**Circulaire CBFA_2009_17 dd. 7 april 2009**

## Financiële diensten via het Internet : prudentiële vereisten

***Toepassingsveld :***

Kredietinstellingen, verzekeringsondernemingen, beleggingsondernemingen en beheervennootschappen van instellingen voor collectieve belegging naar Belgisch recht en de Belgische bijkantoren van deze instellingen die ressorteren onder het recht van een staat die geen lid is van de Europees Economische Ruimte (EER).
De circulaire wordt tevens ter kennis gebracht aan de in België gevestigde instellingen die ressorteren onder een lidstaat van de EER.

***Samenvatting/Doelstelling :***

In een eerste deel worden de basisprincipes besproken die als referentiekader dienen voor de CBFA bij de beoordeling van de passende organisatie van financiële instellingen die hun diensten aanbieden via het Internet. Meer bepaald worden de risico's toegelicht evenals de vereisten inzake organisatie en interne controle. Verder wordt de naleving van de gedragsregels onder de aandacht gebracht evenals de mogelijke impact van het grensoverschrijdende verkeer via Internet.
In een tweede deel dat als bijlage gaat aan het eerste deel wordt specifiek aandacht besteed aan de gezonde praktijken inzake het beheer van de Internetbeveiligingsrisico's.

Geachte mevrouw,
Geachte heer,

### 1. Verantwoording

Kredietinstellingen, verzekeringsondernemingen, beleggingsondernemingen en beheervennootschappen van instellingen voor collectieve belegging, hierna gezamenlijk aangeduid met de "financiële instellingen", moeten beschikken over een voor hun activiteit passende organisatie[1].

Tal van deze financiële instellingen bieden financiële diensten aan via het Internet, waarbij cliënten de mogelijkheid wordt geboden informatie op te vragen, verrichtingen uit te voeren en te communiceren met hun instelling.

Deze circulaire geeft een aantal aanbevelingen en duiding bij de belangrijkste bepalingen uit het bestaande reglementaire en prudentiële kader die specifiek toepassing vinden op de financiële dienstverlening via Internet.

Deze aanbevelingen zijn mee geïnspireerd op een aantal internationale standaarden[2] inzake risk management die als referentiekader voor de Belgisch praktijk van nut kunnen zijn.

[1] Zie artikelen 20 en 20bis van de wet van 22 maart 1993 (kredietinstellingen), artikel 14bis van de wet van 9 juli 1975 (verzekeringsondernemingen), artikelen 62 en 62bis van de wet van 6 april 1995 (beleggingsondernemingen). Voor de beheervennootschappen van instellingen voor collectieve belegging wordt verwezen naar artikel 153 van de wet van 20 juli 2004 betreffende bepaalde vormen van collectief beheer van beleggingsportefeuilles.

In een afzonderlijke bijlage wordt specifiek ingegaan op de goede beheerspraktijken inzake het beheer van de beveiligingrisico's verbonden aan de financiële dienstverlening over het Internet.

De circulaire D1 2000/2 van de CBF van 5 mei 2000 inzake financiële diensten via het Internet die gericht was aan de kredietinstellingen en de beleggingsondernemingen wordt opgeheven.

## 2. Toepassingsgebied

### A. Ratione personae

De gezonde beheerspraktijken zijn van toepassing op de kredietinstellingen, de verzekeringsondernemingen, de beleggingsondernemingen en beheervennootschappen van instellingen voor collectieve belegging naar Belgisch recht.

Ze zijn ook van toepassing op de Belgische bijkantoren van kredietinstellingen, verzekeringsondernemingen, beleggingsondernemingen en beheervennootschappen van instellingen voor collectieve belegging, die ressorteren onder het recht van een staat die geen lid is van de EER.

Onverminderd de bevoegdheden van de toezichthouders van het land van herkomst wat het toezicht op de organisatie en de interne controle betreft, wordt het tevens nuttig geacht de aanbevelingen van deze circulaire ter kennis te brengen van de bijkantoren van financiële instellingen onder het recht van andere staten van de EER. Zij zullen als referentie dienen bij het toezicht van de CBFA op deze kantoren.

### B. Ratione materiae

De prudentiële vereisten slaan zowel op de informatie- en adviesverstrekking via het Internet, als op de Internetdiensten die de financiële instellingen aan hun cliënten aanbieden om hun gegevens te consulteren en/of te beheren en verrichtingen uit te voeren.

Financiële instellingen maken hiervoor meestal gebruik van verschillende soorten websites. Zo heeft men naast louter informatieve websites met gegevens over de financiële instelling, zijn diensten- en productenaanbod, en interactieve websites met educatieve en simulatiefuncties, ook transactionele websites die het mogelijk maken financiële diensten te verrichten, zoals geld overschrijven, betalingen doen, kredieten aangaan, verzekeringspolissen onderschrijven, informatie te beheren of beleggingsinstrumenten te kopen of te verkopen.

Financiële Internetdiensten hebben als kenmerk dat de communicatie tussen de cliënten en hun financiële instelling voor het raadplegen van informatie, het consulteren van de cliëntensituatie en het afwikkelen van verrichtingen, via het Internet gebeurt. Daarbij wordt de Internetdienstverlening meestal en steeds meer, van het begin tot het einde, volledig automatisch uitgevoerd (*straight through processing*) zonder menselijke controles waardoor het van essentieel belang is dat de nodige interne (identificatie van de cliënt, stand van de rekeningen, bezit van de verkochte effecten, limieten, …) en externe controles (conformiteit van de verrichting met de regels van de beurs of de betalingsinfrastructuur waarvoor hij bestemd is) in de Internetdiensten worden ingebouwd. Deze noodzaak wordt nog versterkt door de evolutie om alsmaar meer verrichtingen zoals beurs- en betalingsverrichtingen in *real time* uit te voeren, waardoor de beschikbare tijd om controles uit te voeren uiterst beperkt is.

Omwille van de eraan verbonden risico's, zijn het inzonderheid de transactionele Internetdiensten die vanuit prudentieel oogpunt de meeste aandacht verdienen.

---

[2] "Risk Management Principles for Electronic Banking", "Electronic Banking Group of the Basel Committee on Banking Supervision", July 2003 and Management and Supervision of Cross-Border Electronic Banking Activities, Electronic Banking Group of the Basel Committee on Banking Supervision, July 2003.

## 3. Prudentiele vereisten

### A. Uitgangspunten en risico's verbonden aan het verrichten van financiële diensten over het Internet

De financiële instellingen die financiële diensten aanbieden of verrichten via het Internet, dienen in het algemeen - net zoals bij de aanwending van andere distributiekanalen - alle wettelijke en reglementaire bepalingen na te leven die op deze verrichtingen van toepassing zijn.

Bovendien moeten deze instellingen ook over een passende structuur en organisatie beschikken, alsook over controle- en beveiligingsvoorzieningen op het gebied van de elektronische informatieverwerking en adequate interne controleprocedures om de specifieke risico's verbonden aan het gebruik van het Internet op een passende wijze te dekken.

Deze risico's - waarvan de realisatie een belangrijke weerslag kan hebben op de financiële positie en reputatie van de instelling - hebben onder meer betrekking op :

a) ***juridische risico's*** : het aanwenden van het Internet voor haar dienstverlening noopt de instelling tot het onderzoeken van een reeks (soms nieuwe) juridische situaties in België of in het buitenland, waarvoor een passende omkadering noodzakelijk is, terwijl het wettelijke of reglementaire kader in voorkomend geval geheel nieuw, onzeker, onvolledig dan wel onbestaande is ;

b) ***operationele risico's :*** de aanwending van het Internet bij de dienstverlening veronderstelt aangepaste informatica- en beveiligingssystemen en procedures voor de opvolging van de cliëntenverrichtingen of prestaties door derde dienstverleners, door de medewerkers van de instelling, die daartoe moeten worden opgeleid ;

c) ***reputatierisico's :*** de instelling kan reputatieschade lijden wanneer haar dienstverlening over het Internet gebrekkig, onveilig of onbetrouwbaar is, niet aan de verwachtingen van de gebruikers en het publiek voldoet, dan wel lacunes vertoont of inbreuken inhoudt op het vlak van de Belgische en/of buitenlandse wettelijke en reglementaire bepalingen ter zake.

### B. Vereisten inzake organisatie en interne controle

#### 1. Algemeen

Alvorens informatie of diensten aan te bieden over het Internet, moet de financiële instelling de hieraan gebonden risico's in kaart brengen en haar organisatie en interne controles hieraan aanpassen en waar nodig testen. Daarbij dient rekening gehouden te worden met de aard van de aangeboden diensten, de complexiteit en de omvang ervan.

Hierna worden de prudentiële verwachtingen toegelicht. Deze hebben onder meer betrekking op het algemene beleid van de instelling, alsook op de specifieke aspecten van de organisatie inzake het Internetaanbod, zoals de juridische en de operationele omkadering van de activiteit, de beveiliging, de gebeurlijke rol van tussenpersonen, de identificatie en authentificatie van de cliënten, outsourcing en audit trails.

#### 2. Beleidsaspecten

De effectieve leiding, in voorkomend geval het directiecomité, is verantwoordelijk voor de uitwerking van een beleid en een strategie inzake het verstrekken van diensten via het Internet en voor de organisatie en opvolging ervan. Dit beleid wordt aan het wettelijke bestuursorgaan ter goedkeuring voorgelegd. In het kader van dit beleid kunnen volgende aandachtspunten worden vermeld :

a) vastleggen van een algemeen, financieel en commercieel beleid ;

b) vastleggen van de marketingdoelstellingen en de inhoud van de website ;

c) vastleggen van de technische doelstellingen en opties op het vlak van de beveiliging zoals verder uiteengezet in de bijlage aan deze circulaire ;

d) vastleggen van het risicobeheer en de implicatie van de verschillende controleniveaus van de instelling (interne controle, interne audit, revisor) ;

e) vastleggen van de interne rapporteringsvereisten waarbij rekening wordt gehouden met de risico's en met de waargenomen bedreigingen en beveiligingsincidenten ;

f) onderzoek naar en beheersing van de juridische implicaties en risico's ;

g) vastleggen van de middelen en de procedures inzake het bewaren van de gegevens ;

h) de afstemming van het interne controlesysteem op de organisatie van de dienstverlening via het Internet.

De interne auditfunctie neemt de werking en de toepassing van het Internetbeleid op in haar auditplanning en -werkzaamheden en evalueert die. Daartoe worden passende auditprogramma's en -technieken ingezet.

De activiteit wordt opgenomen in de jaarlijkse verslaggeving van de effectieve leiding inzake de beoordeling van het interne controlesysteem[3]**.**

## 3. Contractuele relaties

De financiële instellingen die hun cliënten toelaten hun gegevens te consulteren, te beheren en verrichtingen uit te voeren via het Internet, sluiten ter zake voorafgaand een overeenkomst af met hun cliënten. Een dergelijke specifieke overeenkomst is niet nodig voor een louter informatieve website waar er geen gepersonaliseerde gegevens kunnen geconsulteerd worden.

In deze overeenkomst dient naast de omschrijving van de aard en de draagwijdte van de dienstverlening, tevens aandacht besteed te worden aan de specifieke omkadering en modaliteiten eigen aan het gebruik van het Internet. Zo dient er onder meer aandacht besteed te worden aan een precieze beschrijving en aflijning van de verantwoordelijkheden van de partijen bij het gebruik van de door de instelling ter beschikking gestelde of aanbevolen technologieën om de cliënt te identificeren en te authentificeren en de verrichtingen te valideren.

De naleving van de wetgeving inzake het voorkomen van witwassen impliceert bovendien dat de instelling de uitvoering van transacties voor rekening van een cliënt moet kunnen opschorten voor een regelmatigheidscontrole en/of moet kunnen weigeren. Verder dient er tevens aandacht besteed te worden aan een passende overeenkomst indien er voor het aanbieden, ontwikkelen, beheren of ondersteunen van de websites en Internetdiensten, beroep wordt gedaan op leveranciers, alsook met de tegenpartijen en de al dan niet gereglementeerde markten die worden betrokken in de Internetdienstverlening.

## 4. Beveiliging

Financiële instellingen die het Internet gebruiken voor hun dienstverlening worden geconfronteerd met diverse beveiligingsrisico's.

In bijlage wordt een overzicht gegeven van de gezonde beheerspraktijken waarvan de CBFA verwacht dat de financiële instellingen zich hiernaar zullen richten in de aanpassing van hun beveiligingsplannen. Deze gezonde beheerspraktijken maken een onderscheid tussen aandachtspunten en aanbevelingen die verband houden met de beveiliging van :

- de eigen informatica-infrastructuur (interne computerinfrastructuur, firewalls, mail- en webservers, …) tegen bedreigingen van het Internet, enerzijds en ;

[3] Zie Circulaire CBFA_2008_12 dd. 9 mei 2008 inzake de verslaggeving van de effectieve leiding inzake de beoordeling van het interne controlesysteem en de verklaring van de effectieve leiding inzake de prudentiële periodieke rapportering.

- financiële verrichtingen, raadplegingen en beheersdaden over het Internet, anderzijds.

De gezonde beheerspraktijken zijn relevant voor zowel grote als kleine instellingen, hoewel de karakteristieken van de aangeboden Internetdiensten en de bedreigingen kunnen verschillen van instelling tot instelling. De financiële instellingen worden geacht de gezonde beheerspraktijken na te leven of afwijkingen ervan aan de CBFA toe te lichten (*comply or explain*).

De financiële instellingen worden verzocht :
- een delta-analyse uit te voeren tussen hun (interne) organisatie van de Internetactiviteiten en de richtlijnen opgenomen in de bijlage aan deze circulaire;
- een planning op te stellen op het vlak van de benodigde werkzaamheden en middelen.

De belangrijkste conclusies van deze delta-analyse samen met de planning worden tegen uiterlijk **31 augustus 2009** aan de CBFA bezorgd. Hierbij worden tevens alle afwijkingen van de gezonde beheersprincipes in de bijlage aan de circulaire, die de instelling aanvaardbaar acht, op een adequate wijze onderbouwd en toegelicht (*comply or explain*).

Voor financiële instellingen die deel uitmaken van een groep, kan de groepsdimensie een belangrijke rol spelen in de concrete invulling van het beveiligingsbeleid voor de Internetdiensten. De instelling moet in dergelijk geval aantonen dat de groepsgewijze organisatie geen afbreuk doet aan de deugdelijkheid van haar beveiligingsbeleid en –maatregelen.

De CBFA verwacht dat ze onverwijld geïnformeerd wordt over risicovolle incidenten waarbij derden er via het Internet effectief in slagen om de beveiliging van de Internetdiensten of de eigen informatica-infrastructuur te omzeilen.

## 5. Operationele aspecten - beschikbaarheid, continuïteit en correct verloop van de verrichtingen

Een hoge beschikbaarheid is een belangrijke en voor de buitenwereld zeer zichtbare maatstaf voor de kwaliteit en betrouwbaarheid van de aangeboden websites en Internetdiensten. De instelling bepaalt ter zake de nagestreefde beschikbaarheidsdoelstellingen en zorgt ervoor dat de hiervoor benodigde organisatorische en technische maatregelen worden ingevuld. De instelling beschikt in dit verband onder andere over een aangepast incidentbeheer om eventuele storingen van de websites en Internetdiensten binnen de vooropgestelde (tijds- en kwaliteits-) objectieven te herstellen.

In functie van de aard en het belang van de aangeboden websites en Internetdiensten en de beoogde continuïteitsobjectieven beschikt de instelling tevens over aangepaste noodplannen en noodvoorzieningen om het hoofd te bieden aan grootschalige verstoringen van de Internetdienstverlening. De principes opgenomen in de circulaires PPB 2005/2 en PPB/D.256 van 10 maart 2005 betreffende “Gezonde beheerspraktijken inzake de bedrijfscontinuïteit van financiële instellingen”, zijn hier onverkort van toepassing.
Bij het opstellen van de noodplannen wordt tijdens de risico-evaluatie en bedrijfsimpactanalyse, tevens aandacht besteed aan de, alsnog beperkte, doch snel toenemende "(D)DOS"[4]-aanvallen, die de beschikbaarheid van de aangeboden websites en Internetdiensten op een ernstige en mogelijks langdurige wijze (enkele uren tot in uitzonderlijke gevallen zelfs weken) trachten te ondergraven.

De financiële instelling moet de verrichtingen die haar via het Internet worden overgemaakt tenslotte adequaat opvolgen door procedures te voorzien die het correcte verloop van deze verrichtingen vooropstellen en waarbij de inherente risico’s passend beheerst worden. De instelling moet erop toezien dat het personeel dat met de Internettoepassing te maken heeft (of kan hebben) daartoe voldoende is opgeleid.

[4] (D)DOS-aanvallen of m.a.w. *[Distributed] Denial of Service* aanvallen, zijn erop gericht de Internetwebsites van ondernemingen of individuen onbeschikbaar te maken door deze gedurende een bepaalde periode te bestoken met gigantische hoeveelheden aan (soms speciaal gefabriceerde) Internetberichten.

## 6. Betrokkenheid van externe dienstverleners

Indien in het kader van het aanbieden van websites en/of financiële Internetdiensten bepaalde activiteiten worden uitbesteed of indien er beroep gedaan wordt op externe dienstverleners voor de nodige ondersteuning, dient de financiële instelling de nodige garanties te bekomen dat deze dienstverlener over de bekwaamheid en hoedanigheid beschikt om de uitbestede taken op betrouwbare en professionele wijze uit te voeren en de continuïteit ervan te verzekeren.

Indien de instelling het beheer van websites en/of Internetdiensten uitbesteedt aan een derde partij, ziet de effectieve leiding, in voorkomende geval het directiecomité, er bovendien op toe dat de externe dienstverlener de nodige onafhankelijke veiligheidsonderzoeken (zie bijlage punten 2.2.9 en 3.2.7) laat uitvoeren, dat de instelling geïnformeerd wordt over de resultaten van deze onderzoeken en dat de dienstverlener de veiligheid van de aangeboden Internetdiensten periodiek en zo veel als nodig evalueert met oog voor de evoluties van de bedreigingen. Indien de dienstverlener niet alle voormelde beveiligingstaken invult, staat de instelling zelf in voor de uitvoering ervan en worden de verantwoordelijkheden van de betrokken partijen duidelijk in het contract met de externe dienstverlener afgelijnd. Bovendien moet de financiële instelling in de overeenkomst met de dienstverlener voorzien dat zij het recht heeft op eigen initiatief een veiligheidsaudit te laten uitvoeren.

De principes opgenomen in de circulaires PPB 2004/5 en PPB 2006/1 van respectievelijk 22 juni 2004 en 6 februari 2006 betreffende “Gezonde beheerspraktijken bij uitbesteding” door kredietinstellingen, beleggingsondernemingen en verzekeringsondernemingen, blijven onverkort van toepassing.

## 7. Identificatie van de cliënt op afstand

De instelling kan via het Internet personen bereiken, die door de gebeurlijke geografische afstand niet gemakkelijk in een face-to-face contact kunnen worden geïdentificeerd.

Voor de identificatie van de cliënten op afstand dienen de financiële instellingen de bepalingen na te leven van de wet van 11 januari 1993, in het bijzonder van artikel 6bis evenals van het reglement van de CBFA van 27 juli 2004, goedgekeurd bij KB van 8 oktober 2004, in het bijzonder van de artikelen 8, §2, 34 en 37 waarbij de instelling verplicht wordt over een toezichtssysteem te beschikken waarmee atypische verrichtingen kunnen worden opgespoord.

Deze reglementering wordt toegelicht in de diverse circulaires van de CBFA over de waakzaamheidsverplichtingen met betrekking tot de cliënteel en de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme[5].

## C. Vereisten inzake de naleving van gedragsregels

De afstandsrelatie die bij online dienstverlening zowel bij het aanknopen van de zakenrelatie als nadien bij het uitvoeren van transacties een vast gegeven kan zijn, schakelt een aantal klassieke “menselijke” contacten en tussenkomsten uit, die anders kunnen instaan voor de uitwisseling van informatie tussen de bemiddelaar en de belegger.

Het is dan ook van belang dat de instelling zich bij het aanknopen van de zakenrelatie ervan vergewist dat de dienstverlening op afstand (het volledige aanbod dan wel bepaalde delen ervan) geen vrijgeleide is om af te zien van de vereiste informatie-uitwisseling en begeleiding van de cliënt.

**Voor de kredietinstellingen, beleggingsondernemingen en beheervennootschappen van ICB's** wordt in het bijzonder verwezen naar de volgende bepalingen :

- de wet van 14 juli 1991 betreffende de handelspraktijken en de voorlichting en bescherming van de consument en in het bijzonder de afdeling van deze wet over de overeenkomsten op afstand ;
- de bepalingen van artikelen 27, 28 en 28bis van de wet van 2 augustus 2002 ;
- het KB van 3 juni 2007 tot bepaling van nadere regels tot omzetting van de richtlijn betreffende de markten voor financiële instrumenten.

[5] Zie onder meer circulaire PPB 2004/8 van 22 november 2004 zoals gewijzigd door de circulaire PPB 2005/5 van 12 juli 2005.

Bij het verstrekken van beleggingsdiensten via Internet die betrekking hebben op niet-complexe financiële instrumenten kan zich de bijzondere situatie voordoen waarbij deze dienstverlening zich beperkt tot het uitvoeren van orders of het ontvangen en doorgeven van orders (*execution only*). In dergelijke gevallen kan de instelling met toepassing van artikel 27, §6 van de wet van 2 augustus 2002 verzaken aan het inwinnen van informatie van de cliënt over diens kennis en ervaring.

Het is van belang dat de instellingen op permanente wijze nagaan of de voorwaarden vervuld zijn om onder dit regime hun dienstverlening te kunnen aanbieden. Dit houdt ondermeer in dat er geen enkel initiatief genomen wordt ten aanzien van de cliënt om deze aan te moedigen in te gaan op het aanbod van de instelling voor bepaalde verrichtingen.

Verder ontslaat dit regime de financiële instelling niet van haar algemene verplichting om zich op loyale, billijke en professionele wijze in te zetten voor de belangen van haar cliënten[6] en met name voor wat betreft haar verplichting tot het nemen van regelingen inzake belangenconflicten[7] evenals haar verplichting om het best mogelijke resultaat te bekomen bij de uitvoering van de orders[8].

Bij het uitvoeren van orders of het ontvangen en doorgeven van orders die betrekking hebben op complexe financiële instrumenten dient de financiële instelling van zijn cliënt voorafgaandelijk de nodige informatie te hebben ingewonnen over diens kennis en ervaring. Indien de dienst of het product voor de cliënt niet passend zou zijn, dient de instelling de nodige systemen te voorzien om de cliënt hiervoor te waarschuwen.

Sommige financiële instellingen bieden hun cliënten tevens de mogelijkheid om via Internet beleggingsadvies te ontvangen.
In dat geval zal de instelling zich dienen te houden aan de zorgplicht bedoeld in artikel 27, §4 van de wet van 2 augustus 2002. Vooraleer dergelijke diensten van beleggingsadvies kunnen worden aangeboden dienen de instellingen de nodige IT-schikkingen te treffen die ervoor moeten zorgen dat er voor de betrokken cliënt enkel verrichtingen kunnen worden uitgevoerd die voor hem geschikt zijn rekening houdende met zijn kennis en ervaring, zijn financiële draagkracht en zijn beleggingsdoelstellingen.

**Voor de verzekeringsondernemingen** wordt er in het bijzonder verwezen naar :
- de wet van 14 juni 1991 betreffende de handelspraktijken en de voorlichting en bescherming van de consument en in het bijzonder de afdeling van deze wet over de overeenkomsten op afstand ;
- het KB van 22 februari 1991 houdende algemeen reglement betreffende de controle op de verzekeringsondernemingen, in het bijzonder het artikel 15 ;
- de wet van 27 maart 1995 betreffende de verzekerings- en herverzekeringsbemiddeling en de distributie van verzekeringen, in het bijzonder artikel 12bis tot 12quinquies ;
- het KB van 14 november 2003 betreffende de levensverzekeringsactiviteit, in het bijzonder de artikelen 8 en 72.

Voor zover als nodig wordt tevens verwezen naar de gedragscode inzake reclame en informatieverstrekking over individuele levensverzekeringen die werd opgesteld door de beroepsverenigingen na consultatie van de CBFA.

Tenslotte wordt tevens verwezen naar de individuele infofiches inzake levensverzekeringen en andere verzekeringen die door de beroepsverenigingen werden opgesteld in uitvoering van artikel 12bis, § 3 van de wet van 27 maart 1995.

6 Artikel 27, § 1 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten.

7 Artikel 20bis, §2 van de wet van 22 maart 1993 op het statuut van en het toezicht op de kredietinstellingen en artikel 62bis van de wet van 6 april 1995 inzake het statuut van en het toezicht op de beleggingsondernemingen.

8 Artikel 28 van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten.

## D. Grensoverschrijdend karakter van de aangeboden of verrichte diensten

Een website heeft per definitie een internationale reikwijdte, waardoor een gebeurlijk aanbod tot en het verrichten van de diensten door middel van een website een grensoverschrijdend karakter kunnen hebben.

Bij grensoverschrijdend dienstenverkeer binnen de EER dient de instelling zich vooreerst te houden aan de kennisgevingsverplichtingen zoals voorzien in haar wettelijke statuut[9]. De CBFA heeft met betrekking tot kennisgevingsverplichting tot dusver het standpunt ingenomen dat men ervan dient uit te gaan dat een dienstverlening grensoverschrijdend is, niet alleen wanneer de kenmerkende prestatie van de dienst (d.i. de essentie van de dienst waarvoor betaling is verschuldigd) plaatsvindt op het grondgebied van een andere lidstaat maar ook wanneer de onderneming beleggers in die andere lidstaat solliciteert door zich te verplaatsen, door verkooptechnieken op afstand of door andere dan notoriëteitsreclame. De vraag stelt zich welke regels moeten worden toegepast bij grensoverschrijdende dienstverlening. In de huidige stand van zaken moet een onderscheid gemaakt worden naargelang het soort van diensten dat wordt aangeboden via Internet.

Voor verzekeringsbemiddeling evenals voor financiële of bancaire diensten, andere dan beleggingsdiensten dient de bemiddelaar de regels van algemeen belang, met inbegrip van de gedragsregels, na te leven van het land op wiens grondgebied hij zijn diensten aanbiedt of verstrekt (het gastland of *host*).

Inzake beleggingsdiensten zijn bij de kredietinstellingen en de beleggingsondernemingen zowel de organisatorische regels als de gedragsregels van het land van herkomst toepasselijk (het thuisland of de *home*). Het gastland (*host*) kan haar eigen regels inzake beleggingsdiensten niet opleggen. Andere regels van het gastland, zoals bv. de wetgeving tot voorkoming van het witwassen en de gebeurlijke taalregels blijven wel van toepassing. Ook voor de beheervennootschappen van instellingen voor collectieve belegging worden in de ontwerprichtlijn[10] dezelfde principes gehanteerd.

Wat meer in het bijzonder het gebruik van een Internetwebsite betreft, hebben meerdere buitenlandse toezichthouders het standpunt ingenomen dat het aanbod via Internet van diensten of van instrumenten uit het buitenland wordt geacht op hun grondgebied te worden gedaan, wanneer dat aanbod gericht is aan of beschikbaar wordt gemaakt voor beleggers op hun grondgebied. Bij de beoordeling van deze criteria wordt in de regel elk geval afzonderlijk onderzocht en onder meer nagegaan of de onderdanen van het betrokken land specifiek worden geviseerd (taalgebruik, prijzen in de munt van dat land, vermelding van lokale contactadressen), of er effectief transacties of diensten via de website worden uitgevoerd en/of de beleggers met e-mail of andere communicatietechnieken worden gesolliciteerd.

De instelling moet dus op voorhand haar commerciële doelstellingen nauwkeurig omschrijven en erover waken dat, wanneer zij via haar website cliënten solliciteert op het grondgebied van een andere Staat, zij desgevallend voldoet aan de regels van deze Staat. Om te vermijden dat haar demarches in niet-geviseerde landen verkeerd worden begrepen, kan de instelling een of meer van de volgende voorzorgsmaatregelen nemen, zoals :

a) op de website vermelden dat deze bestemd is voor beleggers van een welomschreven geografische zone, waarin de onderneming conform de reglementering bedrijvig is (vermelding van kennisgevingen, van *warnings and disclaimers*); om de lokalisatie van de belegger na te gaan en te controleren of deze zich in de doelgroep bevindt, kan de instelling gebruik maken van de post, de telefonie of van speciale lokalisatietechnieken ;

b) ervoor zorgen dat de inhoud van de website of van ander promotiemateriaal (bv. in de media of de pers) niet in strijd is met de voornoemde geografische doelzone (bv. indien de website niet tot Britse cliënten is gericht, dienen ook geen lokale adressen te worden vermeld of prijzen in GBP) ;

---

9
- voor kredietinstellingen, zie artikel 38 van de wet van 22 maart 1993 op het statuut van en het toezicht op de kredietinstellingen;
- voor beleggingsondernemingen, zie artikel 87 van de wet van 6 april 1995 inzake het statuut van en het toezicht op de beleggingsondernemingen en uniforme brief aan de beleggingsondernemingen en de kredietinstellingen naar Belgisch recht van 15 oktober 2007;
- voor de beheervennootschappen van ICB's, zie artikel 180 van de wet van 20 juli 2004 betreffende bepaalde vormen van collectief beheer van beleggingsportefeuilles;
- voor de verzekeringsondernemingen, zie artikel 57 van de wet van 9 juli 1975 betreffende de controle der verzekeringsondernemingen.

10 Artikel 18. 3. van de ontwerprichtlijn UCITS IV.

c) een toegangscontrole door paswoordbescherming voorzien voor het geheel of een deel van de website, waarbij paswoorden uiteraard enkel worden verleend aan personen die tot de doelgroep behoren ;

d) contact opnemen met lokale toezichthouders om zich ervan te vergewissen dat de website niet in strijd is met de lokale reglementering.

Hoogachtend,

De Voorzitter,

Jean-Paul SERVAIS.

*Bijlage : CBFA_2009_17-1 / Gezonde praktijken inzake het beheer van de Internet-beveiligingsrisico's.*