese toezichthouder OPCC, de bevindingen van een gezamenlijke onderzoek naar WhatsApp.[7] Hoewel WhatsApp een Amerikaans bedrijf is, was de AP gerechtigd tot onderzoek. Omdat WhatsApp zich (ook) richt op Nederlanders en omdat persoonsgegevens van Nederlanders door middel van de app op smartphones in Nederland worden verwerkt, is de Wbp van toepassing. De toezichthouders stelden vast dat WhatsApp onder andere de volgende persoonsgegevens verwerkt: status, profielfoto, de mobiele telefoonnummer(s) van gebruikers en niet-gebruikers uit het adresboek, en de berichten en bijlagen. Al deze gegevens kunnen ook met Facebook gedeeld worden, met uitzondering van de berichtinhoud en bijlagen; die worden versleuteld. Succesvol afgeleverde berichten worden verwijderd van de servers van WhatsApp. Niet-succesvol afgeleverde berichten worden dertig dagen bewaard en worden daarna alsnog automatisch van de servers verwijderd. De AP concludeert dat de gegevensverwerking van WhatsApp op diverse gronden in strijd is met de Wbp, waaronder een te lange bewaartermijn en onvoldoende beveiliging. Bovendien zouden gegevens van niet-gebruikers niet verwerkt mogen worden.

De beveiliging is grotendeels opgelost door de invoer van versleuteling van berichten, maar de overige punten gelden ook nu nog. Recent oordeelde de rechtbank Den Haag dat WhatsApp een vertegenwoordiger in Nederland moet aanwijzen.[8] Wordt dat niet gedaan dan is een dwangsom verschuldigd van € 10.000,- per dag met een maximum van € 1.000.000,-. WhatsApp gaf aan dat dit onmogelijk is, omdat geen partij WhatsApp wil vertegenwoordigen vanwege de aansprakelijkheid voor boetes en dwangsommen. Let wel: het gaat hier om de verantwoordelijkheid die WhatsApp heeft richting gebruikers. De AP zou echter kunnen oordelen dat een bedrijf dat WhatsApp inzet, wetende dat WhatsApp in strijd met de Wbp handelt, de zorgvuldigheidsnorm van art. 6 Wbp schendt. Een factor om mee te wegen in de risicoanalyse.

5 Frankwatching, 'Hoe wordt WhatsApp zakelijk ingezet? Resultaten eerste onderzoek in Nederland', 16 februari 2016, www.frankwatching.com/archive/2016/02/16/hoe-wordt-WhatsApp-zakelijk-ingezet-resultaten-eerste-onderzoek-in-nederland en Belastingdienst actueel, 'Schrijf u in voor de intermediairdagen!', www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/berichten/nieuws/schrijf_u_in_voor_de_intermediairdagen. NB: Een rechtspersoon kwalificeert echter meestal niet als 'persoonsgegeven' tenzij daar een individu uit herleidbaar is, daarom is communicatie via WhatsApp tussen ondernemers vanuit privacy optiek niet/minder bezwarend.

6 Ook de Telecommunicatiewet (Tw) is van toepassing omdat informatie wordt geplaatst op de randapparatuur van de gebruiker. Omdat het telefoonnummer van een bedrijf wordt toegevoegd door de klant, wordt naar mijn mening daarmee voldaan aan het toestemmingsvereiste van art. 11.7a lid 1 sub b Tw.

7 Autoriteit Persoonsgegevens, Rapport definitieve bevindingen 'Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie whatsapp door WhatsApp Inc.', januari 2013.

8 Rechtbank Den Haag, 22-11-2016, SGR - 15-9125.

Verantwoordelijke(n)

Een bedrijf dat WhatsApp als middel inzet voor haar doelen is de 'verantwoordelijke' voor de wet. De Wbp stelt geen expliciete eisen aan de relatie verantwoordelijke – verantwoordelijke (in tegenstelling tot de Algemene Verordening Gegevensbescherming (AVG) die 25 mei 2018 van kracht wordt). De verplichtingen uit de Wbp blijven wel gelden. Dat betekent dat het bedrijf dat WhatsApp gebruikt, gegevens verstrekt aan WhatsApp en daar afspraken over dient te maken. De enige optie is echter het accepteren van de standaard voorwaarden van WhatsApp waarin onder andere een vrijwel onbeperkt gebruiksrecht op alle data (inclusief de berichtinhoud) wordt bedongen door WhatsApp. De klant heeft als gebruiker van WhatsApp diezelfde voorwaarden geaccepteerd. Een verantwoordelijke voor de wet kan ook een 'natuurlijk persoon' zijn. De klant is dus ook verantwoordelijke.[9] Als een bedrijf WhatsApp aanbiedt en een klant voegt een bedrijf zelf toe, dan kiest de klant ervoor om dit middel in te zetten. Hoewel dit niet afdoet aan de wettelijke verantwoordelijkheid van een bedrijf en de AP een bedrijf hierop kan aanspreken, is het naar mijn mening wel relevant voor de risicoafweging om WhatsApp in te zetten.

Dat geldt des te meer als een bedrijf waarborgen treft om de risico's van de gegevensdoorgifte te beperken. Bijvoorbeeld door geen gevoelige persoonsgegevens zoals gezondheidsgegevens, wachtwoorden of de financiële situatie van een klant via WhatsApp te sturen aan of te vragen.[10] Wijs de klant daar ook actief op. Deelt een klant desondanks gegevens die in deze categorie vallen, verwijs dan bijvoorbeeld naar een ander klantcontactkanaal. Sowieso is het goed informeren van de klant belangrijk, niet voor niets is transparantie een van de belangrijkste uitgangspunten van privacyregelgeving.

Let wel: de AP kan een bedrijf niet aanspreken op de verwerking van gegevens door WhatsApp waar een bedrijf niks mee te maken heeft, zoals het uploaden van de contactpersonenlijst uit het toestel van de klant naar de servers van WhatsApp.

9 Van uitsluitend persoonlijke of huishoudelijke doeleinden conform art. 2a Wbp is naar mijn mening geen sprake als een gebruiker WhatsApp inzet om met een bedrijf te communiceren.

10 Voor de opsomming van 'gevoelige persoonsgegevens' zie CBP Richtsnoeren, 'Beveiliging van persoonsgegevens', februari 2013, pag. 19.

Informatieplicht

Een bedrijf dat WhatsApp inzet, zal de klant moeten informeren over haar identiteit als verantwoordelijke, de doelen waarvoor WhatsApp wordt ingezet en andere informatie als dat nodig is om een behoorlijke en zorgvuldige gegevensverwerking te waarborgen.[11] Die informatie kan gegeven worden op de bedrijfswebsite in combinatie het telefoonnummer waarop het bedrijf bereikbaar is via WhatsApp.

Omdat de servers van WhatsApp in de Verenigde Staten staan, is het goed om de klant hierop te wijzen, ook al heeft de klant zelf al geaccepteerd dat zijn gegevens naar de VS gaan door WhatsApp te installeren. Bijvoorbeeld door op de website de klant uit te leggen dat door het toevoegen van het bedrijf aan de WhatsApp contactpersonen lijst, hij toestemming geeft voor de doorgifte van zijn gegevens naar de Verenigde Staten (hoewel de klant dat zelf ook al geaccepteerd heeft door WhatsApp in gebruik te nemen).[12] WhatsApp doet namelijk vooralsnog niet mee aan het Privacy Shield waarbij een Amerikaans bedrijf zichzelf moet aanmelden om uitwisseling van persoonsgegevens met de EU mogelijk te maken. Moederbedrijf Facebook heeft zich daar wel voor aangemeld, maar slechts voor beperkte doeleinden.

Verwerkingsgrond conform artikel 8 Wbp

Voor gebruik van WhatsApp door een bedrijf richting klanten zijn de meest aannemelijke grondslagen:

- Ondubbelzinnige toestemming: Aan 'ondubbelzinnig' kan invulling worden gegeven door niet als bedrijf het eerste contact te leggen, maar door de klant op de juiste wijze te informeren via de website en het initiatief bij de klant te laten om het bedrijf toe te voegen aan zijn contactpersonen in WhatsApp en een gesprek te starten. Een bedrijf moet de klant ook de mogelijkheid bieden om toestemming in te trekken. Een klant kan het bedrijf blokkeren of verwijderen binnen WhatsApp, dat is standaard functionaliteit. Dat weet het bedrijf dan echter niet. Betoogd kan worden dat een bedrijf het intrekken van toestemming daarom als optie ook zelf (nog) moet aanbieden. Op de website zou hier invulling aan gegeven kunnen worden door bijvoorbeeld te vragen of de klant het bedrijf het (via WhatsApp) wil laten weten als communicatie via WhatsApp niet meer gewenst is. Als het bedrijf

11 Artikel 33 lid 2 en 3 Wbp.

12 Conform artikel 77 lid 1 a Wbp.

WhatsApp enkel gebruikt voor klantcontact en gegevens niet verder gebruikt, vind ik het verdedigbaar dat geleund wordt op de standaard functionaliteit van WhatsApp.

- Noodzakelijk voor de behartiging van een gerechtvaardigd belang: vergt het aantoonbaar afwegen van de belangen van de klant om gevrijwaard te blijven van een privacy inbreuk versus de bedrijfsbelangen, waarbij die laatste moeten prevaleren. Onder de AVG moeten de gerechtvaardigde belangen ook gecommuniceerd worden.
- Noodzakelijk voor de uitvoering van een overeenkomst. Bijvoorbeeld als in een verzekeringsovereenkomst afgesproken wordt dat een schademelding gedaan kan worden via WhatsApp.

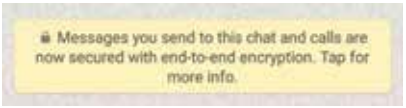
De verantwoordelijke moet passende technische en organisatorische maatregelen treffen

Een bedrijf dat WhatsApp inzet richting klanten is verantwoordelijk voor een goede beveiliging. Als een goede beveiliging niet (tegen acceptabele kosten) kan worden gerealiseerd, dan zou van een verwerking moeten worden afgezien.[13] Met andere woorden: 'Nee, tenzij…'.

Dat is lastig, want hierover zijn geen afspraken te maken met WhatsApp. Bijvoorbeeld over geheimhouding of het toepassen en toegepast houden van beveiligingsmaatregelen in de app. Gelukkig heeft WhatsApp wel beveiligingsmaatregelen getroffen. Voor de berichtinhoud wordt end-to-end-encryptie toegepast na de update van WhatsApp van april 2016.[14] Door de toepassing van deze versleuteling is het voor WhatsApp in principe niet mogelijk om bij de berichtinhoud te komen op hun servers.

Overigens zou het zou kunnen zijn dat WhatsApp de berichtinhoud in de toekomst wel gaat gebruiken. WhatsApp kan immers de inrichting van de dienst wijzigen. Een uitgebreid gebruiksrecht op alle data – en dus ook de berichtinhoud – is nu ook al opgenomen in de voorwaarden:

"Voor de exploitatie en verlening van onze Diensten verleent u aan WhatsApp een wereldwijde, niet-exclusieve, royalty-vrije, sublicentieerbare en overdraagbare licentie voor het gebruik, de reproductie, de distributie, het maken van afgeleide werken van, de vertoning en de uitvoering van de informatie (met inbegrip van de inhoud) die u uploadt, indient, opslaat, verstuurt of ontvangt naar, op of via onze Diensten."



Dit uitgebreide gebruiksrecht dat WhatsApp bedingt, is bezwaarlijk vanuit privacyperspectief en zou een bedrijf normaliter niet moeten accepteren. Wat moet WhatsApp hiermee als ze toch niet bij berichten kunnen door de toegepaste end-to-end-encryptie? Die encryptie zorgt in de praktijk voor een 'passend beschermingsniveau'. Een bedrijf dat WhatsApp inzet, zal deze tegenstelling moeten accepteren (of WhatsApp niet gebruiken).

Let wel: ondanks de end-to-end-encryptie van de berichtinhoud zou het voor WhatsApp technisch mogelijk kunnen zijn om berichten te (gaan) gebruiken, door bijvoorbeeld de Facebook-app toegang te geven tot WhatsApp.

13 CBP Richtsnoeren, 'Beveiliging van persoonsgegevens', februari 2013, pag. 20.

14 Whispersystems.org, 'WhatsApp's Signal Protocol integration is now complete', 5 april 2016. Voor uitleg vanuit WhatsApp over de toegepaste encryptie www.WhatsApp.com/security/WhatsApp-Security-Whitepaper.pdf.

> Een bedrijf dat WhatsApp inzet richting klanten is verantwoordelijk voor een goede beveiliging

Op het toestel van de gebruiker zijn de gegevens immers niet versleuteld. Hetzelfde geldt voor de webversie van WhatsApp, daar zou ook op 'meegelezen' kunnen worden. Voor zover bekend doet WhatsApp dit overigens niet.

Aan de kant van het bedrijf dat WhatsApp inzet, kunnen vanzelfsprekend ook de benodigde technische en organisatorische maatregelen getroffen worden. Bijvoorbeeld het selecteren van een betrouwbare leverancier voor het ontsluiten van WhatsApp, het inrichten van de juiste beveiliging en autorisaties en richtlijnen voor medewerkers die klantcontact hebben via WhatsApp.

Welk risico neemt een bedrijf?

Sancties vanuit WhatsApp

In de voorwaarden van WhatsApp is opgenomen dat gebruik enkel is toegestaan voor persoonlijk gebruik, tenzij een bedrijf toestemming heeft van WhatsApp. Bovendien mag WhatsApp zonder voorafgaande toestemming niet toegankelijk gemaakt worden voor, of de inhoud niet automatisch gekopieerd worden naar, een ander medium. Er zijn diverse partijen die software of een dienst aanbieden waarmee WhatsApp ontsloten wordt. Als hiervoor geen toestemming door WhatsApp is gegeven, wordt inbreuk gemaakt op het intellectueel eigendom en de voorwaarden van WhatsApp door de partij die dit aanbiedt en het bedrijf dat hiervan gebruik maakt. Beide riskeren een geschil met WhatsApp.

Vooralsnog denk ik niet dat dit snel zal gebeuren. Pas als WhatsApp een eigen zakelijk alternatief uitbrengt, daar een verdienmodel voor introduceert en zakelijke gebruikers dwingt om daar gebruik van te maken neemt het risico op een geschil toe voor een bedrijf dat WhatsApp zakelijk inzet. WhatsApp treedt overigens ook nu al op tegen partijen die inbreuk maken op het intellectueel eigendom van WhatsApp door een ontsluiting van WhatsApp als dienst aan andere bedrijven aan te bieden.[15] Vanuit risicoperspectief is het goed om te realiseren is dat een dergelijke (niet door WhatsApp geaccordeerde) ontsluiting instabiel kan zijn. Als WhatsApp een wijziging doorvoert in de techniek, moet een leverancier van software of een dienst die WhatsApp ontsluit daar snel genoeg op (kunnen) reageren. Een kleine aanpassing door Whatsapp kan ervoor zorgen dat de software of de dienst niet meer goed werkt of het helemaal niet meer doet.

Sancties vanuit de toezichthouder

De Autoriteit Persoonsgegevens kan de verantwoordelijke sanctioneren voor een overtreding van de Wbp. In beginsel wordt eerst een zogenaamde 'bindende aanwijzing' opgelegd. Dat is een verplichting om iets binnen een bepaalde tijd te doen of na te laten. Echter, als het gaat om een bewuste overtreding van de privacyregelgeving, kan een boete direct opgelegd worden. De maximale boete is momenteel € 820.000,- of, als dat hoger is en passender wordt geacht, 10% van de jaaromzet van een ondernemingsgroep. Let wel, als WhatsApp met de juiste waarborgen wordt ingezet is het niet waarschijnlijk dat boetes zo hoog zijn. De impact van de overtreding op de persoonlijke levenssfeer van de in dit geval de klant is namelijk een factor die meeweegt bij het vaststellen van de boete.[16]

Privacy-inbreuk gering met de juiste waarborgen

Naar mijn mening is samengevat de inbreuk op de persoonlijke levenssfeer van een klant beperkt, mits een bedrijf de informatievoorziening richting klanten goed inricht en de juiste waarborgen treft, waaronder geen gevoelige gegevens verwerken met WhatsApp.

Mr. J. Kooij is compliance officer privacy bij Achmea.

---

15 NOS.nl, 'Startup moet stoppen met klantenservice-systeem via WhatsApp', 23 maart 2016. Vergelijk ook Klantcontact.nl, waar een 'Cease and desist' aanmaning vanuit WhatsApp is gepubliceerd tegen een generieke ontsluiting, www.klantcontact.nl/wp-content/uploads/2015/10/WhatsApps-Cease-and-Desist-and-Demand-Against-Chat-API.pdf

16 Artikel 6.1 sub c Boetebeleidsregels Autoriteit Persoonsgegevens 2016.

Breken met banken

Roderick Noordhoek

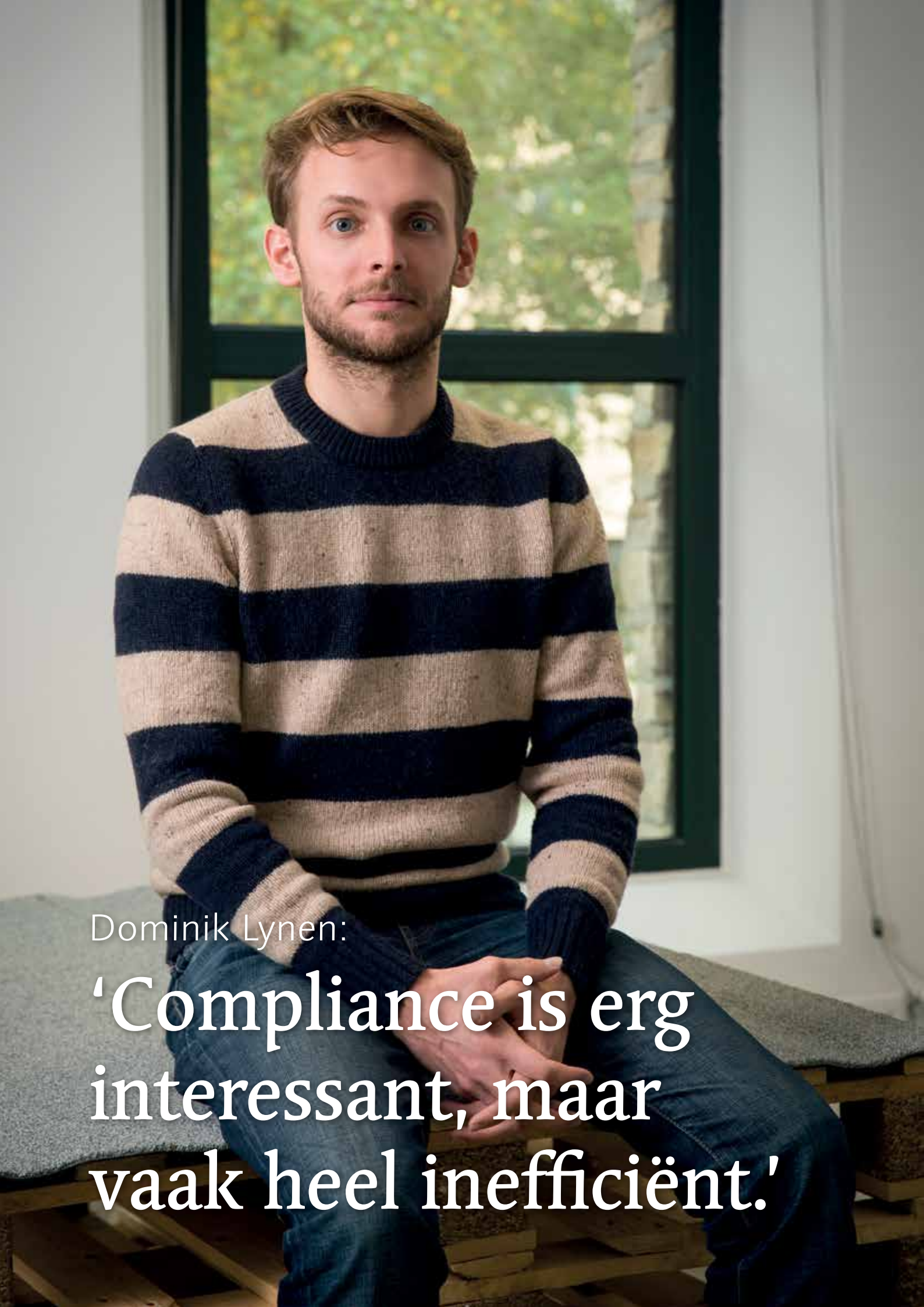
Siebe Huizinga

In deze editie wordt, heel toepasselijk, het boek 'Breken met banken' besproken. Siebe Huizinga beschrijft in het boek de start van bunq, 'het IT-bedrijf met een bankvergunning'.

Bunq is opgericht door Duke Prins en Ali Niknam. Samen met de andere 'bunqers' willen zij geschiedenis schrijven, wat direct duidelijk wordt uit de eerste bladzijde van het boek: *"Fueled with ambition, we are bent on writing history. This could be your chance to be a part of a game changing initiative – if you are up for it!"-bunq.* Dat laatste moet overigens vrij letterlijk worden genomen, zo blijkt. Had het initiatief om een nieuw soort bank te beginnen zo lang geduurd als vooraf was bedacht, zes maanden, dan was dat nog aanvaardbaar geweest voor een hoop mensen. Helaas bleek het een uitputtingsslag van vier jaar. Niet in de laatste plaats doordat DNB op de proef werd gesteld met een geheel nieuw business-model, met daarbij het DSB-debacle nog vers in het geheugen.

Bunq komt regelmatig in een paradoxale situatie terecht, zoals bijvoorbeeld bij het ontwikkelen van producten. Zo moet bunq wachten op een vergunning van DNB, en dus op toegang tot interbancaire gegevens (SWIFT), terwijl DNB eerst een werkend product wil zien voordat ze een vergunning verlenen. Gelukkig hebben ze vanaf het eerste moment Arthur Docters van Leeuwen achter zich staan, zelf lang bestuursvoorzitter van de AFM. De chapter-22-situatie, zoals Ali en de bunqers het noemen, lijkt bunq een aantal keer de das om te doen. Maar Ali, Duke en de andere bunqers zijn vastberaden een bank te beginnen, ook als dat betekent dat werk-nemers vervangen moeten worden of dat er nog meer eigen geld van Ali in het bedrijf gestoken moet worden. Niet alleen moet er een aantal keer pas op de plaats worden gemaakt vanwege het ontbreken van een vergun-ning, ook krijgt Ali te maken met hersenletsel na een val. En wordt hun anti-bankhouding een aantal keer flink op de proef gesteld, niet in de laatste plaats als blijkt dat er door de buffervereisten van DNB nog eens miljoenen extra geïnvesteerd moeten worden, waarna bunq zich toch moet wenden tot ... een bank. Ook is het voor de medewerkers lastig om aan de verwachtingen te blijven voldoen die bunq stelt. Met name de coders (die technisch gezien de app ontwikkelen) krijgen het te verduren wanneer voor de zoveelste keer alles wat zij aan coderingen hebben geschreven door Ali persoonlijk in de prullenbak wordt gegooid. Als die prullenbak er al was, want bunq begint vanuit een anti-kraakpand en dat betekent: een lift met een eigen wil, slapende zwervers in het pand en in de winter werken met jassen aan.

Het streven naar geschiedenis schrijven zorgt ervoor dat alleen het beste talent door bunq wordt aangetrokken. Alleen het allerbeste talent mag plaatsnemen in de zogenaamde 'pro-room'. Het beleid van bunq is direct en wars van enige politieke correctheid, maar bunq bewijst dat, dat ook helemaal niet nodig is. Want waar de gemiddelde lezer waarschijnlijk al een aantal keer had gedacht dat bunq er nooit van zou komen, lijkt het alsof het idealisme van de 'inner circle' groeit tot surrealistische hoogte (voor zover dat niet al een contradictio in terminis is). En dat... Dat was dus precies Niknam's bedoeling, want zoals hij zelf zegt: *"Realistische verwachtingen leiden tot realistische resultaten."*
En zo het geschiedde.



Dominik Lynen:

‘Compliance is erg interessant, maar vaak heel inefficiënt.’

In 2014 was het zover: na vijfendertig jaar was er een nieuwe bank opgericht, bunq. Een bijzonder moment, want bunq was de eerste nieuwe bank na DSB. Met de boodschap dat zij de concurrentie aangingen met de bestaande banken, lagen de verwachtingen hoog, niet in de laatste plaats van de toezichthouder. Na de oprichting duurde het uiteindelijk nog een jaar voordat bunq haar eerste product lanceerde. Inmiddels is bunq uit de start-up-fase en is de app steeds populairder aan het worden. Want dat is bunq: een IT-bedrijf met een app waarmee je gratis geld over kan maken, betalingsverzoeken kan doen, tien verschillende rekeningen kan openen en rekeningen kan delen, maar dan een stuk makkelijker dan bij een traditionele bank. Hoe het is om compliance officer te zijn bij een bedrijf als bunq, dat vertelt *Dominik Lynen*, in gesprek met Roderick Noordhoek.

Wat is jouw achtergrond voor en bij bunq? "Ik heb Europees recht gestudeerd in Maastricht en ben mij later gaan focussen op ondernemingsrecht. Verder heb ik in mijn studententijd veel gedaan met het ontwikkelen van (web) applicaties. Daarna ben ik bij bunq terechtgekomen; een geheimzinnige IT-start-up die op zoek was naar een jurist. Ik ben toen begonnen als legal counsel en heb in het begin met een klein team de aanvraag bankvergunning geschreven. Zo belandde ik direct in de compliance-functie; ik was bekend met de rules & regulations, want die had ik grotendeels zelf geschreven. Daarbij kreeg ik in het begin overigens wel ondersteuning van een externe compliance officer."

Hoe was het om betrokken te zijn bij die bankvergunning? "De toezichthouder was bij ons erg 'supportive' en de wet vormt een goed raamwerk. Het lastige is dat je de wet moet gaan toepassen op dusdanige wijze dat deze aansluit bij de situatie waar bunq zich op dat moment in begeeft. Als je alleen al kijkt naar de functies die vereist zijn: een information security officer, een risk officer, een finance officer, een compliance officer, etcetera. Dit had voor ons het bijkomende gevolg dat we te maken kregen met functiescheidingen (segregation of duties) binnen een heel beperkt team. Dat was dus nogal een klus."

Ga jij bij het uitvoeren van de compliancefunctie zo veel mogelijk uit van de geest van de wet? "Het is altijd een afweging tussen je focussen op de regels of op de cultuur. Ik heb ervoor gekozen om mij op dat laatste te focussen. Ik ben ervan overtuigd dat je daarmee de compliancefunctie veel effectiever kan uitvoeren dan wanneer je reageert met nog meer regels. Wij proberen echt zoveel mogelijk awareness te creëren en mensen zelf te laten nadenken. Een collega van mij vatte dat samen door te zeggen: 'wij hebben hier eigenlijk zeventig compliance officers rondlopen'. Iedereen hier weet wanneer er compliance issues kunnen spelen in hun activiteiten. Dat is veel belangrijker, zo ontwikkel je namelijk een soort 'compliance by design' en hoef je niet te gaan hameren op regels."

Is het ook een voordeel om als compliance officer vanaf nul te beginnen bij een start-up? "Het kan een voor- en nadeel zijn. In een kleine organisatie kent iedereen elkaar en kan je daarom wellicht elkaar makkelijker aanspreken. Uitdagend zijn aan de andere kant weer die checks & balances. Je moet er echt voor zorgen dat de cultuur goed in elkaar zit en daarop verder bouwen. Daarnaast maakt het feit dat we van nature 'disruptive' zijn en de markt willen opschudden het extra spannend."

Gebruik je daarbij de bestaande methodieken, zoals bijvoorbeeld het cultuurhuis? "Wij kijken natuurlijk naar dit soort methodieken. De manier waarop wij cultuur hier ontwikkelen past – als je er van een afstand naar kijkt – in een model zoals het cultuurhuis. Het is vooral belangrijk dat je naar cultuur kijkt met gezond verstand. Bij een start-up is iets als 'uitvoerbaarheid' daarnaast een interessant onderwerp. Het tempo van innovaties ligt hoog, en het is zaak als

> Het feit dat we van nature 'disruptive' zijn en de markt willen opschudden, maakt het extra spannend

compliancefunctie om goed aangehaakt te blijven om de compliancerisico's te kunnen onderkennen en te kunnen mitigeren zonder voor onnodige vertraging te zorgen."

Jij was van het begin af aan betrokken bij bunq. Hoe zorg je dat je niet in de spagaat komt tussen uitvoerbaarheid en de vereiste reflectie op de integriteit van het handelen, van jezelf en van bunq? "Van nature ben ik meer behoudend dan anderen. Ik ben niet voor niets jurist. Dus af en toe loop je inderdaad tegen dingen aan waarvan je weet dat ze niet kunnen. In het uiterste geval moet je dan die 'business killer' zijn. Maar dat gebeurt alleen als er geen alternatieve oplossingen zijn; het streven is om mee te denken in oplossingen. In het algemeen dek ik liever een risico af dan dat ik het accepteer, met name als een toezichthouder nog een eerste indruk moet krijgen. Daarbij is het goed om in gesprek te blijven met de internal auditor, die kritische vragen stelt en je laat leren van fouten. Daarbij legitimeert de internal auditor ook de werkwijze van de compliance officer. Door de toetsing van internal audit kun je aan de business laten zien dat alle belangen zo volledig mogelijk zijn afgewogen."

Mag compliance ook een lerend vermogen hebben, vallen en opstaan? "Ja, dat denk ik wel. Ook compliance maakt afwegingen aan de hand van risico's en geeft daarin een advies. Je loopt als compliance regelmatig tegen nieuwe situaties aan, waarbij je ook wel eens een verkeerde afweging maakt. Risico's zijn soms lastig te definiëren en te kwantificeren. Het gaat er uiteindelijk om dat je fouten door middel van goede monitoring snel kunt herstellen."

En bij dat herstellen focus jij dus op gedrag en cultuur? "Ja absoluut, maar je blijft natuurlijk ook een aantal hard controls nodig hebben. Een voorbeeld daarbij is vereisten aan de zorgplicht richting de klant. Aan de andere kant is die zorgplicht, of het klantbelang centraal stellen ook precies de reden dat bunq is opgericht, waarbij compliance eigenlijk een soort strategie is. Toch moet je bij elke ontwikkeling ook weer toetsen aan de regels die vanuit het productacceptatieproces in de wet staan beschreven. Dat is ook een leerproces voor compliance en moet meegroeien op de manier waarop bunq zelf ook groeit. In ons geval zijn de complianceprocessen zo veel mogelijk 'agile' ingericht."

De Wwft-eisen zijn ook uitgebreid en complex. Hoe richt je dat in bij een start-up? "Gelukkig zie je ook op dit vlak steeds meer technologische ontwikkelingen. Er zijn in het algemeen veel hulpmiddelen die je als compliance kunt gebruiken. Een voorbeeld is daarbij 'big data analytics'. Die data kun je ook gaan gebruiken in het CDD-proces. Daarbij heb je natuurlijk nog het 'harde' identificeren en verifiëren; dit proces is, net als al onze processen, gebaseerd op IT. Wat je vervolgens niet met IT op kan lossen, kun je dan nog handmatig doen."

Denk jij dat compliance in de toekomst steeds meer geautomatiseerd kan worden? "Absoluut, dat is een van de uitdagingen waar compliance officers tegenaan gaan lopen. Als je de processen en de data waarop je toezicht moet houden verder kunt automatiseren en daarbij de juiste 'parameters' kunt ontwikkelen, kun je de compliancefunctie nog veel efficiënter maken."

Frustreert die inefficiëntie jou in het algemeen? "Ja. Compliance is op zich erg interessant, maar het is vaak heel inefficiënt. Bij een start-up – waarbij de focus natuurlijk ligt op alles van begin af aan zo efficiënt mogelijk inrichten – is het niet handig als je maar tegen deze beperkingen aan blijft lopen. Ik denk dat het goed is als hier in de sector meer over gesproken gaat worden. Er ligt heel veel potentieel om de processen en de monitoring te verbeteren en te automatiseren. Dan kan je ook echt focussen op gedrag en cultuur."

Welke competenties heb je in de toekomst volgens jou nog meer nodig als compliance officer? "Dat hangt ervan af. Er is naar mijn mening een verschuiving gaande naar zowel IT als naar meer mogelijkheden om te focussen op gedrag en cultuur. Als je dat splitst, denk ik dat je voor die groepen apart de competenties kunt bepalen. Die IT-compliance officer moet dan in ieder geval verstand hebben van data-analyse en procesmanagement. De gedrag-en-cultuur-compliance officer moet vooral de wet kunnen interpreteren en de link kunnen leggen tussen de cultuur van de organisatie en de geest van de wet. Dat gaat zelfs een beetje richting HR (maar dan in de tweede lijn)."

Denk jij dat het three-lines-of-defence-model een houdbaar model is, gelet op al die verandering in de compliancefunctie? "Ik denk het wel. Er is wel een sceptische kijk op dergelijke modellen, maar het is een valkuil voor compliance om zich te veel in de 'eerste lijn' te begeven. Juist voor start-ups in de financiële sector is

het daarom goed om een dergelijk model te gebruiken. Zo zorg je ook voor het kaderen van bepaalde functies. Je hebt vanuit het model een instrument om je functie mee te beschermen. Je kunt dan zeggen: 'ik ga dit niet doen'."

Ben je wel eens opgestaan met het idee: 'vandaag ga ik zeggen dat ik geen eerste lijn-activiteiten ga uitvoeren'? "(lachend) Ja natuurlijk. Maar dat is vaak ook echt een afspraak die je met jezelf moet maken. Ik vind de IT-kant van bunq ook gewoon erg interessant, dus het is ook wel mijn eigen schuld als ik me daar te veel in meng. Als compliance ook meer gebruik gaat maken van IT en data uit de 'eerste lijn' gaat verzamelen, kan dat er overigens automatisch voor zorgen dat je niet meer in die valkuil loopt. Je kan dan een groot deel van de informatie aangeleverd krijgen die je niet meer in de lijn hoeft op te halen. Overigens wordt het wel interessant wat de rol gaat zijn van HR naarmate je meer met data van medewerkers gaat doen. Het kan zijn dat zij ook automatisch meer naar de tweede lijn verschuiven en daarmee een deel van de compliancetaken over gaan nemen."

Welke compliance- of integriteitrisico's voorzie jij in de toekomst als het gaat om FinTech? "Privacy wordt uiteraard een steeds belangrijker onderwerp. Het gebruik van klantdata voor (commerciële) doeleinden is een lopende discussie. Hoever moet je daarin gaan? Daarnaast voorzie ik ook risico's bij het digitaliseren van het CDD-/KYC-proces. Wanneer iemand één keer fraudeert met zijn/haar identiteit en zich daarmee vervolgens overal kan identificeren, krijg je een soort sneeuwbaleffect van compliancerisico's. Het kan overigens ook zijn dat je identiteit wordt gehackt. Stel dat we straks met alleen Facebook een bankrekening kunnen openen, dan kun je met een nepprofiel een hoop kwaad aanrichten. Je verliest als bank elke vorm van verbinding met de werkelijke klant. Je hebt dus meer data, maar niet per se meer kennis over je klant. Bij big data zie je ook het risico dat een correlatie wordt gezien als een causaal verband. Wanneer je gaat doen aan 'profiling', kun je misschien heel goed kredietrisico's inschatten bij klanten, maar tegelijkertijd kun je er ook compleet de mist mee ingaan. Het stijgende gebruik van data (zij het voor commercieel of non-commercieel gebruik) is een thema waarbij compliance goed het debat kan faciliteren. Wellicht kan compliance daarbij zelfs een soort ombudsman zijn voor de klant (en voor de medewerker, als het om zijn data gaat).
Een ander risico kan zijn dat we, als onderdeel van een grotere keten, bepaalde data moeten eisen van klanten, omdat dat door de organisaties waarmee we in de keten zitten wordt geëist. Als we dat niet doen, zullen we mensen kunnen gaan uitsluiten en dat is onwenselijk. Tegelijkertijd willen we ook staan voor die persoonlijke vrijheid van mensen om een keuze te maken in hoeverre zij hun privacy willen 'opgeven. Vanuit FinTech-perspectief moet je als compliance officer dus eigenlijk ook een soort ethicus zijn als het gaat over de toepassing van data. Met name op het vlak van risicobeheersing, zowel extern als intern. Daarbij kan te veel monitoren van medewerkers en hen op de voet volgen ook een averechts effect hebben. Mensen kunnen het idee krijgen dat de vertrouwensrelatie ondermijnd wordt en gaan proberen die monitoring te ontlopen. Dat is zonde, want vertrouwen zorgt juist voor een meer integriteit-bewuste cultuur. Een mooie kijktip voor de lezers is de serie 'Black Mirror' op Netflix, daar worden dilemma's over data, privacy en profiling mooi neergelegd."

Is het als start-up lastiger om je aan de regels te houden die gemaakt zijn voor een, in bunq's ogen, 'oude werkelijkheid'? "Dat is inderdaad dé uitdaging voor compliance. Meteen vanaf het begin moet de cultuur worden 'neergezet' waarbij die opvattingen helder zijn en in lijn zijn met zowel de geest van de (huidige) regel, als de geest van de start-up. Principle-based regelgeving geeft daar gelukkig wel ruimte in. Ook kan je dan gebruik maken van het comply-or-explain-principe."

Vanuit de toezichthouder is er ook meer toenadering richting FinTech start-ups. Zo hebben ze nu de 'InnovationHub' en 'sandbox' ingericht. In de tijd van bunq was die er niet. Zijn jullie jaloers? "We denken vooral dat we daaraan hebben bijgedragen. Ook voorafgaand aan de oprichting van de InnovationHub en de sandbox was de toezichthouder al erg 'supportive' en wisten ze dat we serieus waren in onze ideeën. Dus we zijn eigenlijk ook wel een beetje trots op deze ontwikkelingen. Die sandbox kan mooi gebruikmaken van de ervaringen met de oprichting van bunq en ondersteunt het idee van disruptie in de financiële sector."

Welke landen moeten we in de gaten houden op compliance-/FinTech-gebied? "Wellicht een minder belicht land op dit gebied is Duitsland. Daar is BaFin een conservatieve speler; als zij iets goedkeuren weet je bijna zeker dat het hier in Nederland ook kan. Een specifiek voorbeeld is 'video onboarding'. Hierover had BaFin twee jaar terug al een mening. Overigens ben ik benieuwd hoe de rol van de toezichthouder zich ontwikkelt in verband met het Europese paspoort."

Zou je nog een boodschap willen meegeven aan compliance officers? "Blijf doorontwikkelen, blijf kijken naar meer efficiëntie voor de compliancefunctie. We zitten op een punt waarop ook binnen compliance disruptie kan plaatsvinden."

De vorderingen in het rentederivatendossier

Ruud van der Mast[1] en Björn Schuitemaker[2]

In de juni-editie[3] van de DCO schetsten wij onze visie op het probleem, het compliancekader en de mogelijke oplossingsrichting in het rentederivatendossier. In de tussentijd heeft de Onafhankelijke Derivatencommissie[4] het Uniform Herstelkader Rentederivaten MKB[5] (verder: herstelkader) opgesteld, is het extern onderzoek naar de rol van AFM afgerond[6] en hebben alle betrokken banken[7] vervolgens het herstelkader geaccepteerd. Dit betekent dat een definitieve oplossing voor handen is voor een complex dossier dat al jaren de gemoederen van mkb-ondernemingen, banken en de AFM bezighoudt.

Hoewel de uitvoering van het herstelkader zich nog in de pilot-fase bevindt, is het in onze optiek aardig om de vorderingen tot dusver te bespreken. Daarvoor zullen wij achtereenvolgend ingaan op de stappen van het herstelkader en de eisen aan de externe beoordelaars en diens plannen van aanpak. Tot slot zullen wij enkele woorden wijden aan de volgende mijlpaal in het rentederivatendossier.

De stappen van het herstelkader

In het herstelkader is voorgeschreven hoe de herbeoordelingen moeten worden uitgevoerd en welke herstelacties in specifieke situaties moeten worden uitgezet om eventuele schades te compenseren en toekomstige schades te voorkomen. Het herstelkader minimaliseert aldus de interpretatieruimte van banken bij de herbeoordelingen, hetgeen zowel het gevolg is van fouten in de herbeoordeling van de banken[8] als het gevolg van fouten in het AFM-toezicht.

Het herstelkader gaat in de basis uit van vier stappen.[9] De eerste stap voorziet in een eenvoudiger alternatief voor bijzonder complexe derivaten. De tweede stap voorziet in een compensatie voor mismatches ten aanzien van de omvang, de looptijd en de modaliteit et cetera. Vervolgens voorziet de derde stap in een generieke coulancevergoeding. Tot slot voorziet de vierde stap in een coulancevergoeding

1 Ruud van der Mast is directeur bij het Nederlands Compliance Instituut.

2 Björn Schuitemaker is jr. compliance officer bij het Nederlands Compliance Instituut.

3 Van der Mast, R., & Schuitermaker, B. (2016). De rentederivaten-problematiek: Het equivalent van de woekerpolissen maar dan voor banken? De Compliane Officer, 22, 8-10.

4 De onafhankelijke Derivatencommissie bestaat uit drie deskundigen die door de minister van Financiën zijn benoemd, te weten: de heren Schimmelpenninck en Knüppe (deskundigen op het terrein van collectieve schadeafwikkeling) en de heer Kocken (deskundige op het terrein van rentederivaten).

5 Knüppe, B.F.M., Kocken, T.P., Schimmelpennick, R.J. (2016). Uniform Herstelkader Rentederivaten MKB. Amsterdam: Onafhankelijke Derivaten Commissie.

6 Alvarez & Marsal. (2016). Onderzoek AFM: Extern onderzoek op AFM toetsing van de herbeoordelingen rentederivaten door banken. Amsterdam: AFM.

7 ABN Amro, Rabobank, ING, SNS, Van Lanschot en Deutsche Bank.

8 Kamerstukken II, 2015-2016, 31311, nr. 166.

9 Knüppe, B. F. M., Kocken, T. P., & Schimmelpenninck, R. J. (2016). Uniform Herstelkader Rentederivaten MKB. Amsterdam: Onafhankelijke Derivatencommissie.

voor onverwachte verhogingen van renteopslagen. Bij de laatste stappen is bewust voor een coulancevergoeding gekozen. Dit omdat het een tijds- en kostenintensieve aangelegenheid is om van geval tot geval te bepalen in hoeverre: a) de ontoereikende informatievoorziening een schending van de zorgplicht oplevert en b) de betreffende ondernemer daardoor schade heeft geleden.[10]

Het herstelkader is met andere woorden geen ex post-beoordeling van de productpassendheid. Dit brengt met zich mee dat het ondernemers vrijstaat om te kiezen of zij de compensatie aanvaarden dan wel een individuele gang naar het tijdelijke Kifid-loket of de rechter maken.

De eisen aan de externe beoordelaars en diens plannen van aanpak

Het herstelkader schrijft een uniforme aanpak voor. Om vervolgens de correcte toepassing van het herstelkader te verzekeren, huren de betrokken banken externe beoordelaars in die aan de selectiecriteria van de AFM voldoen. Deze externe beoordelaars stellen een plan van aanpak op, rapporteren over de voortgang aan de AFM en geven een verklaring af over de kwaliteit van de aangeboden herstelacties.[11] Met deze verklaring geeft de externe beoordelaar aan dat het aangeboden herstel, inclusief de coulancevergoeding, aan het herstelkader voldoet.

De eisen aan de externe beoordelaars

De AFM had graag de externe beoordelaars zelf aangesteld om hun onafhankelijkheid en deskundigheid te waarborgen. Echter, door het ontbreken van een wettelijke bevoegdheid zijn de externe beoordelaars door de banken zelf aangesteld en heeft de AFM een aantal selectiecriteria voor hen opgesteld. Zo moeten de externe beoordelaars over voldoende expertise beschikken en mogen zij:[12]

- niet betrokken zijn bij de eerdere herbeoordeling van individuele rentederivatencontracten;
- vanaf 2012 niet als controlerend accountant van de opdrachtgevende bank hebben geopereerd; en
- niet economisch afhankelijk zijn van de opdrachtgevende bank.

De aangestelde partijen zijn volgens de AFM, op één partij na, allen accountant.[13] Dit is gelet op de stringente voorwaarden aan de aanstellingen opmerkelijk, daar de grote accountantskantoren begin dit jaar nog zijn beboet voor het niet-naleven van de zorgplicht.[14] De betrokken banken zelf wilden (nog) geen informatie prijsgeven over de wijze waarop de opvolging van het herstelkader intern is georganiseerd.

De eisen aan het plan van aanpak

De externe beoordelaars stellen een bankspecifiek plan van aanpak op ter toepassing van het herstelplan en ter borging van de kwaliteit. Aan deze plannen heeft de AFM een aantal eisen gesteld. Zo moeten de plannen omschrijven:[15]

- hoe de dossiercontrole per stap uit het herstelkader is ingericht;
- op welke wijze het vier-ogen-principe wordt toegepast;
- wie de berekening in een individueel dossier accordeert; en
- op welke wijze er met klanten wordt gecommuniceerd.

Vervolg

Met het herstelkader en het aanstellen van externe beoordelaars zijn belangrijke mijlpalen in de rentederivatenproblematiek bereikt. Het herstelkader zit evenwel nog tot eind oktober in de pilot-fase. Dit om bijvoorbeeld na te gaan welke documentatie benodigd is voor het uitvoeren van het herstelkader en waar interpretatieverschillen tussen de banken in gelijkaardige dossiers zitten.[16] Na deze fase zal het definitieve herstelkader door de Onafhankelijke Derivatencommissie worden gepubliceerd en kunnen de betrokken banken starten met het herstellen van de eventuele schades uit het verleden en mogelijke schades in de toekomst. De verwachting is dat medio 2017 alle dossiers zijn getoetst aan het herstelkader en de klanten dienovereenkomstig zijn gecompenseerd.

10 Kamerstukken II, 2015-2016, 31 311, nr. 175.

11 Kamerstukken II, 2015-2016, 31 311, nr. 175.

12 Kamerstukken II, 2015-2016, 31 311, nr. 175.

13 AFM. (2016). Position Paper van de Autoriteit Financiële Markten voor de ronde tafel inzake rentederivaten op 27 september 2016.

14 AFM (2016). Geraadpleegd op 7 november 2016, van: www.afm.nl/nl-nl/professionals/nieuws/2016/mrt/boete-big4.

15 Kamerstukken II, 2015-2016, 31 311, nr. 175.

16 Kamerstukken II, 2015-2016, 31 311, nr. 175.

Bijeenkomst NVB: FinTech en compliance-(risico's)

Roderick Noordhoek

"Het onderwerp FinTech is hot in de sector, maar of dit ook onder compliance officers geldt…" Dat was de vraag van de NVB toen zij samen met het Nederlands Compliance Instituut de bijeenkomst 'FinTech en compliance(risico's)' organiseerde. Wat blijkt? Compliance officers hebben helemaal geen keuze. Ze moeten mee! Een verslag van deze bijeenkomst.

FinTech

Don Ginsel (Holland FinTech) trapte de, door vijftig compliance officers bezochte, FinTech-middag af en beantwoordde direct de vraag: wat is FinTech? Don stelt dat het draait om een onderdeel van een andere beweging, namelijk innovatie. *"En dat doen we in de financiële sector al eeuwen."* Een van de beste innovaties binnen de sector is volgens Don de beurs. *"Door innovatie ontstond standaardisatie en dat heeft de hele aandelenhandel mogelijk gemaakt."* Wat je nu ziet is dat hiervoor technologie wordt gebruikt die het mogelijk maakt om verder te innoveren. En dat is niet iets van de laatste twee jaar. Zo is mobiel bankieren al heel lang mogelijk en dat valt ook onder FinTech. *"We hebben er nu alleen een naam voor verzonnen."* Volgens Don doet Nederland het op dit gebied overigens heel goed en kunnen we internationaal meekomen. Nadat FinTech gedefinieerd werd, ging hij verder met voorbeelden van technologische innovatie ten behoeve van de compliancefunctie. Met name op het gebied van risicobeheersing en CDD zijn er steeds meer partijen die technologische oplossingen aanbieden.

Verder zette Don vraagtekens bij hoever we moeten gaan met technologie. *"Iedereen focust nu sterk op blockchain, maar we moeten niet vergeten dat dit systeem voorlopig heel erg traag is."* Zijn visie over de toekomst: steeds meer niet-gereguleerde partijen gaan aanhaken bij gereguleerde partijen. Op dit vlak ziet Don een groot risico voor data-beveiliging. Ook ziet hij PSD2 als ontwikkeling die zorgt voor meer partijen die actief betrokken raken bij de financiële sector. Hij waarschuwt dan ook de toezicht-houders dat zij hierop voorbereid moeten zijn.

Blockchain

Om blockchain beter te begrijpen was Chris Huls (Rabobank) uitgenodigd. Hij schreef zijn scriptie over scenario's waarin blockchain kan worden toegepast en wist er meer dan één miljoen te verzinnen. Daarna kon hij direct als expert aan de slag bij Rabobank, waar hij nu verschillende blockchain-projecten heeft opgezet. Na zijn toelichting op blockchain lichtte Chris toe dat hij er heel lang over had gedaan om de techniek te begrijpen; dit ter opluchting van sommige compliance officers. Tegelijk gaf hij aan dat er ook voor compliance veel voordelen te behalen zijn met blockchain. Met name op het gebied van de identificatie en verificatie van klanten.

Toezicht op technologische ontwikkelingen

Namens de AFM gaf Mirèl ter Braak toelichting op de wijze waarop de AFM omgaat met deze innovaties en hoe zij in een spagaat zitten tussen het ondersteunen van nieuwkomers in de sector versus het behouden van een level playing field voor de bestaande partijen. Hier kwamen veel vragen over. Met name het gebruik van een sandbox doet in dat opzicht veel stof opwaaien. De sandbox is een onderdeel van de InnovationHub die is opgezet in samenwerking met DNB. De sandbox is een testomgeving die gecontroleerd wordt door de toezichthouder en waarin innovatieve bedrijfsmodellen en productinnovaties getest kunnen worden. Mirèl beschreef vervolgens ook het internationale toezichthoudersspectrum. Daarbij gaf zij aan dat de AFM nauw samenwerkt met onder andere de Engelse toezichthouder FCA, die in het algemeen als een van de voorlopers wordt gezien op dit vlak.

Witwasrisico's

Inhoudelijk werd de middag afgesloten door Rutger de Doelder van de Erasmus Universiteit. Hij presenteerde zijn visie over de witwasrisico's die de FinTech-ontwikkelingen met zich meebrengen. De rode draad hierin is dat het voor start-ups van belang is dat zij een bepaalde 'basishygiëne' hebben ten aanzien van integriteit. Hoewel het gaat over niet-gereguleerde ondernemingen is het voor hen ook cruciaal voor de continuïteit om niet in aanraking te komen met witwaspraktijken, ongeacht welke wet- en regelgeving er van toepassing is. Ook de onder toezicht staande instellingen in de financiële sector moeten zich beseffen dat deze basishygiëne op orde is bij FinTech-partijen waarmee zij in aanraking komen. Middels een aantal praktijkvoorbeelden over betalingsverkeer, de bitcoin en kredietverlening schetste Rutger een aantal specifieke, nieuwe compliancerisico's, zoals de handel in cryptocurrency en verschuivingen in de verantwoordelijkheid bij het uitvoeren van CDD-onderzoek. Ook gaf hij drie manieren weer waarop banken hiermee in aanraking kunnen komen: als onderdeel van de keten, wanneer FinTech-start-ups klant worden en wanneer bestaande klanten misbruik maken van FinTech.

Tot slot voorziet Rutger nog een aantal voorspellingen:

1. Een verbreding van de reikwijdte van de Wwft, bijvoorbeeld door bitcoin exchange onder toezicht te laten vallen.
2. Het opnieuw definiëren van geld of synoniemen in de wet.
3. Een verbod op anonieme betalingen.

Met onder andere deze maatregelen denkt Rutger dat de basishygiënenorm kan worden bereikt.

De middag werd afgesloten met een borrel waarbij een ieder zijn/haar visie over de toekomst (van compliance) met elkaar deelde. De NVB gaf aan open te staan voor suggesties op dit thema om meer voor compliance bij de banken te betekenen.

Roderick Noordhoek is voorzitter van het Young Compliance Professional-netwerk en is werkzaam bij het Nederlands Compliance Instituut als junior compliance officer. Dit artikel is op persoonlijke titel geschreven.

Speakers' Corner: Jan Willem Taams

Keurmerkdynamiek bij trustkantoren

Holland Quaestor heeft voor trustkantoren die lid zijn van deze branchevereniging een keurmerk verplicht gesteld. Dit keurmerk is ondergebracht bij de onafhankelijke Stichting AQTO. De eerste eenentwintig keurmerken zijn uitgereikt op de dag dat de Panama Papers werden gepubliceerd. Ondertussen heeft De Nederlandsche Bank (DNB) haar zorgen uitgesproken over vier trustkantoren aan wie het keurmerk is toegekend. Bovendien ligt de trustsector onder het vergrootglas van de politiek en de media. Dynamiek in overvloed in een sector die bij voorkeur discreet haar cliënten bedient. Tijd voor een tussenstand, na ruim anderhalf jaar keurmerk.

DNB en het HQ-keurmerk

'Zonder wrijving geen glans' is het gezegde. En dat geldt ook voor het keurmerk van Holland Quaestor. Het aantal leden van Holland Quaestor is sinds de introductie van het keurmerk teruggelopen van zevenenvijftig naar drieënveertig leden. Reden van opzegging varieert van fusie en overname tot het niet kunnen of willen voldoen aan de keurmerkcriteria en de steeds hogere compliancekosten. Niettemin werden op 4 april 2016 de eerste eenentwintig keurmerken uitgereikt aan leden van Holland Quaestor. Dat proces is niet zonder slag of stoot verlopen. 'Zonder wrijving geen glans' bleek ook tijdens het seminar van DNB voor alle trustkantoren in Nederland, dat precies vijftig dagen na de eerste uitreiking van de keurmerken door DNB werd georganiseerd. Directeur Frank Elderson hield daar een toespraak. Hij was in het eerste gedeelte complimenteus over de initiatieven van Holland Quaestor. Even later deelde Frank Elderson mede dat DNB grote zorgen heeft over tenminste vier van de trustkantoren waaraan inmiddels een keurmerk is verleend. Hij vervolgde: *"Mocht het zover komen dat wij ons genoodzaakt zouden zien formele maatregelen op te leggen aan één of meer kantoren met een keurmerk, dan komt hiermee het 'Huis van het Keurmerk' in een geheel ander daglicht te staan."* Over zonder wrijving geen glans, gesproken!

De trustsector kent circa honderdvijfenveertig partijen met een Wtt-vergunning. Holland Quaestor heeft per 1 juli 2016, drieënveertig leden met circa 75% marktvolume. Vanaf 1 januari 2017 dienen alle leden van Holland Quaestor verplicht te beschikken over het keurmerk. Integriteit vormt de rode draad van het keurmerkhuis waarin de keurmerkcriteria zijn vastgelegd. Naast compliancecriteria nemen criteria gericht op gedrag & cultuur een essentiële plek in. De trustkantoren met een keurmerk worden om het jaar gevisiteerd door van buiten de trustsector afkomstige visiteurs van Stichting AQTO (Assured Quality & Trustworthy Organisations). Het bestuur van Stichting AQTO opereert volledig autonoom bij de toekenning van de keurmerken. Dit is vastgelegd in de statuten, waaruit onder andere blijkt dat drie van de vijf bestuursleden afkomstig zijn van buiten de trustsector. Bestuurders van Stichting AQTO kunnen ook niet werkzaam zijn bij een trustkantoor.

> Het zijn niet de sterkste of slimste trustkantoren die overleven, maar die zich het beste aanpassen aan de omstandigheden

Doelstelling van het HQ-keurmerk:
- Verhoging van professionaliteit primair bij de leden van Holland Quaestor.
- Objectieve borging van kwaliteit.
- Vergroten geloofwaardigheid leden van Holland Quaestor bij belanghebbenden.
- Bewustwording structurele verandering trustsector.

De grote zorgen over deze vier trustkantoren zijn tot op heden niet concreet gemaakt door DNB. Waarom sprak Frank Elderson deze woorden dan over een keurmerk dat ook DNB belangrijk vindt? Het is aannemelijk dat DNB, ondanks het goede keurmerkinitiatief, de druk op de ketel wil blijven houden met betrekking tot het veranderingsproces dat gaande is in de trustsector. Veranderingen die lang niet door iedereen worden omarmd. In de trustsector zijn veel ondernemers actief die een minimum aan regelgeving prefereren, terwijl sommigen zich niet eens altijd aan deze regelgeving houden. Hiermee heeft de trustsector 'de tucht' van DNB over zich afgeroepen in een tijd dat ook DNB zich weinig fouten kan permitteren. Al met al een delicate combinatie die er mede toe heeft geleid dat de woorden van Frank Elderson als vanzelfsprekend direct werden overgenomen in het FD met de kop: *"Ook twijfels over trustkantoren met een keurmerk"*.

Is dit erg? Het antwoord luidt volmondig: *"nee"*. Is dit vervelend? Het antwoord luidt volmondig: *"ja"*. Het leidt immers af van het proces van verandering dat in gang is gezet door de leden van Holland Quaestor. Daar dient de volle aandacht en energie naar toe te gaan. DNB zal inhoudelijk natuurlijk terechte kritiek hebben; er is geen reden daar op voorhand aan te twijfelen. De toezichthouder heeft absoluut gelijk dat het bij een aantal kantoren beter zal moeten. En voor leden van Holland Quaestor die wel forse inspanningen plegen om de kwaliteit en professionaliteit te verhogen, is dat niet leuk om te lezen en/of te horen. Dat hoort ook bij een proces van verandering.

'Three lines of defence' en het HQ-keurmerk

De bevindingen van DNB komen voort uit zijn toezichtonderzoeken. Vaststellen van de juiste opzet, het tijdige bestaan en de volledige werking van de interne werkwijzen met betrekking tot dossiers van cliënten van trustkantoren is het doel. De uitkomsten van deze dossieronderzoeken van DNB kunnen dus ook de kwaliteit van het keurmerk raken. Hoe borgt Stichting AQTO de risico's van haar keurmerk op dit gebied? De visiteurs van Stichting AQTO mitigeren deze risico's door beoordeling van het 'three lines of defence'-model bij het betreffende trustkantoor, waarbij in de eerste plaats lijnmanagement verantwoordelijk is voor de dossiers van de doelvennootschappen. In de tweede plaats toetst de compliancefunctie of beleid en uitvoering van de dossiers deugt. Tot slot beoordeelt de RIB-auditfunctie, gebaseerd op de Regeling Integere Bedrijfsvoering, de effectiviteit van de organisatie-inrichting, de effectiviteit van de procedures en maatregelen en de effectiviteit van de compliancefunctie, mede in relatie tot de dossiers van cliënten van trustkantoren. De visiteurs van Stichting AQTO maken daarnaast gebruik van de eerder genoemde onderzoeksrapporten van DNB, die ook wel de 'fourth line of defence' wordt genoemd. Stichting AQTO steunt dus naast haar eigen werkzaamheden, gericht op de beoordeling van de keurmerkcriteria, op de eerder genoemde functies mits zij heeft kunnen vaststellen dat iedere functie zijn verantwoordelijkheid neemt.
In de afgelopen periode heeft de trustsector de compliancefunctie redelijk geaccepteerd en is het voor de trustsector wennen aan de, in 2015 geïntroduceerde, RIB-auditfunctie. De wetgever heeft zich beperkt in haar uitwerking van de RIB-auditfunctie. Ook de Q&A van DNB maakt onvoldoende duidelijk waar een RIB-audit precies aan dient te voldoen, los van onafhankelijkheid. Holland

Zonder wrijving geen glans; dat geldt ook voor het keurmerk van Holland Quaestor

Quaestor heeft deze lacune ingevuld door een brochure op te stellen die richtinggevend is voor leden van Holland Quaestor. Met betrekking tot de RIB-audit zal nog het nodige water door de Rijn dienen te stromen, voordat is uitgekristalliseerd wat verwacht mag en kan worden van de RIB-auditfunctie en de wijze van rapporteren aan het trustkantoor, mede ten behoeve van het keurmerk.
Ook DNB laat zich niet onbetuigd over de RIB-audit en heeft een themaonderzoek in gang gezet, waarbij als eerste stap self assessments zijn gestuurd naar trustkantoren. De uitkomsten volgen in de loop van 2017 en leiden ongetwijfeld tot 'guidance' en opbouwende kritiek van de toezichthouder.

Evaluatie en het HQ-keurmerk

Na een jaar keurmerk heeft een grondige evaluatie plaatsgevonden. De conclusie luidt dat het keurmerk een passend instrument is om de leden van Holland Quaestor te ondersteunen in hun proces van ontwikkeling naar trustkantoren met een kwalitatief goede werkwijze en een geïnternaliseerde integere cultuur. Het is dus niet zo, zoals Marcel Pheijffer in zijn prikkelende column in het FD suggereerde, dat het automatisch goed zit bij een trustkantoor dat lid is van Holland Quaestor omdat een gedragscode en een keurmerk van toepassing zijn. Regels maken en vaststellen wil niet zeggen dat het gedrag daarmee is veranderd. Iedereen weet dat gedragsverandering de meest complexe verandering is die er bestaat. Beleidsplan, gedragscode en keurmerk zijn geen garantie voor een geïnternaliseerde integere cultuur.
De kunst is van regels naar gedrag te groeien en dat vraagt tijd. Tijd die de trustsector weinig meer wordt gegund. Politiek, toezichthouder en samenleving zijn (terecht of onterecht) ongeduldig. Het is alleen de trustsector zelf die dit kan veranderen. Bij de leden van Holland Quaestor is het bewustzijn ontstaan dat zij de hand in eigen boezem dient te steken. Daarbij dienen ook de handen uit de mouwen te worden gestoken, niet alleen om cliënten te bedienen, maar vooral ook om de cliënten te bedienen conform de geldende wetten, waarden, normen en opvattingen die leven en van toepassing zijn in Nederland. *"Dames en heren, u bent er nog niet. U bent er, als u mij toestaat, nog lang niet. De tijd dit onder ogen te zien is nu. Ontkenning is geen goede strategie"*, om nog maar eens een quote aan te halen van Frank Elderson.

De leden van Holland Quaestor weten dat. Dit is ook de reden voor een substantiële verzwaring van de eisen van het HQ-keurmerk. Naast de update van de essentiële compliancecriteria is tevens fiscale en morele ethiek een voorwaardelijk criterium geworden voor het (opnieuw) toekennen van het keurmerk, evenals de criteria voor maatschappelijk verantwoord ondernemen. Daarnaast is de normering significant aangescherpt en hebben actuele ontwikkelingen, zoals 'error management' een plek gekregen in het keurmerk 2.0. Op deze manier creëren de leden van Holland Quaestor hun eigen hoge druk om te ontwikkelen naar een geïnternaliseerde integere cultuur. Ook dat zal niet vanzelf gaan. Dat vraagt substantiële bijdragen in tijd, geld, energie en aandacht van alle mensen die werkzaam zijn bij de leden van Holland Quaestor. De vertaling van regels naar gedrag is de opdracht. Dat kan alleen door dicht bij de mensen te staan die in de trustsector werken. De missie van deze mensen is de transitie van fiscaal gedreven trustkantoren naar trustkantoren die in brede zin bijdragen aan het vestigingsklimaat van Nederland. Deze transitie, met de daarbij behorende geïnternaliseerde integere cultuur, is een boeiende opdracht die onder andere slaagt door complexe zaken eenvoudig te maken. Ondernemende trustkantoren kunnen dat als geen ander. Ieder trustkantoor heeft daarbij gelijke kansen, want parafraserend op Darwin: *"Het zijn niet de sterkste of slimste trustkantoren die overleven maar die zich het beste aanpassen aan de omstandigheden."*

Jan Willem Taams is partner/inspirator van bestuurskamers. Hij was afkomstig van buiten de trustsector voordat hij bruggenbouwer en kwartiermaker werd bij Holland Quaestor in relatie tot de ontwikkeling van het HQ-keurmerk. Daarna is hij door het bestuur van Stichting AQTO benoemd als kwartiermaker van deze stichting tot 1 juli 2016. Deze publicatie is geschreven op persoonlijke titel.

Compliance highlight: u kunt stemmen voor de Nationale Compliance Award

Het Nederlands Compliance Instituut kent jaarlijks de Nationale Compliance Award toe aan de persoon of de instelling die zich bijzonder verdienstelijk heeft gemaakt voor het vakgebied compliance en de professionalisering van de compliancefunctie in het bijzonder.

Van 5 januari tot en met 20 januari kunt u uw stem uitbrengen op één van de genomineerden via: **www.compliance-instituut.nl/over-ons/compliance-award**

10 januari	LCP Module 4 - groep 5 (dag 1)
11 en 12 januari	LCP Module 2 - groep 1
7 februari	LCP Module 4 - groep 5 (dag 2)
8 februari	LCOZ Module 1
14 en 15 februari	LCP Module 5 - groep 5
14, 15 en 16 februari	LCP Module 3 - groep 1
7 maart	Competentietraining - groep 1
7 maart	Compliance & Integriteit voor HR-professionals (dag 1)
8 en 9 maart	LCP Module 2 - groep 2
16 maart	Introductie Compliance
16 maart	LCP Module 4 - groep 1 (dag 1)
16 maart	Compliance & Integriteit voor HR-professionals (dag 2)
21 maart	LBW Module 2
23 maart	LCOZ Module 3
23 maart	Toezichtrecht voor niet-juristen
28 maart	LBW Module 3
29 en 30 maart	Opleiding Privacy Officer
4 april	LBW Module 4
12 april	LCOZ Module 4
13 april	LCP Module 4 - groep 1 (dag 2)
18, 19 en 20 april	LCP Module 3 - groep 2
20 april	LCOZ Module 5
9 mei	Masterclass Soft Controls (dag 1)
16 en 17 mei	LCP Module 2 - groep 4
17 mei	LCP Module 4 - groep 2 (dag 1)

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

Jaarboek Compliance 2017

De nieuwe editie is verschenen!

Gedrag en cultuur

Ontwikkelingen in de compliancepraktijk

Ontwikkelingen in wet- en regelgeving

Nederlands compliance Instituut

Leading in compliance