de Berlaimontlaan 14 – BE-1000 Brussel
tel. +32 2 221 37 40 – fax + 32 2 221 31 04
ondernemingsnummer: 0203.201.340
RPR Brussel
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Circulaire

Brussel, 19 juni 2018

Kenmerk: NBB_2018_20

uw correspondent:

Thomas Bodequin
tel. +32 2 221 53 65 – fax +32 2 221 31 04
thomas.bodequin@nbb.be

EBA aanbevelingen inzake uitbesteding aan aanbieders van clouddiensten

Toepassingsveld

Deze circulaire is van toepassing op kredietinstellingen en beursvennootschappen naar Belgisch recht, en in België gevestigde bijkantoren van kredietinstellingen en beursvennootschappen die ressorteren onder het recht van een staat die geen lid is van de EER.

Samenvatting/Doelstelling

Deze circulaire geeft uitvoering aan de aanbevelingen van de Europese Bankautoriteit (hierna, de “EBA”) inzake uitbesteding aan aanbieders van clouddiensten en dient samen gelezen te worden met circulaire PPB_2004/5 over gezonde beheerspraktijken bij uitbesteding door kredietinstellingen en beleggingsondernemingen[1] en mededeling NBB_2012_11 over de prudentiële verwachtingen ten aanzien van Cloud Computing.

Geachte mevrouw
Geachte heer

Conform artikel 66 van de wet van 25 april 2014 (hierna, de "Bankwet”) dient elke instelling passende maatregelen te nemen om, enerzijds, het operationeel risico dat gepaard gaat met uitbesteding te beperken en, anderzijds, geen wezenlijke afbreuk te doen aan het passende karakter van de interne controleprocedures van de instelling of aan de mogelijkheid van de toezichthouder om na te gaan of de instelling haar wettelijke en reglementaire verplichtingen nakomt.

Met deze circulaire wenst de NBB aan te geven dat de aanbevelingen van de EBA inzake uitbesteding aan aanbieders van clouddiensten geïntegreerd zijn in haar toezichtspraktijk.

De circulaire omvat een korte samenvatting van de EBA-aanbevelingen inzake uitbesteding aan aanbieders van clouddiensten. Instellingen dienen zich tot het uiterste in te spannen om integraal aan deze aanbevelingen te voldoen. Deze aanbevelingen kunnen in beide landstalen geconsulteerd worden op de website van de EBA via volgende link:
https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers

[1] De EBA heeft de intentie om de CEBS-richtsnoeren met betrekking tot uitbesteding te herzien en de aanbevelingen inzake uitbesteding aan aanbieders van clouddiensten in deze nieuwe richtsnoeren te integreren. Deze nieuwe richtsnoeren worden verwacht in de loop van 2019.

Net zoals deze EBA-aanbevelingen inzake uitbesteding aan aanbieders van clouddiensten een aanvulling zijn op de CEBS-richtsnoeren inzake uitbesteding, is deze circulaire een inhoudelijke aanvulling op de circulaire PPB-2004/5 en mededeling NBB_2012_11 van de NBB. Dit houdt in dat de circulaire PPB-2004/5 en mededeling 2012_11 onverminderd van toepassing blijven.

Deze circulaire treedt in werking op 1 juli 2018.

Korte samenvatting:

Instellingen dienen, alvorens een activiteit of deel daarvan uit te besteden, de materialiteit van deze activiteit te beoordelen. Hierbij dient vooral aandacht besteed te worden aan de potentiële impact die een onderbreking van de dienstverlening zou hebben, maar ook aan de impact van een slechte dienstverlening en van een schending van de vertrouwelijkheid van of het verlies van gegevens.

Instellingen die een activiteit wensen uit te besteden die zij materieel beschouwen, dienen de toezichthouder hierover voorafgaand te informeren. De aanbevelingen bevatten een lijst van informatie die minimum aan de toezichthouder gerapporteerd moet worden. De toezichthouder kan vervolgens bijkomende informatie[2] vragen indien hij dit nodig acht.

Instellingen dienen daarnaast een register bij te houden, ook op groepsniveau indien van toepassing, die alle uitbestedingen bevat ongeacht of zij materieel zijn. De aanbevelingen bevatten een lijst van informatie die tenminste in dit register vervat moet zijn. Op vraag van de toezichthouder deelt de instelling dit register alsook een kopie van de uitbestedingsovereenkomsten die de toezichthouder wenst na te kijken.

Verder dienen instellingen ruime garanties te bieden inzake toegangs- en auditrechten. Daartoe dienen zij specifieke voorzieningen op te nemen in de uitbestedingsovereenkomsten, en ervoor te zorgen dat de toegangs- en auditrechten op geen enkele manier verhinderd of beperkt worden. Dit zowel wat betreft deze rechten voor de instelling zelf, als voor de toezichthouder en elke derde partij door hen aangeduid inclusief de interne en externe auditor.

Deze toegangs- en auditrechten moeten uitgeoefend worden, proportioneel met het risico. Gelet op de bijzonderheden van aanbieders van clouddiensten, stellen de aanbevelingen enkele alternatieve auditinstrumenten voor die gehanteerd kunnen worden voor deze uitbestede diensten: gemeenschappelijke audits ('pooled audits'), certificering door derden, en externe en interne auditrapporten (van de aanbieder van clouddiensten). De toegangs- en auditrechten zoals hierboven beschreven blijven evenwel onverminderd van toepassing en deze alternatieve instrumenten kunnen enkel gebruikt worden indien zij als passend kunnen beschouwd worden. Zie ook hier de aanbevelingen voor enkele minimumvereisten.

Instellingen moeten toezien op de continuïteit en de kwaliteit van de geleverde diensten. Daartoe nemen zij verschillende maatregelen, waaronder: (i) een onderzoek voorafgaand aan de uitbesteding dat nagaat of een activiteit geschikt is om uitbesteed te worden, en de gevoeligheid van de betrokken gegevens en systemen analyseert evenals de aangewezen bescherming ervan, (ii) het vastleggen van de prestatievereisten inzake kwaliteit, continuïteit en bescherming van gegevens, en, (iii) het monitoren van de prestaties, waaronder ook het opvolgen van incidenten en het eventueel nemen van corrigerende maatregelen.

Instellingen dienen bijzonder voorzichtig te zijn bij het uitbesteden naar landen buiten de EER, en ervoor te zorgen dat zij geen buitensporige risico's nemen inzake gegevensbescherming, en dat de toezichthouder doeltreffend toezicht kan houden op de uitbestede activiteiten. De instelling onderzoekt de mogelijke juridische en compliance risico's die gepaard gaan met het uitbesteden naar derde landen, inclusief in geval van faling van de dienstverlener, en houdt hierbij rekening met alle landen waar diensten geleverd kunnen worden en alle plaatsen waar de gegevens mogelijk opgeslagen of verwerkt kunnen worden.

2 Dit slaat in de eerste plaats op de zaken waarvoor de NBB een degelijke documentatie verwacht in lijn met circulaire PPB_2004/5, zoals onder meer de grondige risico-evaluatie voorafgaand aan de uitbesteding.

Bij het afsluiten van uitbestedingsovereenkomsten wordt vastgelegd welke zaken uitgesloten zijn van onderuitbesteding. Bij onderuitbesteding moet de onderaannemer de verplichtingen die gelden tussen de uitbestedende instelling en de dienstverlener nakomen en dient de instelling op dezelfde manier de diensten geleverd via onderuitbesteding te monitoren. De uitbestedende instelling wordt voorafgaandelijk ingelicht bij wijzigingen in de onderuitbesteding en krijgt de kans deze wijzigingen te beoordelen. Indien deze wijzigingen het risico voor de instelling buitensporig verhogen, kan de instelling de overeenkomst vroegtijdig stopzetten.

Tot slot dienen instellingen operationele continuïteitsplannen en exitstrategieën te hebben, zodat zij de continuïteit en kwaliteit van de dienstverlening jegens hun klanten kunnen garanderen. Deze plannen kunnen bijvoorbeeld bestaan uit het opnieuw zelf uitoefenen van uitbestede activiteiten of het overschakelen naar een andere dienstverlener. Deze plannen besteden de nodige aandacht aan de snelheid waarmee ze uitgevoerd kunnen worden en de mogelijke hindernissen die de instelling hierbij kan ondervinden, onder meer inzake het recupereren van data bij dienstverleners.

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

Hoogachtend

Jan Smets
Gouverneur