de Berlaimontlaan 14 – BE-1000 Brussel
tel. +32 2 221 44 74
ondernemingsnummer: 0203.201.340
RPR Brussel
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Circulaire

Brussel, 5 mei 2020

Kenmerk: NBB_2020_018

uw correspondent:
Nicolas Strypstein
tel. +32 2 221 44 74
nicolas.strypstein@nbb.be

Aanbevelingen van de Bank inzake uitbesteding aan aanbieders van clouddiensten

Toepassingsveld

Deze circulaire is van toepassing op:

- *verzekerings- en herverzekeringsondernemingen naar Belgisch recht die onderworpen zijn aan de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen (met uitzondering van de verzekeringsondernemingen als bedoeld in de artikelen 275, 276 of 294 van de voornoemde wet van 13 maart 2016);*
- *vergunninghoudende bijkantoren in België van verzekeringsondernemingen waarvan de zetel is gevestigd in een derde land (dat geen partij is bij de Overeenkomst betreffende de Europese Economische Ruimte (EER)); en*
- *entiteiten die verantwoordelijk zijn*[1] *voor een verzekerings- of herverzekeringsgroep naar Belgisch recht in de zin van de artikelen 339, 2°, en 343 van de wet van 13 maart 2016 of voor een financieel conglomeraat naar Belgisch recht in de zin van de artikelen 340, 1°, en 343 van de wet van 13 maart 2016.*

Samenvatting/Doelstelling

Deze circulaire preciseert de aanbevelingen van de Nationale Bank van België (de Bank) inzake uitbesteding aan aanbieders van clouddiensten. Ze geeft uitvoering aan de richtsnoeren van de Europese Autoriteit voor verzekeringen en bedrijfspensioenen (EIOPA) over dit onderwerp en is van toepassing vanaf 1 januari 2021.

Deze circulaire omschrijft ook de aanpak van de Bank op het gebied van rapportering. In dit opzicht dient ze samen gelezen te worden met hoofdstuk 7 van de overkoepelende circulaire betreffende het governancesysteem NBB_2016_31, waarin de algemene aanbevelingen van de Bank inzake uitbesteding nader worden toegelicht (deze aanbevelingen werden recentelijk herzien via mededeling NBB_2020_017).

[1] En meer bepaald verzekerings- of herverzekeringsondernemingen naar Belgisch recht die een deelnemende onderneming in ten minste één verzekerings- of herverzekeringsonderneming in de Europese Economische Ruimte of van een derde land zijn, verzekerings- of herverzekeringsondernemingen naar Belgisch recht met als moederonderneming een gemengde verzekeringsholding of gemengde financiële holding in de Europese Economische Ruimte of van een derde land en verzekeringsholdings of gemengde financiële holdings naar Belgisch recht die moederondernemingen zijn van een verzekerings- of herverzekeringsonderneming naar Belgisch recht, voor zover deze onderworpen zijn aan de bepalingen van de wet van 13 maaart 2016.

Geachte mevrouw
Geachte heer

Conform artikel 92 van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen (hierna de "Toezichtswet Verzekeringen") dient elke verzekerings- of herverzekeringsonderneming passende maatregelen te nemen om te vermijden dat het gebruik van uitbesteding (i) de kwaliteit van het governancesysteem van de onderneming ernstig in gevaar brengt, (ii) het operationeel risico onnodig doet toenemen, (iii) de Nationale Bank van België (de "Bank") verhindert om na te gaan of de onderneming haar wettelijke en reglementaire verplichtingen nakomt en (iv) de continuïteit en de toereikendheid ondermijnt van de dienstverlening aan de verzekeringnemers, de verzekerden en de begunstigden van verzekeringsovereenkomsten of aan de personen die bij de uitvoering van de herverzekeringsovereenkomsten zijn betrokken.

De algemene regels inzake uitbesteding worden omschreven in artikel 274 van Gedelegeerde Verordening 2015/35 van 10 oktober 2014 tot aanvulling van de Solvabiliteit II-richtlijn (hierna "Gedelegeerde Verordening 2015/35") en in hoofdstuk 7 van de overkoepelende circulaire betreffende het governancesysteem NBB_2016_31 (dit hoofdstuk werd recentelijk bijgewerkt via mededeling NBB_2020_017).

Met deze circulaire wenst de NBB bijzondere aanvullende aanbevelingen te verstrekken voor het specifieke geval van uitbesteding aan aanbieders van clouddiensten. Deze aanbevelingen vertalen de "Guidelines on outsourcing to cloud service providers" van EIOPA van 6 februari 2020 in de Belgische regelgeving.

1. Aanbevelingen van de Bank

Definities

Voor de toepassing van deze circulaire gelden de volgende definities:

- Onderneming: een verzekerings- of herverzekeringsonderneming die binnen het hierboven beschreven toepassingsgebied valt.
- Dienstverlener: een derde partij die een proces, een dienst of activiteit, of onderdelen daarvan, uitvoert of verricht op grond van een uitbestedingsovereenkomst.
- Aanbieder van clouddiensten: een dienstverlener, zoals hierboven gedefinieerd, die verantwoordelijk is voor het leveren van clouddiensten in het kader van een uitbestedingsovereenkomst.
- Clouddiensten: diensten geleverd door middel van cloudcomputing, dat wil zeggen een model voor het op aanvraag beschikbaar stellen van netwerktoegang tot een pool van configureerbare IT-middelen (bv. netwerken, servers, opslag, toepassingen en diensten) die met een minimale beheerinspanning of tussenkomst van dienstverleners snel kunnen worden op- en afgeschaald.
- Publieke cloud: cloudinfrastructuur voor vrij gebruik door het algemene publiek.
- Private cloud: cloudinfrastructuur voor exclusief gebruik door één onderneming.
- Gemeenschappelijke cloud: cloudinfrastructuur voor exclusief gebruik door een bepaalde gemeenschap van ondernemingen, bv. meerdere ondernemingen binnen één groep.
- Hybride cloud: cloudinfrastructuur bestaande uit twee of meer onderscheiden cloudinfrastructuren.

Aanbeveling 1 – Clouddiensten en uitbesteding

De onderneming moet bepalen of een overeenkomst met een aanbieder van clouddiensten onder de definitie van uitbesteding in de zin van de Toezichtswet Verzekeringen valt.

Bij deze beoordeling moet worden nagegaan:
a. of de operationele functie of activiteit (of een onderdeel daarvan) die (dat) wordt uitbesteed, periodiek of doorlopend wordt verricht; en
b. of deze operationele functie of activiteit (of een onderdeel daarvan) normaliter tot de operationele functies of activiteiten behoort die door de onderneming in het kader van haar gewone verzekerings- of

herverzekeringsactiviteiten zouden of zouden kunnen worden verricht, zelfs als de onderneming deze operationele functie of activiteit in het verleden niet heeft verricht.

Wanneer een overeenkomst met een dienstverlener betrekking heeft op meerdere operationele functies of activiteiten, moet de onderneming bij haar beoordeling rekening houden met alle aspecten van de overeenkomst.

Wanneer de onderneming operationele functies of activiteiten uitbesteedt aan dienstverleners die geen aanbieders van clouddiensten zijn, maar voor het verrichten van hun diensten sterk afhankelijk zijn van cloudinfrastructuren (bijvoorbeeld wanneer de aanbieder van clouddiensten deel uitmaakt van een onderuitbestedingsketen), valt de uitbestedingsovereenkomst onder het toepassingsgebied van deze Aanbevelingen.

Aanbeveling 2 – Algemene governancebeginselen voor de uitbesteding aan clouddiensten

Onverminderd artikel 274, lid 3, van Gedelegeerde Verordening 2015/35 moeten de raad van bestuur en het directiecomité van de onderneming ervoor zorgen dat elk besluit om kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten uit te besteden, gebaseerd is op een grondige risicobeoordeling, met name van alle relevante risico's die verbonden zijn aan de overeenkomst, zoals informatie- en communicatietechnologierisico's ("ICT"), bedrijfscontinuïteitsrisico's, juridische en compliancerisico's (waaronder vertrouwelijkheid), concentratierisico's, andere operationele risico's en, in voorkomend geval, risico's verbonden aan de gegevensmigratie- en/of uitvoeringsfase.

In geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten moet de onderneming in voorkomend geval in haar beoordeling van het eigen risico en de solvabiliteit ("ORSA") rekening houden met de veranderingen in haar risicoprofiel als gevolg van haar overeenkomsten voor uitbesteding van clouddiensten.

Het gebruik van clouddiensten moet stroken met de strategieën van de onderneming (bijvoorbeeld ICT-strategie, informatiebeveiligingsstrategie, strategie voor operationeel risicobeheer) en met de interne beleidslijnen en processen, die indien nodig moeten worden bijgewerkt.

Aanbeveling 3 – Bijwerking van het schriftelijk uitbestedingsbeleid

In geval van uitbesteding aan aanbieders van clouddiensten moet de onderneming het **schriftelijk uitbestedingsbeleid** bijwerken (bijvoorbeeld door het te herzien, een aparte bijlage toe te voegen of nieuwe specifieke beleidslijnen te ontwikkelen), net zoals de andere relevante interne beleidslijnen (bijvoorbeeld informatiebeveiliging), rekening houdend met de specifieke kenmerken van de uitbesteding van clouddiensten op ten minste de volgende gebieden:

a. de taken en verantwoordelijkheden van de betrokken functies van de onderneming, met name de raad van bestuur en het directiecomité, en de functies die verantwoordelijk zijn voor ICT, informatiebeveiliging, compliance, risicobeheer en interne audit;
b. de processen en rapporteringsprocedures die vereist zijn voor de goedkeuring, de uitvoering, de bewaking, het beheer en, in voorkomend geval, de verlenging van overeenkomsten voor uitbesteding van clouddiensten die betrekking hebben op kritieke of belangrijke operationele functies of activiteiten;
c. het toezicht op de clouddiensten dat in verhouding staat tot de aard, de omvang en de complexiteit van de risico's die inherent zijn aan de verrichte diensten, met inbegrip van (i) de beoordeling van de risico's die verbonden zijn aan de overeenkomsten voor uitbesteding van clouddiensten en de waakzaamheid ten aanzien van aanbieders van clouddiensten, met inbegrip van de frequentie van de risicobeoordeling; (ii) bewakings- en beheerscontroles (bijvoorbeeld verificatie van de "service level agreement"); (iii) veiligheidsnormen en -controles;

d. voor de uitbesteding in de cloud van kritieke of belangrijke operationele functies of activiteiten wordt verwezen naar de contractuele vereisten die beschreven worden in Aanbeveling 8;
e. documentatievereisten en schriftelijke kennisgeving aan de toezichthoudende autoriteit met betrekking tot de uitbesteding in de cloud van kritieke of belangrijke operationele functies of activiteiten;
f. voor elke overeenkomst voor uitbesteding van clouddiensten die kritieke of belangrijke operationele functies of activiteiten betreft, de verplichting om over een gedocumenteerde en, in voorkomend geval, voldoende geteste "exitstrategie" te beschikken die in verhouding staat tot de aard, de omvang en de complexiteit van de risico's die inherent zijn aan de verleende diensten. De exitstrategie kan een reeks van beëindigingsprocessen inhouden, waaronder maar niet noodzakelijkerwijs beperkt tot het staken, het weer bij de onderneming zelf onderbrengen of het overdragen van de diensten die in de overeenkomst voor uitbesteding van clouddiensten zijn opgenomen.

Aanbeveling 4 – Analyse vóór uitbesteding

Alvorens een overeenkomst te sluiten met aanbieders van clouddiensten, moet de onderneming:
a. beoordelen of de overeenkomst voor uitbesteding van clouddiensten een kritieke of belangrijke operationele functie of activiteit betreft, in overeenstemming met Aanbeveling 5;
b. alle relevante risico's van de uitbestedingsovereenkomst identificeren en beoordelen, in overeenstemming met Aanbeveling 6;
c. passende waakzaamheidsmaatregelen ("due diligence") nemen ten aanzien van de mogelijke toekomstige aanbieder van clouddiensten, in overeenstemming met Aanbeveling 7;
d. de belangenconflicten die door de uitbesteding kunnen worden veroorzaakt, identificeren en beoordelen, in overeenstemming met de vereisten van artikel 274, lid 3, onder b), van Gedelegeerde Verordening 2015/35.

Aanbeveling 5 – Beoordeling van het kritieke karakter of het belang van de uitbesteding van clouddiensten

Alvorens een uitbestedingsovereenkomst te sluiten met aanbieders van clouddiensten moet de onderneming beoordelen of de overeenkomst voor uitbesteding van clouddiensten een kritieke of belangrijke operationele functie of activiteit betreft. Bij deze beoordeling moet de onderneming in voorkomend geval nagaan of de overeenkomst in de loop van de tijd kritiek of belangrijk kan worden. Ook moet de onderneming het kritieke karakter of het belang van de operationele functie of activiteit die eerder aan aanbieders van clouddiensten werd uitbesteed, opnieuw beoordelen indien de aard, de omvang en de complexiteit van de risico's die inherent zijn aan de overeenkomst, wezenlijk veranderen.

Bij de beoordeling moet de onderneming niet alleen rekening houden met de uitkomsten van de risicobeoordeling, maar ten minste ook met de volgende factoren:
a. de mogelijke gevolgen van een materiële verstoring van de uitbestede operationele functie of activiteit of van het feit dat de aanbieder van clouddiensten de diensten niet op de overeengekomen niveaus van dienstverlening verricht, voor haar: i. vermogen om continu aan haar regelgevingsverplichtingen te voldoen; ii. financiële veerkracht en levensvatbaarheid op de korte en lange termijn; iii. bedrijfscontinuïteit en operationele veerkracht; iv. operationeel risico, inclusief gedrag, ICT en juridische risico's; v. reputatierisico's;
b. de mogelijke gevolgen van de uitbestedingsovereenkomst op het vermogen van de onderneming om: i. alle relevante risico's te identificeren, te bewaken en te beheren; ii. te voldoen aan alle wettelijke en reglementaire vereisten; iii. passende audits met betrekking tot de uitbestede operationele functie of activiteit uit te voeren;
c. de geaggregeerde blootstelling van de onderneming (en/of van de groep, indien van toepassing) aan dezelfde aanbieder van clouddiensten en de mogelijke cumulatieve gevolgen van uitbestedingsovereenkomsten op hetzelfde werkterrein;

d. de omvang en complexiteit van elk werkterrein van een onderneming waarop de uitbestedingsovereenkomst betrekking heeft;
e. de mate waarin het mogelijk is om de voorgestelde uitbestedingsovereenkomst indien nodig of wenselijk, aan een andere dienstverlener over te dragen of weer bij de onderneming zelf onder te brengen ("vervangbaarheid");
f. de bescherming van persoons- en andere gegevens en de mogelijke gevolgen van een schending van de vertrouwelijkheid of waarborging van de beschikbaarheid en integriteit van gegevens op basis van onder meer Verordening (EU) nr. 2016/67912, voor de onderneming, de verzekeringnemers of andere relevante betrokkenen. De onderneming dient met name rekening te houden met gegevens die bedrijfsgeheim en/of gevoelig zijn (bijvoorbeeld de gezondheidsgegevens van de verzekeringnemers).

Aanbeveling 6 – Beoordeling van de risico's verbonden aan de uitbesteding van clouddiensten

In het algemeen moet de onderneming een aanpak hanteren die in verhouding staat tot de aard, de omvang en de complexiteit van de risico's die inherent zijn aan de diensten die worden uitbesteed aan aanbieders van clouddiensten. Dit houdt in dat de mogelijke gevolgen van de uitbesteding van clouddiensten, met name op hun operationele en reputatierisico's, moeten worden beoordeeld.

In geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten moet de onderneming:
a. rekening houden met de verwachte baten en lasten van de voorgestelde overeenkomst voor uitbesteding van clouddiensten, wat ook inhoudt dat significante risico's die kunnen worden verkleind of beter kunnen worden beheerd, worden afgewogen tegen significante risico's die uit de voorgestelde overeenkomst voor uitbesteding van clouddiensten kunnen voortvloeien;
b. indien van toepassing en van nut, de risico's beoordelen, inclusief juridische, ICT-, compliance- en reputatierisico's, en de daaruit voortvloeiende beperkingen van het toezicht:
    i. de geselecteerde clouddienst en de voorgestelde modellen voor de uitrol van de cloud (d.w.z. publiek/privaat/hybride/gemeenschappelijk);
    ii. de migratie en/of de uitvoering;
    iii. de activiteiten en bijbehorende gegevens en systemen die in beginsel in aanmerking komen voor uitbesteding (of die zijn uitbesteed) en hun gevoeligheid en benodigde veiligheidsmaatregelen;
    iv. de politieke stabiliteit en de veiligheid in de landen (binnen of buiten de EU) waar de uitbestede diensten worden of kunnen worden verricht en waar de gegevens worden of kunnen worden opgeslagen. Bij deze beoordeling moet het volgende worden bekeken: 1. de geldende wetgeving, met inbegrip van de wetten inzake gegevensbescherming; 2. de bestaande voorzieningen voor rechtshandhaving; 3. het insolventierecht dat van toepassing zou zijn in geval van faillissement van een dienstverlener en de mogelijke beperkingen die zich zouden voordoen bij een urgent herstel van de gegevens van de onderneming;
    v. onderuitbesteding, inclusief de aanvullende risico's die zich kunnen voordoen als de onderaannemer in een derde land of een ander land dan de aanbieder van clouddiensten is gevestigd en het risico dat door lange en complexe ketens van onderuitbesteding de onderneming minder goed in staat is toezicht op haar kritieke of belangrijke operationele functies of activiteiten te houden en de toezichthoudende autoriteiten minder goed toezicht op deze ondernemingen kunnen uitoefenen;
    vi. het algemeen concentratierisico van de onderneming ten aanzien van dezelfde aanbieder van clouddiensten, met inbegrip van uitbesteding aan een aanbieder van clouddiensten die niet gemakkelijk kan worden vervangen of meerdere uitbestedingsovereenkomsten met dezelfde aanbieder van clouddiensten.

Bij de beoordeling van het concentratierisico moet de onderneming (en/of, in voorkomend geval, de groep) rekening houden met al haar uitbestedingsovereenkomsten met die aanbieder van clouddiensten.

De risicobeoordeling moet worden uitgevoerd vooraleer de uitbestedingsovereenkomst wordt gesloten. Indien de onderneming kennis krijgt van belangrijke tekortkomingen en/of belangrijke wijzigingen in de geleverde diensten of in de situatie van de aanbieder van clouddiensten, moet de risicobeoordeling onmiddellijk worden herzien of opnieuw worden uitgevoerd. In het geval van een herziening van de inhoud of het toepassingsgebied van de uitbestedingsovereenkomst (bijvoorbeeld uitbreiding van het toepassingsgebied of opname in het toepassingsgebied van kritieke of belangrijke operationele functies die er voorheen niet in waren opgenomen), moet de risicobeoordeling opnieuw worden uitgevoerd.

Aanbeveling 7 – Waakzaamheid ten aanzien van de aanbieder van clouddiensten

Tijdens haar selectie- en beoordelingsprocedure moet de onderneming erop toezien dat de aanbieder van clouddiensten geschikt is overeenkomstig de criteria die in haar schriftelijk uitbestedingsbeleid zijn vastgelegd ("due diligence"-proces).

Het waakzaamheidsonderzoek met betrekking tot de aanbieder van clouddiensten moet worden uitgevoerd vooraleer de operationele functie of activiteit wordt uitbesteed. Indien de onderneming een tweede overeenkomst sluit met een aanbieder van clouddiensten die reeds is beoordeeld, moet de onderneming via een risicogebaseerde aanpak bepalen of er een tweede waakzaamheidsonderzoek moet worden uitgevoerd. Indien de onderneming kennis krijgt van significante tekortkomingen en/of belangrijke wijzigingen in de geleverde diensten of de situatie van de aanbieder van clouddiensten, moet het waakzaamheidsonderzoek onmiddellijk worden herzien of opnieuw worden uitgevoerd.

In geval van uitbesteding van kritieke of belangrijke operationele functies moet het waakzaamheidsonderzoek een beoordeling omvatten van de geschiktheid van de aanbieder van clouddiensten (bijvoorbeeld vaardigheden, infrastructuur, economische situatie, bedrijfs- en regelgevingsstatus). In voorkomend geval kan de onderneming ter ondersteuning van het waakzaamheidsonderzoek gebruikmaken van bewijsmateriaal, certificeringen op basis van internationale normen, auditverslagen van erkende derden of interne auditverslagen.

Aanbeveling 8 – Contractuele vereisten

De respectieve rechten en plichten van de onderneming en van de aanbieder van clouddiensten moeten duidelijk worden afgebakend en in een schriftelijke overeenkomst worden vastgelegd.

Onverminderd de vereisten van artikel 274 van Gedelegeerde Verordening 2015/35 moet, in geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan een aanbieder van clouddiensten, de schriftelijke overeenkomst tussen de onderneming en de aanbieder van clouddiensten het volgende behelzen:

a. een heldere beschrijving van de te verrichten uitbestede functie (clouddiensten, met inbegrip van het soort ondersteunende diensten);
b. de aanvangsdatum en einddatum, indien van toepassing, van de overeenkomst en de opzeggingstermijnen voor de aanbieder van clouddiensten en de onderneming;
c. de bevoegde rechtbank en de wetgeving die op de overeenkomst van toepassing is;
d. de financiële verplichtingen van de partijen;
e. of de onderuitbesteding van een kritieke of belangrijke operationele functie of activiteit (of materiële onderdelen daarvan) is toegestaan en zo ja, de voorwaarden die voor de significante onderuitbesteding gelden (zie Aanbeveling 13);

f. de locatie(s) (d.w.z. regio's of landen) waar de betrokken gegevens zullen worden bewaard en verwerkt (locatie van datacenters), en de voorwaarden waaraan moet worden voldaan, met inbegrip van de vereiste om de onderneming in kennis te stellen als de dienstverlener voorstelt de locatie(s) te wijzigen;
g. bepalingen inzake de toegankelijkheid, beschikbaarheid, integriteit, vertrouwelijkheid, privacy en veiligheid van de betrokken gegevens, rekening houdend met de specificaties van Aanbeveling 10;
h. het recht van de onderneming om de prestaties van de aanbieder van clouddiensten doorlopend te bewaken;
i. de overeengekomen niveaus van dienstverlening, die nauwkeurige kwantitatieve en kwalitatieve prestatiedoelen omvatten om tijdige bewaking mogelijk te maken, zodat zonder onnodig uitstel passende corrigerende maatregelen kunnen worden genomen als de overeengekomen dienstverleningsniveaus niet worden gehaald;
j. de verplichtingen van de aanbieder van clouddiensten inzake rapportering aan de onderneming, inclusief, indien van toepassing, de verplichting om verslagen over te leggen die relevant zijn voor de veiligheidsfunctie en de sleutelfuncties van de onderneming, zoals verslagen van de interneauditfunctie van de aanbieder van de clouddiensten;
k. of de aanbieder van clouddiensten zich verplicht tegen bepaalde risico's dient te verzekeren en, indien van toepassing, de vereiste hoogte van de verzekeringsdekking;
l. de vereiste om bedrijfsnoodplannen ten uitvoer te leggen en te testen;
m. de vereiste voor de aanbieder van clouddiensten om aan de onderneming, haar toezichthoudende autoriteiten en aan iedere andere persoon die door de onderneming of de toezichthoudende autoriteiten is aangewezen: i. volledige toegang te verlenen tot alle relevante bedrijfslocaties (hoofdkantoren en operationele centra), inclusief het volledige scala aan relevante apparatuur, systemen, netwerken, informatie en gegevens die worden gebruikt om de uitbestede functie te verrichten, waaronder bijbehorende financiële informatie, personeel en de externe auditors van de aanbieder van clouddiensten ("toegangsrechten"); ii. een onbeperkt recht van inspectie en audits met betrekking tot de uitbestedingsovereenkomst ("auditrechten"), om hen in staat te stellen de uitbestedingsovereenkomst te bewaken en ervoor te zorgen dat aan alle toepasselijke regelgeving en contractuele voorschriften wordt voldaan;
n. bepalingen die ervoor zorgen dat de gegevens die eigendom van de onderneming zijn, snel kunnen worden hersteld wanneer de aanbieder van clouddiensten insolvent is, zich in een afwikkelingsproces bevindt of zijn bedrijfsactiviteiten beëindigt

Aanbeveling 9 – Toegangs- en auditrechten

De overeenkomst voor uitbesteding van clouddiensten mag de doeltreffende uitoefening van de toegangs- en auditrechten van de onderneming of haar mogelijkheden om controle uit te oefenen op de clouddiensten om aan haar regelgevingsverplichtingen te voldoen, niet beperken.

De onderneming moet haar toegangs- en auditrechten uitoefenen en de auditfrequentie en de te auditeren gebieden en diensten bepalen op grond van een risicogebaseerde aanpak.

Bij het bepalen van de frequentie en de reikwijdte van de uitoefening van haar toegangs- of auditrechten moet de onderneming nagaan of de uitbesteding van clouddiensten betrekking heeft op een kritieke of belangrijke operationele functie of activiteit, en rekening houden met de aard en de omvang van het risico en de gevolgen van de overeenkomsten voor uitbesteding van clouddiensten voor de onderneming.

Indien de omgeving van de aanbieder van clouddiensten en/of van een andere cliënt van dezelfde aanbieder van clouddiensten in gevaar komt door de uitoefening door de onderneming van haar toegangs- of auditrechten of het gebruik van bepaalde auditmethoden (bijvoorbeeld het effect op het niveau van dienstverlening, de beschikbaarheid van gegevens, vertrouwelijkheidsaspecten), moeten de onderneming en de aanbieder van clouddiensten het eens worden over alternatieven om het door de onderneming vereiste niveau van zekerheid en dienstverlening te waarborgen (bijvoorbeeld voorzien in specifieke

controles die moeten worden getoetst in een specifiek verslag of een specifieke certificering die door de aanbieder van de clouddienst wordt opgesteld).

Onverminderd hun eindverantwoordelijkheid voor de activiteiten die door hun aanbieders van clouddiensten worden geleverd, kunnen de ondernemingen, om de auditmiddelen doelmatiger te gebruiken en de organisatorische lasten voor de aanbieder van clouddiensten en zijn cliënten te verminderen, gebruikmaken van:

a. door de aanbieder van clouddiensten verstrekte externe certificeringen en externe of interne auditverslagen;
b. gemeenschappelijke audits die samen met andere cliënten van dezelfde aanbieder van clouddiensten worden georganiseerd of gemeenschappelijke audits die door een door hen aangestelde derde worden uitgevoerd.

In geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten mogen de ondernemingen enkel gebruikmaken van externe certificeringen en externe of interne auditverslagen op voorwaarde dat zij:

a. erop toezien dat de certificering of het auditverslag betrekking heeft op de systemen (bijvoorbeeld processen, applicaties, infrastructuur, datacentra, enz.) en controles die door de onderneming als essentieel zijn aangemerkt, en de naleving van de relevante regelgevingsvereisten beoordelen;
b. nieuwe certificeringen of auditverslagen continu grondig beoordelen en nagaan of de certificeringen of verslagen niet verouderd zijn;
c. erop toezien dat ook toekomstige versies van de certificering of het auditverslag betrekking hebben op essentiële systemen en controles;
d. een redelijke mate van zekerheid hebben over de geschiktheid van de certificerende of controlerende partij (bijvoorbeeld met betrekking tot de roulering van de certificerende of controlerende organisatie, kwalificaties, deskundigheid, herhaling van de uitvoering/controle van bewijsstukken in het betrokken auditdossier);
e. een redelijke mate van zekerheid hebben dat de certificeringen zijn afgegeven en de audits zijn uitgevoerd overeenkomstig passende normen en dat zij een toetsing omvatten van de operationele doeltreffendheid van de aanwezige essentiële controles;
f. contractueel gerechtigd zijn te verzoeken om uitbreiding van de reikwijdte van de certificeringen of auditverslagen tot andere relevante systemen en controles; het aantal en de frequentie van dergelijke verzoeken dienen redelijk te zijn en vanuit het oogpunt van risicobeheer gerechtvaardigd zijn;
g. het contractuele recht behouden om naar eigen inzicht afzonderlijke audits ter plaatse met betrekking tot de uitbesteding van kritieke of belangrijke operationele functies of activiteiten uit te voeren; dit recht wordt uitgeoefend indien dit vereist wordt door specifieke behoeften waaraan niet kan worden voldaan via andere soorten interacties met de aanbieder van de clouddiensten.

Bij uitbesteding van kritieke of belangrijke operationele functies aan aanbieders van clouddiensten moet de onderneming beoordelen of de in het vijfde lid van deze aanbeveling, onder a) bedoelde externe certificeringen en verslagen adequaat en voldoende zijn om aan haar regelgevingsverplichtingen te voldoen en mag zij, op grond van een risicogebaseerde aanpak, op termijn niet uitsluitend op deze verslagen en certificeringen vertrouwen.

Vóór een gepland bezoek ter plaatse dient de partij die haar recht van toegang wil uitoefenen (onderneming, auditor of derde die namens de onderneming(en) handelt) de aanbieder van clouddiensten een redelijke tijd van tevoren in kennis te stellen, tenzij dat vanwege een nood- of crisissituatie niet mogelijk is. Deze kennisgeving moet de locatie en het doel van het bezoek vermelden, evenals het personeel dat aan het bezoek zal deelnemen.

Gezien het feit dat cloudoplossingen technisch gezien bijzonder complex zijn, dient de onderneming na te gaan of het personeel dat de audit uitvoert – namelijk haar eigen interne auditors, of de namens haar handelende pool van auditors, of de door de aanbieder van clouddiensten aangewezen auditors - of, in voorkomend geval, het personeel dat de externe certificering of auditverslagen van de dienstverlener controleert, de juiste vaardigheden en kennis heeft om de desbetreffende audits en/of beoordelingen uit te voeren.

Aanbeveling 10 - Beveiliging van gegevens en systemen

De onderneming moet ervoor zorgen dat de aanbieders van clouddiensten voldoen aan de Europese en nationale regelgeving en aan de juiste ICT-beveiligingsnormen.

In geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten moet de onderneming in de uitbestedingsovereenkomst specifieke eisen voor de beveiliging van gegevens vaststellen en er voortdurend op toezien dat deze eisen worden nageleefd.

Voor de toepassing van het voorgaande lid moet de onderneming, in geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten aan aanbieders van clouddiensten, op grond van een risicogebaseerde aanpak en rekening houdend met haar verantwoordelijkheden en die van de aanbieder van de clouddiensten:

a. overeenstemming bereiken over de respectieve taken en verantwoordelijkheden van de aanbieder van clouddiensten en de onderneming met betrekking tot de operationele functies of activiteiten waarop de uitbesteding betrekking heeft, die duidelijk moeten worden afgebakend;
b. in het kader van de voorgenomen uitbesteding van clouddiensten passende bescherming voor de vertrouwelijkheid van gegevens, de continuïteit van de uitbestede activiteiten, en de integriteit en herleidbaarheid van gegevens en systemen definiëren en vaststellen;
c. in voorkomend geval nagaan of er specifieke maatregelen nodig zijn voor gegevens in transit, opgeslagen gegevens en gegevens in rusttoestand, zoals de toepassing van versleutelingstechnologieën (encryptie) in combinatie met een passend sleutelbeheer;
d. de mechanismen om de clouddiensten te integreren in de systemen van de ondernemingen, bijvoorbeeld de Application Programming Interfaces (APIs) en een degelijk gebruikers- en toegangsbeheerproces onder de loep nemen;
e. indien van toepassing en haalbaar, er contractueel voor zorgen dat de beschikbaarheid van het netwerkverkeer en de verwachte capaciteit voldoen aan strenge continuïteitsvereisten;
f. passende continuïteitsvereisten definiëren en vaststellen om, indien van toepassing, op elk niveau van de technologische keten adequate niveaus te waarborgen;
g. beschikken over een degelijk en goed gedocumenteerd proces voor het beheer van incidenten, inclusief de respectieve verantwoordelijkheden, bijvoorbeeld door de vaststelling van een samenwerkingsmodel voor het geval er zich feitelijke of vermoede incidenten voordoen;
h. een risicogebaseerde aanpak hanteren met betrekking tot de locatie(s) van gegevensopslag en -verwerking (d.w.z. land of regio) en overwegingen over de beveiliging van informatie;
i. de naleving van de vereisten met betrekking tot de doeltreffendheid en efficiëntie van de controlemechanismen die door de aanbieder van de clouddiensten worden toegepast en die de risico's verbonden aan de verrichte diensten zouden beperken, bewaken.
j. ervoor zorgen dat een kopie van de gegevens wordt opgeslagen in een of meer locaties buiten de hoofdvestiging van de aanbieder van clouddiensten die beveiligd zijn en voldoende ver verwijderd zijn van de hoofdvestiging zodat deze niet wordt blootgesteld aan dezelfde risico's, alsook, voor kritieke gegevens, onderzoeken of het mogelijk is om onafhankelijk van de aanbieder van clouddiensten een kopie te hebben, zodat de activiteiten kunnen worden hervat in het geval van een permanent in gebreke blijven van de dienstverlener;

k. ervoor zorgen dat de toegang van de beheerders van de clouddiensten wordt beschermd door sterke authenticatieoplossingen;
l. er contractueel voor zorgen dat de beheerders van de aanbieder van clouddiensten geen permanente toegang hebben tot haar systemen en gegevens, in overeenstemming met het "least privilege"-beginsel;
m. nagaan of er adequate oplossingen kunnen worden gevonden om elke ongewenste blootstelling van het dataverkeer tussen de onderneming en de clouddienst te voorkomen.

Aanbeveling 11 – Onderuitbesteding

Indien de onderuitbesteding van kritieke of belangrijke operationele functies (of een onderdeel daarvan) wordt toegestaan, moet de uitbestedingsovereenkomst tussen de onderneming en de aanbieder van clouddiensten minstens de volgende elementen bevatten:

a. de vermelding van alle soorten activiteiten die uitgesloten zijn van onderuitbesteding;
b. de voorwaarden waaraan de onderuitbesteding moet voldoen, bijvoorbeeld dat de onderaannemer ook volledig voldoet aan de bestaande verplichtingen van de aanbieder van clouddiensten. Deze verplichtingen omvatten de audit- en toegangsrechten en de beveiliging van gegevens en systemen;
c. de aanbieder van clouddiensten blijft volledig verantwoordelijk voor de onderuitbestede diensten en het toezicht daarop;
d. wanneer de aanbieder van clouddiensten belangrijke wijzigingen voorneemt wat betreft onderaannemers of onderuitbestede diensten en deze wijzigingen de aanbieder van clouddiensten zouden kunnen hinderen de verplichtingen uit hoofde van de uitbestedingsovereenkomst ten volle na te komen, is de aanbieder van clouddiensten verplicht om de onderneming in kennis te stellen van deze voorgenomen wijzigingen. De kennisgevingstermijn voor dergelijke wijzigingen wordt zodanig vastgesteld dat de onderneming in staat is ten minste de risico's als gevolg van de voorgestelde wijzigingen wat betreft de onderaannemers of de onderuitbestede diensten te beoordelen voordat zij daadwerkelijk van kracht worden;
e. wanneer de aanbieder van clouddiensten wijzigingen voorneemt wat betreft onderaannemers of onderuitbestede diensten en deze wijzigingen een nadelig effect zouden kunnen hebben op de beoordeling van de risico's die aan de overeengekomen diensten zijn verbonden, heeft de onderneming het recht bezwaar te maken tegen dergelijke wijzigingen en/of is de onderneming gerechtigd de overeenkomst te beëindigen.

Aanbeveling 12 – Opvolging van en toezicht op overeenkomsten voor uitbesteding van clouddiensten

De onderneming moet de uitvoering van de activiteiten, de beveiligingsmaatregelen en de naleving van het overeengekomen dienstverleningsniveau door haar aanbieders van clouddiensten regelmatig volgen op grond van een risicogebaseerde aanpak. De aandacht dient gevestigd te worden op de uitbesteding van kritieke en belangrijke operationele functies.

Daartoe moet de onderneming in voorkomend geval opvolgings- en toezichtsmechanismen opzetten die, voor zover haalbaar, rekening houden met het feit dat kritieke of belangrijke operationele functies of een onderdeel daarvan worden onderuitbesteed.

Het directiecomité moet regelmatig op de hoogte worden gebracht van de vastgestelde risico's met betrekking tot de uitbesteding van kritieke of belangrijke operationele functies of activiteiten.

Om hun overeenkomsten voor de uitbesteding van clouddiensten op passende wijze te kunnen opvolgen en om er een passend toezicht op te kunnen uitoefenen, moeten de ondernemingen over voldoende personele middelen met passende vaardigheden en kennis beschikken om de uitbestede diensten te op te volgen. Het personeel van de onderneming dat met deze activiteiten is belast, moet over de ICT- en bedrijfskennis beschikken die noodzakelijk worden geacht.

Aanbeveling 13 – Beëindigingsrechten en exitstrategieën

In geval van uitbesteding van kritieke of belangrijke operationele functies of activiteiten moet de overeenkomst voor uitbesteding van clouddiensten een duidelijk omschreven clausule over exitstrategie bevatten zodat de onderneming de overeenkomst indien nodig kan beëindigen zonder dat dit ten koste gaat van de continuïteit en de kwaliteit van haar dienstverlening aan cliënten. Daartoe moet de onderneming:

a. exitplannen ontwikkelen die volledig, servicegebaseerd, gedocumenteerd en voldoende getoetst zijn (bijvoorbeeld door de mogelijke kosten, gevolgen, middelen en tijdsimplicaties van de verschillende mogelijke exitopties te analyseren);
b. alternatieve oplossingen zoeken en passende en haalbare overgangsplannen opstellen waarmee zij bestaande activiteiten en gegevens bij de aanbieder van clouddiensten kan weghalen en naar andere dienstverleners kan overbrengen of weer bij de onderneming zelf kan onderbrengen. Hierbij dient rekening te worden gehouden met de uitdagingen die zich kunnen voordoen vanwege de locatie van de gegevens en moeten de nodige maatregelen worden genomen om in de overgangsfase de bedrijfsactiviteit te waarborgen;
c. waarborgen dat de aanbieder van clouddiensten de onderneming voldoende ondersteunt om de uitbestede gegevens, systemen of toepassingen over te brengen naar een andere dienstverlener of weer bij de onderneming zelf onder te brengen;
d. met de aanbieder van clouddiensten overeenkomen dat haar gegevens na de overbrenging naar de onderneming in alle regio's volledig en veilig door de aanbieder van clouddiensten worden gewist.

Bij het bepalen van een exitstrategie neemt de onderneming het volgende in overweging:

a. zij bepaalt de doelstellingen van de exitstrategie;
b. zij bepaalt de indicatoren die aanleiding kunnen geven tot een activering van de exitstrategie ("triggering events"), bijvoorbeeld belangrijke risico-indicatoren die aangeven wanneer de dienstverlening onaanvaardbaar is geworden;
c. zij voert een businessimpactanalyse uit van de potentiële bedrijfsschade in verhouding tot de uitbestede activiteiten om na te gaan welke personele en materiële middelen nodig zouden zijn om het exitplan uit te voeren en hoe lang dat zou duren;
d. zij wijst taken en verantwoordelijkheden toe voor het beheer van exitplannen en overgangsactiviteiten;
e. zij stelt criteria vast om te bepalen of de overgang geslaagd is.

Aanbeveling 14 – Cloud uitbesteding in een derde land

Onverminderd het bepaalde in afdeling 7.4.3. van de overkoepelende circulaire betreffende governance is uitbesteding aan een aanbieder van clouddiensten waarvan de gegevens zich buiten de Europese Economische Ruimte (in niet-EER-landen of derde landen) bevinden, toegestaan op voorwaarde dat de onderneming uitdrukkelijk kan waarborgen dat zijzelf, haar commissaris-erkend revisor en de Bank hun recht op inzage en nazicht (audit) kunnen uitoefenen en doen toepassen overeenkomstig artikel 307 van de Toezichtswet Verzekeringen. Dit impliceert dat de onderneming, haar commissaris-erkend revisor en de Bank in België te allen tijde toegang moeten hebben tot de gegevens die zich buiten de EER bevinden.

Naast deze algemene regel moet de uitbesteding aan een aanbieder van clouddiensten waarvan de gegevens zich in een derde land bevinden, indien dit als een kritieke of belangrijke uitbesteding wordt beschouwd, voldoen aan de volgende voorwaarden:

a. er bestaat een samenwerkingsovereenkomst tussen de Bank en de prudentiële toezichthouder van het derde land waar de gegevens zich bevinden of, indien de aanbieder van clouddiensten deel uitmaakt van een groep die is onderworpen aan toezicht op groepsniveau in overeenstemming met Richtlijn 2009/138/EG (artikel 343 van de Toezichtswet Verzekeringen), bestaat er een coördinatieafspraak met betrekking tot een college van toezichthouders waarbij de Bank en de prudentiële toezichthouder van het derde land partij zijn; en

b. de in punt a. bedoelde samenwerkingsovereenkomst of coördinatieafspraak waarborgt dat de Bank ten minste in staat is om, enerzijds, op verzoek de informatie te verkrijgen die noodzakelijk is voor het uitvoeren van haar taken en, anderzijds, passende toegang te krijgen tot gegevens, documenten, locaties of personeel in het derde land die van belang zijn voor de uitoefening van haar toezichtsbevoegdheden (artikel 307 van de Toezichtswet Verzekeringen).

Deze twee voorwaarden moeten echter niet vervuld zijn als de aanbieder van clouddiensten waarvan de gegevens zich in een derde land bevinden, deze gegevens toegankelijk en controleerbaar maakt vanuit een in de EER gevestigd(e) dochteronderneming of bijkantoor.

Aanbeveling 15 – Bewaring van verzekeringsdocumenten

Er gelden specifieke regels wanneer de uitbesteding van clouddiensten betrekking heeft op de bewaring van de originele exemplaren van (i) de verzekerings-of herverzekeringsovereenkomsten (polissen en aanhangsels), (ii) de brieven die worden verzonden aan de verzekeringnemers en (iii) de prudentiële rapporteringen die zijn vereist op grond van de Toezichtswet Verzekeringen en die welke zijn vereist op grond van de wet van 4 april 2014 betreffende de verzekeringen.

Artikel 76 van de Toezichtswet Verzekeringen bepaalt immers dat deze documenten moeten worden bewaard op de zetel van de onderneming of op een andere plaats die vooraf door de Bank is goedgekeurd in overleg met de FSMA.

Bijgevolg dienen de ondernemingen die voornemens zijn een beroep te doen op aanbieders van clouddiensten om de bovengenoemde documenten te bewaren, niet alleen de regels van deze circulaire maar ook de door de Bank uitgewerkte aanvullende regels voor de bewaring van verzekeringsdocumenten naleven.

2. Documentatie en rapportering aan de Bank

2.1. Interne documentatie

Zoals vermeld in afdeling 7.6. van de overkoepelende circulaire betreffende governance wordt uitbestedende ondernemingen aanbevolen een register bij te houden met informatie over al hun (al dan niet kritieke/belangrijke) uitbestedingsovereenkomsten. Meer specifiek wat betreft de uitbesteding van clouddiensten wordt de onderneming aanbevolen een administratie bij te houden van haar overeenkomsten in dat register (dat regelmatig wordt bijgewerkt). De onderneming wordt ook aangeraden een administratie bij te houden van de beëindigde overeenkomsten voor de uitbesteding van clouddiensten, en dit gedurende een passende bewaarperiode. De onderneming moet op verzoek aan de Bank alle informatie beschikbaar stellen die nodig is om deze laatste in staat te stellen toezicht op de onderneming uit te oefenen, waaronder een kopie van de uitbestedingsovereenkomst.

2.2. Rapportering aan de Bank

De algemene verplichtingen inzake rapportering over uitbesteding zijn opgenomen in afdeling 7.6. van de overkoepelende circulaire betreffende governance.

2.2.1. Lijst van kritieke of belangrijke uitbestedingen

De als kritiek of belangrijk beschouwde uitbestedingen van clouddiensten moeten worden opgenomen in de lijst van kritieke of belangrijke uitbestedingen die doorlopend moet worden bezorgd aan de Bank via het eCorporate-platform (rapportering B.9 als vermeld in de eCorporate-mededeling).

Voor als kritiek of belangrijk beschouwde uitbestedingen van clouddiensten moet deze lijst dezelfde informatie bevatten als voor alle andere kritieke of belangrijke uitbestedingen (cf. afdeling 7.6. van de overkoepelende circulaire betreffende governance), maar ook de volgende aanvullende informatie:

(i) dat het gaat om uitbesteding van clouddiensten;
(ii) de datum waarop voor het laatst een risicobeoordeling heeft plaatsgevonden, en een korte samenvatting van de belangrijkste resultaten;
(iii) de data van de meest recente en volgende geplande audits, indien van toepassing;
(iv) de uitkomsten van de beoordeling van de vervangbaarheid van de aanbieder van clouddiensten (bijvoorbeeld gemakkelijk, moeilijk of onmogelijk); en
(v) of de onderneming een exitstrategie heeft voor het geval van beëindiging door een van beide partijen of verstoring van de dienstverlening door de aanbieder van clouddiensten.

2.2.2. Kennisgeving aan de Bank

Voor de voorafgaande kennisgeving aan de Bank voor een nieuwe kritieke of belangrijke uitbesteding van clouddiensten moet het standaardformulier worden gebruikt opgenomen in bijlage 4 van de overkoepelende circulaire betreffende governance[2]. Voor de uitbesteding van clouddiensten moeten bepaalde aanvullende bijlagen die nader worden toegelicht in het punt Bijlagen, onder c. van dat formulier worden bezorgd aan de Bank.

De Bank vraagt de ondernemingen ook om haar onverwijld in kennis te stellen van materiële wijzigingen en/of kritische incidenten met betrekking tot de uitbesteding van clouddiensten. Deze kennisgeving kan gebeuren via een bijwerking van het oorspronkelijke formulier.

Daarnaast wordt overeenkomstig de algemene regels inzake uitbesteding van hoofdstuk 7 van de overkoepelende circulaire betreffende governance verduidelijkt dat bij het aan de Bank te bezorgen kennisgevingsdossier voor een belangrijke of kritieke uitbesteding van clouddiensten altijd een advies moet worden gevoegd van de verantwoordelijke voor de compliancefunctie waarin de naleving van de governanceregels inzake uitbesteding alsook de volledigheid van de ingediende kennisgeving wordt bevestigd (cf. bijlage 5 van de overkoepelende circulaire betreffende governance).

3. Inwerkingtreding

Deze circulaire is van toepassing vanaf 1 januari 2021. Dit houdt in dat alle uitbestedingen die vanaf deze datum worden aangegaan, hernieuwd of aangepast door de verzekerings- of herverzekeringsondernemingen in overeenstemming moeten zijn met deze circulaire.

Voor reeds bestaande en lopende uitbestedingen van clouddiensten die betrekking hebben op kritieke of belangrijke operationele functies of activiteiten, hebben de ondernemingen tot 31 december 2022 om aan deze circulaire te voldoen[3]. Tot dan blijven deze uitbestedingen onderworpen aan mededeling NBB_2012_11 over de prudentiële verwachtingen ten aanzien van Cloud Computing. Deze circulaire heft mededeling NBB_2012_11 over de prudentiële verwachtingen ten aanzien van Cloud Computing dus definitief op vanaf 1 januari 2023.

2 Als een uitbesteding van clouddiensten die oorspronkelijk niet als kritiek of belangrijk werd beschouwd, dit na een bepaalde tijd wel wordt, moet de verzekeringsonderneming de Bank hiervan ook onmiddellijk op de hoogte brengen via het in bijlage 1 opgenomen formulier.

3 Wanneer het onderzoek van de overeenkomsten voor uitbesteding van clouddiensten die betrekking hebben op kritieke of belangrijke operationele functies of activiteiten niet is afgerond op 31 december 2022, stelt de onderneming de Bank hiervan onmiddellijk in kennis, waarbij zij toelichting geeft over de maatregelen die zijn gepland om dit onderzoek af te ronden of over de eventuele exitstrategie. In voorkomend geval kan de Bank met de onderneming een langere termijn overeenkomen om dit onderzoek te voltooien. Voor het onderzoek van reeds bestaande en lopende uitbestedingen van clouddiensten die geen betrekking hebben op kritieke of belangrijke functies of activiteiten, moet de onderneming de Bank vóór 31 december 2022 laten weten of zij al dan niet van plan is deze uitbestedingen in overeenstemming te brengen met de *guidelines* EIOPA.

Er wordt een kopie van deze circulaire verzonden naar de commissaris(sen), erkend revisor(en) van uw onderneming.

Hoogachtend

Pierre WUNSCH
Gouverneur