Due diligence en uitbestedingsrisico: wettelijke eisen

Peter Laaper

INLEIDING

Uitbesteding brengt risico's met zich. Deze moet men beheersen. Dat vereist dat men de risico's eerst in kaart brengt. Immers, risico's die men niet kent, kan men niet beheersen. Het is als in volle vaart autorijden op de snelweg, maar zonder goed zicht.

Om de risico's in kaart te brengen, voert men een due diligence-onderzoek uit. Is de due diligence goed uitgevoerd, dan kan men bepalen (i) welke risico's te accepteren, (ii) op welke wijze risico's te beheersen als men de risico's niet wil accepteren of (iii) om geheel af te zien van uitbesteding aan de beoogde partij.

Een goede due diligence is niet alleen verstandig. Vanwege het cruciale belang voor de risicobeheersing bij uitbesteding is ze ook verplicht. In regelgeving worden al veel onderwerpen genoemd die in de due diligence moeten worden meegenomen. Dit is geen afvinklijst: er zijn ook onderwerpen die opvallend onvermeld blijven, zoals onderuitbesteding. Met het afstrepen van de onderwerpen die in de wet genoemd zijn, is men er dus nog niet: men moet zelf blijven nadenken wat de risico's bij *deze* uitbesteding van *deze* werkzaamheden aan *deze* dienstverlener zijn. Voorts komt de vraag op wat met de geïdentificeerde risico's gedaan moet worden: moeten ze volledig worden geëlimineerd of slechts teruggedrongen? En kan dat zuiver contractueel door de verantwoordelijkheid volledig of grotendeels bij de dienstverlener te leggen, of houdt de uitbesteder zelf ook een actieve rol?

Deze vragen zijn niet te beantwoorden zonder eerst een blik te werpen op doel en ratio van de wettelijke uitbestedingsvoorschriften. In deze bijdrage begin ik daarmee. Daarna ga ik in op de in een due diligence te betrekken onderwerpen. Tot slot behandel ik hoe de geïdentificeerde risico's te beheersen en hoever men moet gaan in het treffen van risicobeheersingsmaatregelen.

Deze bijdrage schrijf ik met het oog op de (AIFMD)-beheerder van een beleggingsportefeuille die een derde inschakelt om een deel van het vermogensbeheer uit te voeren. Dit verhoogt de lees-

Peter Laaper
Advocaat bij Keijser van der Velden en universitair docent aan de Universiteit Utrecht

baarheid omdat de specifieke voorschriften vaak net wat verschillen tussen bijvoorbeeld AIFMD-beheerders en ICBE-beheerders, pensioenfondsen en verzekeraars, maar ook beleggingsondernemingen en *bank*beleggingsondernemingen. Voor een goed begrip van de uitbestedingsvoorschriften hebben deze verschillen echter weinig belang: in alle gevallen geldt dat elke uitbestedende onderneming alle relevante risico's moet onderkennen (de due diligence) en beheersen.

DOEL EN RATIO VAN DE REGELGEVING

Beheerders mogen best risico's nemen, maar alleen verantwoorde risico's. Beheerders moeten daarom de risico's die zij nemen, beheersen. Dat volgt uit hun fiduciaire zorgplicht naar hun klanten. Ze zijn het ook verplicht op grond van de Wet op het financieel toezicht (Wft). Juridisch heet dit dat de manager over een *beheerste en integere bedrijfsvoering* moet beschikken. In vlot jargon heet het dat hij *in control* moet zijn.

> RISICO'S DIE MEN NIET KENT, KAN MEN NIET BEHEERSEN. HET IS ALS IN VOLLE VAART AUTORIJDEN OP DE SNELWEG, MAAR ZONDER GOED ZICHT

Het probleem met uitbesteden is dat een deel van die bedrijfsvoering in feite buiten de eigen onderneming wordt geplaatst. Of anders geformuleerd: de bedrijfsvoering van de dienstverlener wordt onderdeel van de eigen bedrijfsvoering. Dat is prima waar het voordelen betreft, zoals lagere kosten, betere kwaliteit of toegang tot specialistische kennis. Maar de uitbestedende beheerder haalt ook de risico's en tekortkomingen in de bedrijfsvoering van zijn dienstverlener binnen. Als de ingeschakelde vermogensbeheerder ongeschikte beleggingen selecteert, staat de portefeuille aan ongewenste beleggingsrisico's bloot. Administreert de vermogensbeheerder onjuist de beleggingen, dan kan de beheerder niet correct rapporteren aan zijn cliënten en toezichthouders. En erger: door de uitbesteding kan hij ook niet meer (rechtstreeks) ingrijpen om tekortkomingen te herstellen. De uitvoering ligt immers bij een ander: zijn dienstverlener. Is de beheerder dan nog wel *in control* over de uitbestede werkzaamheden, over het uitbestede deel van wat in feite zijn eigen bedrijfsvoering is?

De oplossing van de wetgever is rigoureus: een uitbestedende onderneming blijft jegens cliënten en toezichthouders volledig verantwoordelijk voor het handelen en nalaten van zijn dienstverlener als was het zijn eigen handelen en nalaten. De uitbesteder heeft maar te organiseren dat hij *in control* blijft.[1] Van belang hierbij is dat *total control* onnodig is: *in control* is voldoende. De ratio van een uitbesteding is dat de dienstverlener een activiteit beter of goedkoper kan dan de uitbesteder dat kan. Die hele rationale valt weg als de uitbesteder *micro-managent* zijn dienstverlener moest vertellen wat wanneer te doen. De dienstverlener kan dat ook niet accepteren: hij zou zelf niet meer in control zijn over zijn eigen bedrijfsvoering. Waar het om gaat is dat de uitbesteder *voldoende* control kan uitoefenen om de omvang van de risico's te reduceren tot een niveau dat verantwoord is.

> DOOR UITBESTEDING WORDT DE BEDRIJFSVOERING VAN DE DIENSTVERLENER ONDERDEEL VAN DE EIGEN BEDRIJFSVOERING

Daarvoor is noodzakelijk een capabele dienstverlener te selecteren die aantoonbaar in staat is om de uitbestede werkzaamheden voldoende consistent conform vastgestelde (minimum)normen te verrichten. Dat is de stap waar due diligence op ziet. Immers, de bedrijfsvoering van de dienstverlener is onderdeel gemaakt van de eigen bedrijfsvoering, en de eigen bedrijfsvoering moet beheerst en integer zijn.

IN DE DUE DILIGENCE TE BETREKKEN ONDERWERPEN

Uit het voorgaande zijn een aantal categorieën aan onderwerpen af te leiden waar in een due diligence op gelet moet worden. Ik onderscheid: (i) zijn de primaire processen van de dienstverlener in staat om de werkzaamheden conform de gestelde eisen te verrichten? (paragraaf 1-2); (ii) kan hij dat consistent en ook bij verstoringen? (paragraaf 3-6); (iii) kan de dienstverlener ook voldoen als de wettelijke eisen of de wensen van de beheerder veranderen? (paragraaf 7).

Deze categorieën kunnen worden uitgewerkt. Zo zijn andere eisen te stellen naar gelang de aard van de werkzaamheden (bijvoorbeeld portefeuillebeheer, risicobeheer, administratie of ICT-ondersteuning). En hoe hoog de lat ligt op die eisen is afhankelijk van het gewenste kwaliteitsniveau.

Uit regelgeving is een lange lijst van eisen te destilleren die in een due diligence meegenomen moeten worden. In deze bijdrage is geen ruimte om deze eisen allemaal te behandelen. Bovendien biedt de regelgeving geen sluitende lijst. Ik beperk mij daarom tot een aantal onderwerpen die (i) specifiek op vermogensbeheer zien, (ii) vanwege hun belang aandacht behoeven, of (iii) in de praktijk vaak onvoldoende aandacht krijgen.

1. PRIMAIRE PROCESSEN

Primaire processen zijn de processen die direct bijdragen aan de dienstverlening. Voor de casus in deze bijdrage gaat het om het vermogensbeheer. De beheerder moet zich ervan vergewissen dat de primaire processen van de externe vermogensbeheerder op orde zijn en zo kunnen worden ingericht dat de gevraagde diensten geleverd worden. Het gaat over processen als de selectie van beleggingen en de orderuitvoering, maar ook of de externe vermogensbeheerder kan voldoen aan het ESG-beleid van de beheerder.

2. RAPPORTAGES

Rapportages kan men zien als onderdeel van de primaire processen: een uitbesteding zonder rapportages bestaat niet. Voor zijn beeld van de uitvoering van de uitbestede werkzaamheden is de beheerder immers afhankelijk van de rapportages van zijn dienstverlener. Elke dienstverlener biedt standaardrapportages. De beheerder kan eenvoudig onderzoeken of de standaardrapportage alle gewenste informatie bevat en duidelijk weergeeft. DNB constateerde in het verleden dat de inhoud en complexiteit van rapportages niet altijd aansluit op de behoeften van opdrachtgevers.

3. BEHEERSTE EN INTEGERE BEDRIJFSVOERING

De bedrijfsvoering van de dienstverlener wordt onderdeel van de eigen bedrijfsvoering en moet daarom beheerst en integer zijn. Het gaat niet alleen over de primaire processen; het gaat ook om de secundaire processen: de processen die het primaire proces ondersteunen, zoals ICT, compliance en management. Dit zijn belangrijke onderwerpen. Immers, ook bij de dienstverlener gaan in de bedrijfsvoering onvermijdelijk dingen mis. Dat is inherent. Bij een beheerste en integere bedrijfsvoering blijven de gevolgen voor de beheerder binnen de perken.

> EEN UITBESTEDENDE ONDERNEMING IS TEGENOVER CLIËNTEN EN TOEZICHTHOUDERS VERANTWOORDELIJK VOOR HET HANDELEN EN NALATEN VAN ZIJN DIENSTVERLENER ALS WAS HET ZIJN EIGEN HANDELEN EN NALATEN

De beheerder kan onderzoek doen naar beleidsdocumenten zoals het ICT-beleid, het *cloud*-beleid, het beloningsbeleid, het compliancebeleid en het integriteitsbeleid. Minstens zo belangrijk is of het beleid ook wordt uitgevoerd. Bestaan er werkelijk backup- en noodvoorzieningen? Functioneren die ook? Het kan zinvol zijn om de laatste rapporten van de compliance-afdeling in te zien. Uiteraard wordt een ISAE 3402-verklaring[2] opgevraagd, maar het is belangrijk om ook de inhoud van het rapport te bestuderen. Ziet het rapport bijvoorbeeld op alle relevante processen of is de scope beperkter dan dat?

Voor de digitale voorzieningen van de dienstverlener is het verstandig alvast voor te sorteren op de eisen die per 17 januari 2025 zullen gelden. De *Digital Operational Resilience Act* ("DORA")[3] stelt verhoogde eisen aan de robuustheid van de digitale systemen van financiële ondernemingen en hun dienstverleners.

4. BELANGENTEGENSTELLINGEN

Bij uitbesteding van portefeuille- of risicobeheer moet de beheerder vaststellen of er sprake is van belangentegenstellingen en, zo ja, of die reeds afdoende worden beheerst. Of sprake is van belangentegenstellingen inzake portefeuille- of risicobeheer moet worden bepaald aan de hand van verscheidene criteria. De meeste daarvan zien op de waarschijnlijkheid van belangentegenstellingen. Een andere aanwijzing voor belangentegenstellingen is wanneer, door het bestaan van groepsverbanden of contractuele relaties, (i) de dienstverlener zeggenschap kan uitoefenen in de beheerder of (ii) een belegger zeggenschap kan uitoefenen in de dienstverlener.[4] Het portefeuille- of risicobeheer mag sowieso niet aan de bewaarder worden uitbesteed.[5] De bewaarder heeft namelijk diverse controletaken tegenover de beheerder.[6]

5. ONDERUITBESTEDING

Waarschijnlijk maakt de dienstverlener zelf ook gebruik van diensten van derden. Vanuit het perspectief van de beheerder is dat een onderuitbesteding. De beheerder moet in de due diligence vaststellen of hiervan sprake is en verzekeren dat de (keten van) onderuitbesteding voldoet aan zowel het wettelijk voorgeschreven als het door de beheerder gewenste kwaliteits- en beheersingsniveau.[7]

6. REPUTATIE EN REFERENTIES

Dit is geen juridisch voorgeschreven eis, maar wel een heel praktische. Op papier en in theorie kan men alles mooi maken, maar het is de weerbarstige werkelijkheid die telt. Er is nauwelijks een snellere en effectievere manier om door een papieren werkelijkheid heen te prikken dan door referenties op te vragen. Resultaten uit (andermans) verleden bieden geen garantie, maar scheppen wel verwachtingen voor de toekomst.

> *TOTAL CONTROL* IS ONNODIG, *IN CONTROL* IS VOLDOENDE

Het is verstandig óók referenties op te vragen bij voormalige klanten. Waarom zijn ze weggaan? Zijn ze ook gedurende de overgangsfase keurig behandeld?

7. WIJZIGING VAN EISEN

In de loop van de uitbestedingsrelatie kunnen eisen wijzigen. Dit kan het gevolg zijn van nieuwe regelgeving. Het is ook mogelijk dat veranderde marktomstandigheden bij de beheerder tot andere wensen aan de uitvoering van de werkzaamheden leiden. Wat de oorzaak ook moge zijn: dienstverlening die perfect voldoet aan de overeengekomen, maar inmiddels verouderde afspraken, is van weinig nut. Dit kan bij langlopende overeenkomsten een probleem zijn. Er moeten dan mechanismen bestaan om – met inachtneming van de redelijke belangen van de dienstverlener – toch tot wijziging van eisen te komen.

BEHEERSING VAN DE GEÏDENTIFICEERDE RISICO'S

Nadat de relevante risico's zijn geïdentificeerd, komt men toe aan het adequaat beheersen ervan. Adequaat beheersen betekent niet dat risico's moeten worden uitgebannen. Door het nemen van risicobeheersingsmaatregelen moet het risico dat met de uitbesteding gepaard gaat, worden beperkt. De omvang van het risico dat overblijft, moet zo klein worden dat de beheerder het kan accepteren. Anders gezegd: het *restrisico* moet kleiner zijn dan de *risk appetite*[8] van de beheerder.

Hieruit volgt dat het bij het treffen van beheersingsmaatregelen niet om individuele beheersingsmaatregelen gaat. Het gaat om het geheel aan genomen maatregelen dat bepaalt of risico's adequaat worden beheerst. Dat is nuttig, want de dienstverlener kan zijn eigen redenen hebben om bepaalde beheersingsmaatregelen niet of niet volledig te willen. Die beheersingsmaatregelen grijpen immers in in *zijn* bedrijfsvoering.

> AAN DE HAND VAN DE GEÏDENTIFICEERDE RISICO'S MOET DE BEHEERDER RISICOBEHEERSINGSMAATREGELEN VASTSTELLEN OF UITONDERHANDELEN WAARDOOR HET RESTRISICO KLEINER IS DAN DE *RISK APPETITE* VAN DE BEHEERDER

Stel bijvoorbeeld dat de beoogde dienstverlener vanwege een beperkte kapitalisering of een risicovol mandaat, een relatief kleine aansprakelijkheid voor schade wil accepteren. Dat betekent een financieel risico voor de beheerder wanneer zulke schade zich voordoet. Dit financiële risico kan hij verkleinen door bijvoorbeeld verzekering van het risico te eisen, een korte contractuele opzegtermijn zodat steeds verder oplopende schade niet lang oploopt, of frequente rapportages in combinatie met ruime mogelijkheden om wijzigingen aan te brengen in de uitvoering van het vermogensbeheer. Voor beheerder en dienstverlener valt er dus wat te kiezen en te onderhandelen, om zo tot een voor beide acceptabel resultaat te komen.

Adequaat beheersen betekent evenmin dat de dienstverlener contractueel volledige verantwoordelijkheid en aansprakelijkheid moet aanvaarden voor wat eventueel fout gaat. Dat lijkt misschien best redelijk: gaat iets mis in de bedrijfsvoering van de dienstverlener, dan moet hij de gevolgen maar dragen. Weliswaar blijft de beheerder verantwoordelijk en aansprakelijk jegens beleggers en toezichthouder, maar de beheerder kan zich op zijn beurt omdraaien naar de dienstverlener en hem aanspreken. Toch is dit geen oplossing – als de dienstverlener er al in zou meegaan.[9] De ratio van de wettelijke uitbestedingsvoorschriften is dat de uitbestedende beheerder *in control* blijft over de uitbestede werkzaamheden. Dat duidt op actief monitoren en zo nodig bijsturen, niet op het achteraf doorleggen van de rekening.

CONCLUSIE

De due diligence is een cruciale stap om in control te zijn over het uitbestede vermogensbeheer. De beheerder moet vaststellen of de dienstverlener (i) in staat is om de werkzaamheden conform de gestelde eisen te verrichten, (ii) over een beheerste en integere bedrijfsvoering beschikt, en (iii) ook kan voldoen als wettelijke eisen of de wensen van de beheerder veranderen. Aan de hand van de geïdentificeerde risico's moet de beheerder risicobeheersingsmaatregelen vaststellen of uitonderhandelen waardoor het restrisico kleiner is dan de *risk appetite* van de beheerder.

Noten

1 P. Laaper, Uitbesteding in de financiële sector, Deventer: Wolters Kluwer 2015, par. 2.3.
2 Een ISAE 3402-verklaring is een door een auditor afgegeven verklaring die inhoudt dat de organisatie waaraan processen zijn uitbesteed, zodanige interne beheersingsmaatregelen heeft getroffen dat zij "in control" is over de eigen bedrijfsvoering. Er zijn twee typen verklaringen. Type I geeft zekerheid over de opzet en het bestaan van interne beheersingsmaatregelen. Type II geeft zekerheid dat de beheersingsmaatregelen ook werken.
3 Verordening 2022/2554 betreffende digitale operationele weerbaarheid voor de financiële sector.
4 Art. 80 lid 1, sub a en b, Gedelegeerde Uitvoeringsverordening AIFMD (Vo 231/2013).
5 Art. 20 lid 2 sub a en 21 lid 4 sub a AIFMD.
6 Art. 21 AIFMD en Hoofdstuk IV Gedelegeerde Uitvoeringsverordening AIFMD.
7 Art. 20 lid 4 AIFMD.
8 De *risk appetite* is de risico-omvang die iemand bereid is te accepteren. Een stevig gekapitaliseerde beheerder zal doorgaans een grotere *risk appetite* hebben: gaat er wat mis en moeten dure herstelmaatregelen genomen dan hij de financiële tegenvaller incasseren zonder daar wezenlijke problemen van te hebben.
De *risk appetite* van de beheerder moet men onderscheiden van die van de beleggers. De *risk appetite* van de beleggers ziet vooral op het risico-rendementprofiel van de beleggingsportefeuille. De *risk appetite* van de manager ziet op de risico's die *hijzelf* loopt bij verstoring van de bedrijfsvoering van hemzelf of van de dienstverlener voor wie hij volledig verantwoordelijk is.
9 De vermogensbeheerder kan geen onbegrensde aansprakelijkheid accepteren. Het potentiële risico staat in geen verhouding tot de vergoeding die hij normaal ontvangt. (Bijna) onbegrensde aansprakelijkheid zou enkel kunnen bij zeer forse tariefsverhoging.