# MiFID II and GDPR: Can't Live with Them, Can't Live without Them?

*Anneleen Van de Meulebroucke en Jean-Marc Gollier*[1]
Advocaten, Eubelius

**ABSTRACT**

**1 "*Data is the new electricity*"[2]. Het citaat is origineler dan "*Data is the new oil*"[3], maar schetst wel evenzeer het belang van gegevens in deze tijd. Ook in de financiële sector is de impact van gegevens, en in het bijzonder persoonsgegevens, fenomenaal.**

**2 In deze bijdrage gaan we in op het kruispunt tussen twee wetgevende teksten, de *Markets in Financial Instruments Directive II* ("MiFID II") en de *General Data Protection Regulation* ("GDPR"), die beide een rol spelen bij de verwerking van persoonsgegevens bij het aanbieden van beleggingsdiensten.**

**MiFID II legt de spelregels op die beleggingsondernemingen moeten volgen bij financiële dienstverlening en is gericht op transparantie en leidt tot een maximalisatie van de**

---

1 De auteurs bedanken Luana Huybrechts en Justine De Meersman voor hun waardevolle voorbereiding bij de totstandkoming van deze bijdrage.

2 J. Thijs 'De echte concurrenten van de banken zijn Google, Facebook en Amazon', De Tijd, 2019.

3 Citaat toegeschreven aan C. Humby, UK ANA Senior marketer's summit, Kellogg School, 2006.

**inwinning van informatie over de cliënt. GDPR is gericht op de controle van het datasubject (de belegger of de cliënt) over de verwerking van zijn persoonsgegevens en het verstrekken van waarborgen ter bescherming van die gegevens, waaronder gegevensminimalisatie. Het simultaan toepassen van één wetgevend kader dat leidt tot gegevensmaximalisatie en één wetgevend kader dat gericht is op gegevensminimalisatie, lijkt op het eerste gezicht tot een onmogelijke combinatie. Het is niet de bedoeling om een gedetailleerd overzicht te geven van beide wetgevende kaders, noch om alle raakvlakken tussen MiFID II en GDPR exhaustief te schetsen[4]. We bekijken daarentegen welke impact GDPR heeft op de verplichtingen van beleggingsondernemingen en de rechten van beleggers onder MiFID II.**

**De bijdrage volgt de volgorde van de *customer journey* van een cliënt van een beleggingsonderneming (deel 2). We beginnen met een bondig overzicht van de achtergrond van beide wetteksten (deel 1).**

## 1 ACHTERGROND VAN MIFID II EN GDPR

3 MiFID II[5] staat voor *Markets in Financial Instruments Directive* en trad in werking op 3 januari 2018. MiFID II is omgezet in Belgisch recht door de Wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten ("**Wet van 2 augustus 2002**")[6]. MiFID II heeft tot doel een geïntegreerde en transparante interne markt te bevorderen en te garanderen dat beleggers beschermd zijn en over toereikende informatie beschikken. Zo moeten beleggingsondernemingen in het kader van MiFID II informatie inwinnen over hun cliënten om op basis daarvan passende beleggingsdiensten aan te bieden. Wanneer ze daarbij gegevens van natuurlijke personen verwerken[7], denk aan een naam, een adres, het beroep, de inhoud van een telefoongesprek, … moeten

4 Zie voor een uitvoerig overzicht: D. Goens, Data protection bij financiële instellingen, Antwerpen, Intersentia, 2018, 856 p.

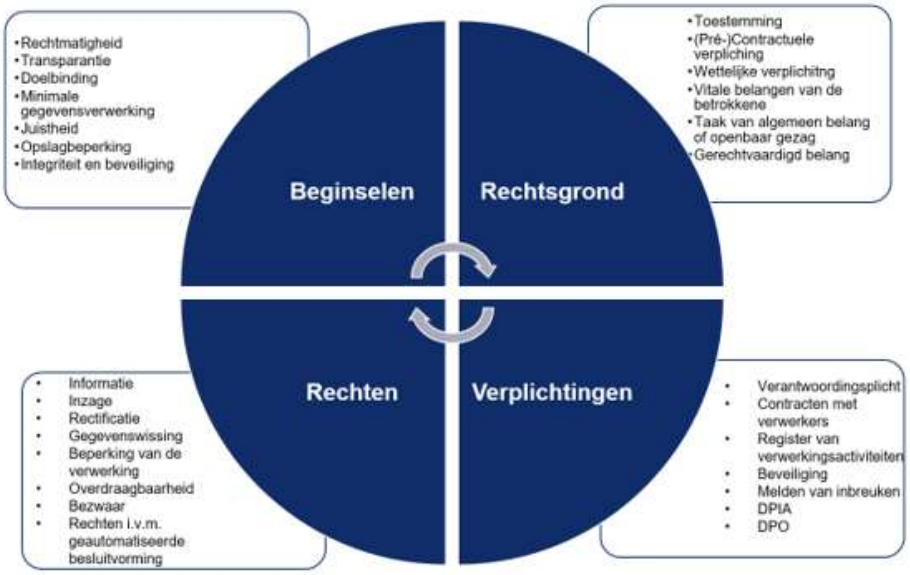
5 Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU.

6 Wet betreffende het toezicht op de financiële sector en de financiële diensten, BS 4 september 2002.

7 Rechtsoverweging 39 Gedelegeerde Verordening 2017/65/EU van de Commissie van 25 april 2016 houdende aanvulling van Richtlijn 2014/65/EU van het Europees parlement en de Raad wat betreft de door beleggingsondernemingen in acht te nemen organisatorische eisen en voorwaarden voor de bedrijfsuitoefening en wat betreft de definitie van begrippen voor de toepassing van genoemde richtlijn.

beleggingsondernemingen de gegevensbeschermingswetgeving[8], waaronder GDPR, naleven.

4 GDPR is de afkorting van *General Data Protection Regulation* (in het Nederlands: algemene verordening gegevensbescherming of AVG)[9] en is sinds 25 mei 2018 van toepassing.
GDPR heeft tot doel om aan de hand van een complex geheel van beginselen, rechten en verplichtingen (zie figuur 1) persoonsgegevens beter te beschermen over de hele Europese Unie. Daarom werd voor een verordening gekozen die rechtstreeks toepasselijk is in de EU-lidstaten.




**Figuur 1 – GDPR in een notendop**

8 Gedelegeerde Verordening 2017/65/EU verwijst eveneens naar de zgn. ePrivacywetgeving (Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie). Die richtlijn is vooral belangrijk in het kader van marketing en werd in België in verschillende wetten omgezet (o.a. de wet van 13 juni 2005 betreffende de elektronische communicatie en het Wetboek van economisch recht). De richtlijn is momenteel onder herziening.

9 Verordening 2016/679/EU van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

## 2 IMPACT VAN GDPR OP MIFID II AAN DE HAND VAN DE CUSTOMER JOURNEY

5 De *customer journey* is een populair begrip in de marketingwereld om de "reis" van de cliënt naar een bepaald bedrijf en de daaropvolgende interactie met dat bedrijf te illustreren. Wij kiezen er in deze bijdrage voor om de impact van GDPR op MiFID II te illustreren aan de hand van vijf fasen uit de *customer journey*, zoals weergegeven in figuur 2:

**Figuur 1 - Customer journey**

### 2.1 Prospectie

6 De zoektocht naar een cliënt vormt de start van de *customer journey*. De beleggingsonderneming zal een potentiële cliënt, een zgn. prospect, informatie over haar beleggingsproducten en –diensten, zgn. *direct marketing*, bezorgen via uiteenlopende kanalen.
De daarbij in acht te nemen regels en richtlijnen[10] volgen uit het ruimere gegevensbeschermingsrecht, waaronder, maar niet beperkt tot, de GDPR. Ze verschillen

[10] De aanbeveling 02/2013 van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, de voorganger van de Gegevensbeschermingsautoriteit ("**GBA**"), van 30 januari 2013 vormt op de datum van het afronden van deze bijdrage het meest omvattende document terzake, maar de GBA duidt dit document zelf als 'verouderd' aan op haar website. De GBA zal zeer binnenkort een nieuwe aanbeveling publiceren (zie haar strategisch plan 2019-2025 waarin zij ook aankondigde dat de sector van direct marketing de bijzondere aandacht van de GBA zal genieten).

naargelang het kanaal dat de onderneming gebruikt om de potentiële cliënt te bereiken; er zijn verschillende verplichtingen voor *direct marketing* per elektronische post (e-mail, SMS, fax, MMS, …), gewone post, telefoon en cookies, wat het voor beleggingsondernemingen complex maakt.
Als basisregel geldt dat een onderneming toestemming nodig heeft van een natuurlijke persoon om *direct marketing* per elektronische post te zenden. Uitzonderingen gelden onder andere voor marketing per elektronische post aan bestaande, directe cliënten van de beleggingsonderneming (onder strikte voorwaarden[11]) en per telefoon, zgn. *cold calling* (artikel VII.110 WER).
We concluderen in deze fase dat de GDPR belangrijke verplichtingen oplegt aan beleggingsondernemingen die hun producten en diensten aan de man proberen brengen. De concrete inhoud van de verplichtingen verschilt naargelang het gekozen marketingkanaal.

## 2.2 Cliëntenclassificatie

7 Zodra een prospect effectief een beroep wenst te doen op een bepaalde beleggingsdienst, moet de beleggingsonderneming die persoon indelen in één van de drie MiFID-categorieën.

1. De **professionele cliënt** is een cliënt met "*de nodige ervaring, kennis en deskundigheid […] om zelf beleggingsbeslissingen te nemen en de door hem gelopen risico's adequaat in te schatten*", zoals kredietinstellingen, verzekeringsondernemingen, institutionele beleggers en grote ondernemingen.
2. De **niet-professionele cliënt** is een cliënt die niet als professionele cliënt kan worden aangemerkt. Deze zgn. *retail investors* zijn meestal KMO's en natuurlijke personen.
3. De **in aanmerking komende tegenpartij** ten slotte is een subcategorie van de professionele cliënten.

De categorie bepaalt de toepasselijke gedragsregels voor de beleggingsonderneming en het beschermingsniveau van de cliënt. De niet-professionele cliënten worden als zwakke marktdeelnemers beschouwd en genieten onder MiFID II het hoogste beschermingsniveau.

8 De beleggingsonderneming informeert de cliënt over zijn categorie en zijn recht om een andere indeling te vragen. Cliënten kunnen een hoger beschermingsniveau vragen

[11] Artikel 1 Koninklijk besluit van 4 april 2003 tot reglementering van het verzenden van reclame per elektronische post. Volgens rechtsoverweging 47 GDPR kan de verwerking van persoonsgegevens ten behoeve van direct marketing worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang.

(*opt-in*). Zij kunnen ook afstand doen van hun beschermingsniveau om toegang te krijgen tot meer risicovolle beleggingsproducten (*opt-out*) indien aan volgende cumulatieve vereisten is voldaan:

1. de cliënt toont aan dat hij de nodige ervaring, kennis en deskundigheid heeft om zelf beleggingsbeslissingen te nemen en de door hem gelopen risico's adequaat in te schatten (kwalitatief vereiste); en
2. de beleggingsonderneming moet bijkomende informatie inwinnen over de situatie van de cliënt, zoals de omvang van de portefeuille, professionele ervaring in de financiële sector en verrichtingen van de cliënt in de voorbije jaren (kwantitatief vereiste).

9 In principe vindt er bij de initiële indeling in een categorie geen specifieke verwerking van persoonsgegevens plaats voor de niet-professionele cliënt die een natuurlijke persoon is. Het loutere feit dat de cliënt een particulier is, volstaat voor de beleggingsonderneming om de cliënt te kwalificeren als niet-professionele cliënt zonder dat er informatie wordt ingewonnen. Dat is echter anders wanneer een niet-professionele cliënt een professionele cliënt wil worden. In dat geval geldt een bijkomende verplichting om informatie in te winnen voor de beleggingsonderneming en gelden enkele aandachtspunten die we hierna toelichten.
In deze fase is de impact van GDPR op MiFID II dus minimaal, op de hierboven genoemde uitzondering, na.

## 2.3 De algemene informatieverplichting (KYC)

10 Beleggingsondernemingen hebben op basis van MiFID II een zorgplicht en moeten op grond daarvan steeds in het belang van de cliënt handelen en zich op loyale en billijke wijze voor dat belang inzetten.
De zorgplicht komt ook tot uiting in de zgn. ken-je-cliënt onderzoeksverplichting (*know your customer* of *KYC*). Afhankelijk van de diensten van de beleggingsonderneming bestaat die verplichting uit het uitvoeren van een geschiktheids- dan wel een passendheidsbeoordeling. Voor die beoordeling zijn beleggingsondernemingen verplicht om een profiel van de cliënt op te maken op basis van informatie die zij krijgen van de cliënt (zie figuur 3).

| Geschiktheidsbeoordeling<br>artikel 27*ter*, §2 Wet van 2 augustus 2002 | Passendheidsbeoordeling<br>artikel 27*ter*, §3 Wet van 2 augustus 2002 |
|---|---|
| Bij het verstrekken van beleggingsadvies of het verrichten van vermogensbeheer, wint de beleggingsonderneming bij de cliënt of de potentiële cliënt de nodige informatie in over: | Bij het verrichten van andere beleggingsdiensten, wint de beleggingsonderneming bij de cliënt of de potentiële cliënt informatie in over: |
| • zijn **kennis en ervaring** op beleggingsgebied met betrekking tot het specifieke soort product of dienst;<br>• zijn **financiële situatie**, met inbegrip van zijn vermogen om verliezen te dragen; en<br>• zijn **beleggingsdoelstellingen**, met inbegrip van zijn risicotolerantie | • zijn **kennis en ervaring** op beleggingsgebied met betrekking tot het specifieke soort van aangeboden of verlangde product of dienst |
| teneinde de cliënt of de potentiële cliënt de voor hem geschikte beleggingsdiensten en financiële instrumenten te kunnen aanbevelen, of voor hem geschikt vermogensbeheer te verstrekken, die met name stroken met zijn risicotolerantie en zijn vermogen om verliezen te dragen. | zodat zij kan beoordelen of het aangeboden product of de te verrichten beleggingsdienst passend is voor de cliënt. |

**Figuur 3 – Overzicht passendheids- en geschiktheidsbeoordeling**

11 De beleggingsonderneming heeft een actieve ondervragingsplicht en een marginale verificatieplicht. De *actieve ondervragingsplicht* houdt in dat de beleggingsonderneming zelf informatie moet inwinnen bij de cliënt en zelf de juiste vragen moet stellen om de nodige informatie te bekomen. De *marginale verificatieplicht* betekent dat de beleggingsonderneming geen verder onderzoek moet doen indien de informatie adequaat en juist lijkt te zijn.

De cliënt heeft een *passieve antwoordplicht*. De cliënt moet steeds correct antwoorden op de gestelde vragen. Indien de cliënt echter weigert om bepaalde informatie te geven en de beleggingsonderneming niet voldoende informatie bekomt om een *geschiktheid*sbeoordeling uit te voeren, mag zij de cliënt geen beleggingsadvies of vermogensbeheer verstrekken (artikel 27,§5 Wet van 2 augustus 2002). Indien de beleggingsonderneming onvoldoende informatie bekomt om een *passendheid*sbeoordeling uit te voeren, mag zij de cliënt wel andere beleggingsdiensten (dan beleggingsadvies of vermogensbeheer verstrekken), maar moet zij de cliënt

waarschuwen dat zij daardoor niet kan vaststellen of de aangeboden dienst passend is. De cliënt heeft ook een *beperkte mededelingsplicht*: indien hij weet dat bepaalde informatie een substantiële impact kan hebben op de beoordeling vanwege de beleggingsonderneming, moet hij die informatie meedelen.

12 Het beginsel van minimale gegevensverwerking in artikel 5(1)(c) GDPR, beperkt de hierboven genoemde ondervragings- en antwoordplicht. Op grond van dat beginsel mogen beleggingsondernemingen enkel gegevens opvragen bij de cliënt die toereikend, ter zake dienend en niet overmatig zijn om (i) de kennis en ervaring op beleggingsgebied en eventueel (ii) de financiële situatie en (iii) de beleggingsdoelstellingen van de cliënt in te schatten. MiFID II bepaalt niet precies welke gegevens nodig zijn om de kennis en ervaring, de financiële situatie van een cliënt en zijn beleggingsdoelstellingen te beoordelen. Discussies of beleggingsondernemingen een volledig CV mogen opvragen (impact op kennis en ervaring), of zij vragen mogen stellen over iemands gezondheidstoestand (impact op beleggingsdoelstellingen) enz. kunnen dan rijzen.

Daarnaast is een interessante vraag of de beleggingsonderneming gegevens uit andere (interne/externe) bronnen, en dus niet bij de cliënt zelf verkregen, mag/moet betrekken bij de geschiktheids- en passendheidsbeoordeling. “Recyclage” van gegevens (zelfs binnen een onderneming) is immers in principe verboden omwille van het doelbindingbeginsel in artikel 5(1)(b) GDPR. Dit beginsel houdt in dat persoonsgegevens verkregen voor een welbepaald doel niet verder mogen worden verwerkt op een manier die onverenigbaar is met dat doel. Indien voor de geschiktheids- en passendheidsbeoordeling persoonsgegevens worden gebruikt die oorspronkelijk voor een ander doel werden verzameld (bv. witwas *compliance* of marketing) dan mogen die gegevens niet zomaar worden hergebruikt. Ze zullen enkel mogen worden gebruikt als de cliënt toestemt met het hergebruik, als de wet het gebruik verplicht (wat bv. het geval is bij kredieten aan particulieren) of na een positief resultaat van een verenigbaarheidstest zoals bedoeld in artikel 6(4) GDPR. Bij een dergelijke test worden alle elementen van de oorspronkelijke en de verdere verwerking grondig beoordeeld.

Ten slotte vergt ook het profileringsaspect van de geschiktheids- en passendheidsbeoordeling bijzondere aandacht. Op basis van de verstrekte persoonsgegevens maakt de beleggingsonderneming een profiel van de cliënt. Profileren en het nemen van geautomatiseerde besluiten zijn zeer gevoelige gegevensverwerkingen waarvoor datasubjecten bijzondere bescherming genieten onder de GDPR, zoals de mogelijkheid om menselijke tussenkomst te vragen, de mogelijkheid om informatie op te vragen over de achterliggende logica van de besluitvorming en het recht om een besluit aan te vechten (artikel 22 GDPR). Op dit punt bevat MiFID II geen specifieke bepaling voor een cliënt om zijn profiel na de geschiktheids- of passendheidsbeoordeling te laten aanpassen.
In deze fase van de *customer journey* zien we de impact van de GDPR op MiFID II opnieuw toenemen. De beginselen van gegevensminimalisering en doelbinding beperken de

bewegingsvrijheid van beleggingsondernemingen op het vlak van het gebruik van persoonsgegevens sterk. GDPR kent ook rechten toe waarop beleggers (natuurlijke personen) zich zouden kunnen beroepen om hun profiel beter te begrijpen.

## 2.4 Uitvoering van het contract

13 Na het sluiten en tijdens de uitvoering van het contract over een beleggingsdienst of -product stopt het verwerken van persoonsgegevens niet. MiFID verplicht beleggingsondernemingen bijvoorbeeld om telefoongesprekken op te nemen alsook alle elektronische communicatie in verband met het ontvangen, doorgeven en uitvoeren van cliëntorders te bewaren en de cliënt daarover te informeren. Een interessante discussie die zich in de marge van de bewaarplicht onder MiFID I gedurende een aantal jaren heeft ontsponnen, had betrekking op de vraag of beleggers (natuurlijke personen) de rechten die zij ontlenen aan de GDPR (en haar voorganger), bv. het recht op een kopie van persoonsgegevens, kunnen gebruiken (volgens sommigen misbruiken) om toegang te krijgen tot (*transcripts* van) hun telefoongesprekken met beleggingsondernemingen. In de lidstaten ontwikkelde zich hierover interessante (tegengestelde) rechtspraak. De discussie lijkt een beetje aan belang te hebben ingeboet nu artikel 27bis, §8 *in fine* Wet van 2 augustus 2002 voorziet in een recht om te verzoeken om opgenomen telefoongesprekken en elektronische communicatie te verstrekken.

14 De beleggingsonderneming heeft gedurende de hele duur van het contract met de cliënt verder de verplichting om gegevens te actualiseren op grond van MiFID II (artikel 27ter, § 2 en 3 Wet van 2 augustus 2002). Een cliënt kan in de loop van de relatie met de beleggingsonderneming immers worden geconfronteerd met gewijzigde persoonlijke omstandigheden (bv. aanzienlijke daling van liquide middelen of jobverlies) die een impact hebben op zijn risicoprofiel. Wat die actualiseringsplicht betreft, lopen MiFID II en GDPR gelijk. GDPR bevat namelijk een beginsel dat beleggingsondernemingen verplicht om alle redelijke maatregelen moeten te nemen opdat persoonsgegevens juist zijn en up-to-date blijven (artikel 5(1)(d) GDPR).
In deze fase van de *customer journey*, zien we in MiFID II gelijkaardige, maar minder uitgesproken beginselen als in GDPR. MiFID II kent net zoals GDPR een (beperkter) recht op toegang tot gegevens en verplicht evenzeer om gegevens te blijven actualiseren.

## 2.5 Na de contractuele relatie

15 We gaven al aan dat beleggingsondernemingen op grond van MiFID II verplicht zijn om alle telefoongesprekken en alle elektronische communicatie bij te houden over alle verleende diensten, activiteiten en transacties. Die opgenomen telefoongesprekken en

elektronische communicatie moeten voor vijf jaar worden bewaard, maar bevoegde instanties kunnen verzoeken om de communicatie zeven jaar te bewaren[12]. Die bewaartermijnen vormen dus de ondergrens voor een beleggingsonderneming bij het bepalen van haar bewaarbeleid. De bovengrens vindt een beleggingsonderneming in het beginsel van opslagbeperking in artikel 5(1)(e) GDPR, dat inhoudt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt. MiFID II en GDPR hebben op dit punt dus een complementaire werking.

De interessantste vraag die beleggingsondernemingen bezighoudt in een *big data* tijdperk is wellicht of zij de berg gegevens die zij tijdens de contractuele relatie hebben verzameld nadien kunnen blijven gebruiken voor eigen interne doeleinden, ingegeven door marketingwensen of wettelijke verplichtingen (bv. witwas *compliance*). Leidinggevend bij die vraag is artikel 6(4) GDPR, dat bij gebrek aan toestemming van de cliënt of een wettelijke verplichting in hoofde van de beleggingsonderneming, neerkomt op een beoordeling van de verenigbaarheid van de oorspronkelijke met de verdere verwerking. In theorie eenvoudig, in de praktijk een hersenbreker.

## 3 CONCLUSIE

16 MiFID II en GDPR zijn twee reglementaire zwaargewichten waarmee beleggingsondernemingen sinds 2018 rekening moeten houden. In deze bijdrage werd de confrontatie tussen beide wetgevende kaders besproken aan de hand van de *customer journey* van een cliënt van een beleggingsonderneming en keken we meer specifiek naar de impact van GDPR op MiFID II. Gebleken is dat GDPR een belangrijke impact heeft op de beleggingsonderneming die persoonsgegevens van een belegger (natuurlijke persoon) verwerkt. De impact is daarbij het grootst in de fase van de prospectie, het uitvoeren van het KYC-onderzoek en na de contractuele relatie, in de mate dat de beleggingsonderneming gegevens wil hergebruiken. Op dit punt zijn de meest interessante vragen te verwachten voor beleggingsondernemingen in het *big data* tijdperk. Beide regelgevende instrumenten huldigen evenwel soms ook gelijkaardige principes en soms vullen beide instrumenten elkaar zelfs aan.

[12] Artikel 26, §5 Wet van 25 oktober 2016 betreffende de toegang tot het beleggingsdienstbedrijf en betreffende het statuut van en het toezicht op de vennootschappen voor vermogensbeheer en beleggingsadvies en artikel 64 Wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen.