



# UW CLOUD-CONTRACT ONDER DE LOEP

## ENKELE JURIDISCHE VUISTREGELS OP EEN RIJ

Cloud computing is op korte tijd geëvolueerd van een hype naar een alledaagse tool. Tijd om even stil te staan bij enkele juridische aandachtspunten. Eerst wordt het begrip cloud computing vanuit juridisch oogpunt nader toegelicht. Daarna worden enkele rechtsregels van toepassing op cloud computing en enkele contractuele aandachtspunten nader besproken. Er wordt afgesloten met een overzicht van de beleidsinitiatieven die momenteel ondernomen worden op Europees niveau.

### **BESTAAT ER EEN JURIDISCHE DEFINITIE VAN CLOUD COMPUTING?**

Onder Belgisch recht wordt het concept cloud computing niet gedefinieerd in een wet of ander bindend juridisch document. Er bestaat (op heden) dus geen wettelijke definitie van het begrip. In de literatuur wordt cloud computing uiteraard wel omschreven en in deze beschrijvingen komen steeds enkele gemeenschappelijke kenmerken terug. In essentie maakt cloud computing het mogelijk om toegang te krijgen tot toepassingen en gegevens via tussenpersonen die hun diensten aanbieden over het internet. Een online emailaccount, een virtuele desktop, een online sociale media-platform, enzovoort kunnen dus voorbeelden zijn van cloud-dienstverlening. Echter, om cloud computing te onderscheiden van een “gewoon” hostingcontract, waarbij bedrijven reeds vóór de cloud-ontwikkeling beroep deden op derde partijen om via externe datacenters toegang te krijgen tot hun gegevens

via het internet (zoals hierboven omschreven), dienen een aantal kenmerken aanwezig te zijn om te kunnen spreken van cloud computing.

Zo worden typisch als kenmerken van een cloud-oplossing aangemerkt:

- **Schaalbaarheid** of “elasticiteit”: de klant kan heel snel de gewenste computing capaciteit aanpassen naar gelang de behoefte, bijvoorbeeld einde boekjaar wanneer gedurende een aantal dagen of weken meer capaciteit nodig is dan op andere ogenblikken;
- **Schaalvoordelen**: deze worden bewerkstelligd doordat dezelfde oplossing op een gestandaardiseerde manier wordt aangeboden aan een veelheid van klanten, wat overigens de prijs van de dienst normaliter doet dalen;
- **Ergens “in de wolken”**: men kan vanop om het even welke locatie toegang nemen tot de toepassingen of gegevens die zich om het even waar bevinden)

- **On demand**: de cloud cliënt moet slechts een minimale inspanning doen om van het aanbod te genieten; in principe dient hij slechts de stekker in te steken en over een internet-connectie te beschikken. Andere investeringen zijn niet langer nodig.

### **HET WETTELIJK EN CONTRACTUEEL KADER VAN TOEPASSING OP CLOUD COMPUTING**

Cloud computing biedt enorme voordelen. De investeringskost in eigen IT-infrastructuur neemt drastisch af, de dienstverlening is vaak relatief goedkoop en de toepassingen zijn doorgaans gebruiksvriendelijk en aangepast aan de noden van de gebruiker. Zeker indien de dienst reeds een tijd wordt aangeboden, aangezien ze dan doorgaans wordt afgenomen door een grotere groep van klanten als standaarddienst en ze normaal gezien is bijgeschaafd op een aantal punten. Het is uiteraard ook zo dat aan het gebruik van cloud computing, net zoals



ANTOON DIERICK  
PATRICK VAN EECKE  
DLA PIPER



met andere types van diensten, bepaalde risico's verbonden zijn. Zo toont recent onderzoek aan dat er zich toch een aantal aandachtspunten stellen alvorens over te schakelen op de cloud:

- Beveiligingsrisico's: op welke wijze worden de gegevens die in de cloud geplaatst worden fysiek en logisch beveiligd?
- Operationele risico's: wat indien bedrijfskritische gegevens of toepassingen die een bedrijf nodig heeft voor haar dagelijkse activiteit plots niet meer toegankelijk zijn en er geen back-up is voorzien?
- Reputatierisico's: Wat indien de dienst die door de onderneming zelf aan haar eigen klanten wordt aangeboden, niet meer geleverd kan worden door een fout in de cloud-dienst?

Deze risico's tonen aan dat betwistingen tussen cloud-dienstverlener en cloud-afnemer mogelijk zijn. Vanuit juridisch oogpunt is het dan ook nuttig te weten welke regels de verhouding tussen de partijen zullen regelen. De belangrijkste bronnen van rechten en plichten tussen de partijen zijn, enerzijds, de toepasselijke wetgeving, en anderzijds, de contractuele afspraken die tussen partijen worden gemaakt. Hieronder worden beide besproken vanuit een praktische invalshoek.

#### WELKE RECHTSREGELS ZIJN VAN TOEPASSING OP EEN CLOUD-DIENSTVERLENING?

Er bestaat geen "cloud"-wet of regelgeving die specifiek van toepassing is op cloud. Dit mag niet verwonderen aangezien het cloud-fenomeen relatief recent is. Wellicht is het ook niet nodig om aparte rechtsregels uit te vaardigen over cloud computing, maar volstaan de bestaande rechtsregels.

Hoewel er geen aparte "wet" bestaat die cloud regelt, zijn er wel verschillende regels van toepassing die een algemene gelding hebben, en zich dus ook uitstrekken tot het cloud-aanbod. Enkele worden hieronder kort aangehaald.

Zo zijn de algemene principes van het verbintenissenrecht eveneens van toepassing op cloud computing. Wanneer een cloud-klant en een cloud-dienstverlener overeenkomen dat een cloud-dienst zal worden geleverd aan de klant, komt een verbintenis tot stand. Algemene regels die van toepassing zijn op de totstandkoming van een verbintenis, het tenietgaan van de verbintenis, de wijze waarop verbintenissen kunnen worden bewezen, de overdracht van verbintenissen (bijvoor-

beeld naar een onderaannemer), etc. worden door deze algemene regels geregeld. Echter, dit geldt doorgaans zolang de overeenkomst tussen de partijen niet van deze regels afwijkt, aangezien de meeste van deze regels niet van dwingende aard zijn.

Onder de algemene laag van verbintenissenrechtelijke regels, bestaan er specifieke regels voor bepaalde contractvormen. Zo kunnen, naar gelang van het type dienst dat wordt geleverd door de cloud-dienstverlener, de regels inzake huur, aanneming en eventueel koop van toepassing zijn. Daarbij horen evenwel twee opmerkingen. Vooreerst is het zo dat ook deze regels vaak slechts aanvullend zijn, zodat ze slechts gelden in zoverre de individuele overeenkomst tussen de partijen er niet van afwijkt. Daarnaast is concrete toepassing van de regels van deze benoemde contracten soms onzeker, omdat de meeste van deze regels stammen uit een tijd waarin er van cloud computing – of van computers überhaupt – nog geen sprake was.

Ook consumentenrechtelijke regels kunnen van toepassing zijn indien de cloud-oplossing B2C wordt aangeboden. Opnieuw zullen dan de regels met algemene gelding (dus ook van toepassing

op een cloud-context) van belang kunnen zijn. Een belangrijk voorbeeld is de regel inzake het al dan niet bestaan van een herroepingsrecht dat (en de informatie daarover die) aan een consument moet worden gegeven in geval van een "overeenkomst op afstand", zeg maar een online contract. Nu veel van de B2C cloud-oplossingen online contracten zijn, zijn deze regels dus bijzonder relevant.

Verder bestaan er nog tal van andere regels die een algemene gelding hebben, en dus ook van toepassing zijn op de cloud-dienstverlening. Voorbeelden zijn de wetgeving inzake de verwerking van persoonsgegevens (bijvoorbeeld indien de cloud-klant beslist om persoonsgegevens van zijn eigen klanten in de cloud te zetten, waaraan strike voorwaarden zijn verbonden), de wetgeving inzake toepasselijk recht op overeenkomst, maar ook andere regels zoals belastingrechtelijke bepalingen, enzovoort.

#### DE CONTRACTUELE AFSPRAKEN: VOORNAAMSTE BRON VAN RECHTEN EN PLICHTEN

Zoals gezegd, bestaat er geen cloud-specifieke wet- of regelgeving die dit computing model regelt. Aangezien de toepasselijke algemene regels vaak van aanvullende aard zijn (zie boven), vormt het contract dat tussen beide partijen wordt afgesloten vaak de belangrijkste bron van rechten en verplichtingen die partijen ten aanzien van elkaar kunnen laten gelden. Een goed begrip van het te sluiten contract is dan ook vaak sterk aangewezen.

Eerst en vooral valt het op dat heel vaak standaardcontracten worden afgesloten, die te nemen of te laten zijn voor de cloud-klant. Deze zijn doorgaans in het voordeel van de cloud-dienstverlener opgesteld en de aanvaarding ervan is doorgaans heel laagdrempelig, bijvoorbeeld door het aanvinken van een "Ik ga akkoord"-knop. Het is belangrijk op te merken dat het aanvaarden van een contract op deze manier doorgaans als rechtsgeldig wordt beschouwd, zeker in een B2B-context.

Zonder allesomvattend te willen zijn, noteren we hieronder enkele contractuele aandachtspunten die van belang zijn in een cloud context:

- **Contractstructuur:** een (op het eerste zicht) kort cloud-contract kan verwijzingen bevatten naar verschillende bijkomende contractuele documenten die van toepassing zijn door de enkele verwijzing ernaar in het hoofddocument; het incor-

“Het contract dat tussen beide partijen wordt afgesloten is vaak de belangrijkste bron van rechten en verplichtingen die partijen ten aanzien van elkaar kunnen laten gelden. Een goed begrip ervan is dan ook sterk aangewezen.”

poreren van contractuele documenten is in principe geldig.

■ **Aard van de verbintenis:** er bestaat een onderscheid tussen middelenverbintenissen (waarbij de persoon die de verbintenis dient na te komen slechts redelijke inspanningen dient te leveren om de verbintenis te honoreren) en resultaatverbintenissen (waarbij de persoon die de verbintenis dient na te komen aansprakelijk is van zodra de verbintenis niet is nagekomen, tenzij en enkel tenzij er een wettelijke reden bestaat waardoor deze persoon zich kan bevrijden, zoals in geval van overmacht). Gelet op de gevolgen van deze verbintenissen, naar gelang hun aard, is het belangrijk duidelijk te verstaan onder welke categorie elk van de verplichtingen van de beide partijen zal vallen aangezien dit bepaalt welke actie kan worden ondernomen indien een bepaalde verplichting niet is nagekomen.

■ **Service levels en service credits:** veel contracten in deze context bepalen zogenaamde dienstenniveaus (*service levels*) die vastleggen aan welke kwaliteitsniveaus een dienst dient te voldoen (bijvoorbeeld hoeveel tijd van de maand de cloud toegankelijk zal zijn (“uptime”), hoe snel een telefoon van de helpdesk opgenomen zal worden, hoe snel een oplossing zal worden voorzien in geval van een defect, etc.). Daarbij is het bijvoorbeeld van belang na te gaan hoe dergelijke niveaus worden berekend, en hoe deze worden gemeten en gerapporteerd. Ook dient men na te gaan welk vergoedingsmechanisme van toepassing is in geval de afgesproken dienstenniveaus niet worden behaald, zoals het toekennen van *service credits*, die de vorm kunnen aannemen van een terugbetaling op de aangerekende bedragen of een korting op de volgende factuur. De aard van deze vergoeding (bijvoorbeeld of dit de enige vergoeding is waarop de cloud-afnemer kan rekenen in geval van het niet-behalen van de dienstenniveaus) zal afhangen van de bewoordingen van het contract.

■ **Duur en recht tot opschorting:** deze bepalingen zijn belangrijk, zeker indien een onderneming kritische gegevens of toepassingen in de cloud plaatst. Een afnemer wil immers zeker zijn dat hij niet van de ene op de andere dag zonder dienstverlening valt, en dat de dienstverlening niet als gevolg van al te veel gevallen kan worden opgeschort.

“Een belangrijke vraag, indien men gegevens of toepassingen bij een derde-dienstverlener plaatst, is wat er gebeurt met deze gegevens en applicaties eens het contract een einde neemt.”

■ **Gevolgen van beëindiging en exit:** een belangrijke vraag, indien men gegevens of toepassingen bij een derde-dienstverlener plaatst, is wat er gebeurt met deze gegevens/applicaties, eens het contract een einde neemt. Heeft de derde-dienstverlener dan de verplichting om deze gegevens/toepassingen terug te bezorgen, in welk formaat gebeurt dit, tegen welke vergoeding, etc.? Recent onderzoek naar cloud computing contracten leert alvast dat zelfs bij cloud-diensten aangeboden onder standaardvoorwaarden, doorgaans wordt voorzien in een dergelijke teruggave (onder bepaalde voorwaarden).

■ **Aansprakelijkheid van de partijen en garanties inzake dienstverlening:** deze bepalingen zijn uiteraard belangrijk, en hun belang zal toenemen naarmate de gegevens/toepassingen die in de cloud worden geplaatst, bedrijfskritisch zijn. Hoe meer dit het geval is, hoe meer de onderneming die in de cloud gaat immers belang zal hebben bij garanties van goede werking en hoe groter de potentiële schade zal worden die door een dergelijke cloud-afnemer kan worden geleden.

■ **Beveiliging:** de fysieke (bijvoorbeeld alarmsystemen, gebruik van beveiliging voor toegang tot een datacenter, etc.) en logische (bijvoorbeeld beveiliging tegen virussen, malware, hackers, etc.) beveiliging van de voor cloud gebruikte systemen is belangrijk, en opnieuw zal het belang stijgen naarmate de gegevens/toepassingen die in de cloud worden geplaatst bedrijfskritisch zijn.

Uiteraard hangt het belang van elk van deze onderwerpen sterk af van het concre-

te geval en meer bepaald hoe “kritisch” de cloud-dienstverlening is voor de afnemer (met andere woorden, hoe sterk de operationele, reputationele, etc. afhankelijkheid van de cloud-dienst is).

#### ENKELE BELEIDSINITIATIEVEN

De notie cloud computing wordt niet wettelijk gedefinieerd noch bestaat er specifieke regelgeving die cloud computing regelt. Toch valt dit computing model onder de toepassing van vele regels van gemeen recht die een algemene draagwijdte hebben en dus ook op een cloud-dienstverlening van toepassing kunnen zijn.

Gelet op deze eerder fragmentarische benadering en aangezien het niet altijd duidelijk is tot welke oplossing de toepassing van het gemeen recht zal leiden in geval van een betwisting, is er een grote rol weggelegd voor het contract tussen de cloud-partijen. Een cloud-contract kent, net als andere types van contracten, bepaalde onderwerpen die van bijzonder belang zijn. Een en ander hangt uiteraard steeds af van het type contract, de kost van de dienstverlening, het belang van de gegevens die in de cloud worden geplaatst, etc.

Andere Europese Lidstaten kennen op dit ogenblik evenmin cloud-specifieke wetgeving. Hier en daar hebben sectorgebonden autoriteiten wel richtlijnen uitgevaardigd (bijvoorbeeld in het bankwezen of op het vlak van cloud en de bescherming van persoonsgegevens) en ook de Belgische Privacycommissie wordt verwacht over dit onderwerp een opinie uit te vaardigen.

Het Europese niveau neemt een voorttrekkersrol op zich in het reguleren van cloud. Zo initieerde de Europese Commissie met haar Mededeling over cloud computing enkele regelgevende initiatieven op verschillende domeinen, zoals standaardisatie en certificatie, het gebruik van cloud in de publieke sector en het opstellen van evenwichtige algemene voorwaarden die aan verzuchtingen van zowel aanbieders als afnemers moeten voldoen. Het valt dus te verwachten dat cloud, vanuit een juridisch oogpunt, een verdere ontwikkeling zal kennen in de nabije toekomst en het zal interessant zijn op te volgen op welke wijze voornamelijk de Europese Commissie zal trachten de verschillende belangen met elkaar te verzoenen. ■



# KBC ZET EERSTE STAPPEN IN MIGRATIE NAAR DE CLOUD

## PROACTIEVE RISICOBEPERKING DOOR AFSPRAKEN MET NBB

Overstappen naar de cloud wordt door velen geassocieerd met heel wat mogelijke risico's en vraagtekens. Bedrijven zijn – vaak onterecht – bang om samen met hun data ook de controle erover te transfereren naar derde partijen. En zoals blijkt uit voorgaande juridische beschouwing, is voorzichtigheid gewenst. Maar dat een instelling als KBC alvast enkele stevige stappen heeft gezet op het vlak van cloudcomputing, mag alleszins een positief sein zijn. CTO Frank Demonie vertelt ons over het implementatietraject van Office 365, waarmee KBC in België al zijn tools op het vlak van tekstbewerking, spreadsheets, presentaties, e-mails, sociale collaboratie, bestandenuitwisseling en virtuele communicatie en vergaderingen zal centraliseren en standaardiseren in de publieke cloud. Voor alle duidelijkheid, de meest gevoelige gegevens zoals bijvoorbeeld transactionele (financiële) data of klantgegevens vallen uit de scope, een strikte aflijning mede onderbouwd door afspraken met nationale regelgever NBB.

Tot 2011 werkte KBC met gekende kantoorapplicaties, zoals Lotus Notes voor het e-mailverkeer en nog een hoop andere, verschillende applicaties voor intern telefonisch- en chatverkeer, virtuele vergaderingen, het delen van bestanden en het intranet. CTO Frank Demonie: “De bestaande tools waren gemaakt door ingenieurs voor ingenieurs, waardoor de gebruiksvriendelijkheid niet optimaal was. Bovendien merkten we het drastisch da-

lende marktaandeel van de providers ervan op, wat supportverlening schaarser én duurder maakt. Deze implementatie was ook meteen het moment om de bestaande spaghettistructuur van applicaties op te kuisen en te vervangen door één geïntegreerde set van tools.”

### ROI VAN ÉÉN JAAR

Vanzelfsprekend was het monetaire voordeel de factor die de business case haar

doorslaggevende, valabele basis gaf. De gerealiseerde jaarlijkse kostenbesparing wordt geschat op een bedrag met zes nullen, exclusief efficiëntiewinst aan de business kant. Die laatste wordt onder meer bekomen door een beter versiemangement (men kan met meerderen in één bestand werken) en de toegenomen virtuele vergadermogelijkheden (resulterend in een significante daling van nationale en internationale reiskosten). De ROI wordt al op één jaar behaald. “Het was dan ook niet moeilijk ons directiecomité in 2011 te overtuigen van de financiële voordelen van dit project” concludeert Demonie. Deze eerste stap in de cloud kadert in de nieuwe bedrijfscultuur en (thuis)werk-omgeving, waar KBC graag een voorloper in wil zijn. De nieuwe opzet laat toe om resultaatgericht te werken en tegelijkertijd de werknemer meer onafhankelijk te maken van tijdstip en locatie om zijn of haar werk uit te voeren. “De implementatie van Office 365 was een eerste stap naar ‘het nieuwe werken’. Gezien onze sector is dat echter niet zo eenvoudig. Maar we willen de trend in de industrie op het vlak van cloud computing volgen in België en daarbuiten. Persoonlijk ben ik er van overtuigd dat we meer en meer business processen zullen zien die gaan geleverd worden door cloud services.”

### Timeline

#### Analysis

- Idea
- RFI
- Vendor Select

#### Migration Prep

- Technical Setup
- Pre-Pilot (20)
- Pilot (650)
- Migration

2011

2012/2013

2013

2013/2014

#### Prep Phase

- User Experience (200)
- Risk Assessment / NBB Validation
- Business Case
- Contract T&Cs
- Migration Prep

#### Change Program

- Detailed joined planning
- Training
- Ambassador Program
- User Forum FAQ
- Migration (20.000)
- Operational Readiness



Frank Demonie, CTO van KBC: “Ook de keerzijde van de medaille moet zeer degelijk bekeken worden, mede aan de hand van een grondige risicoanalyse.”

#### INTENSIEVE RISICOANALYSE

Voorafgaand aan de implementatie van deze applicatiegroep, voerde KBC een diepgaand risk assesment uit. Controle, standaardisatie en transparantie waren belangrijke discussiethema's. ICT werknemers waren ook bezorgd over de veiligheid van de data, de continuïteit van de providers en de exitmogelijkheden. “Deze terechte bezorgdheden moet je echter in balans tegenover de voordelen bekijken: Door een betere technische specialisatie van de provider worden onder meer een betere beveiliging, technologie en schaalvoordelen bekomen. De infrastructuur in huis heeft ook risico's” nuanceert de CTO. Samen met de CRO van de groep werden de belangrijkste risico's onder de loep genomen op het vlak van zowel compliance, maar ook vanuit juridisch- en beveili-

gingsoogpunt. Maar daar hield het niet op voor een bedrijf dat zich in een sterk geregeleerde sector bevindt: KBC diende naar de NBB te stappen om een validatie voor zijn specifiek project te bekomen. “Deze proactieve samenwerking was voor ons noodzakelijk, want we vernamen dat in het buitenland cloud-projecten van andere financiële instellingen achteraf op ernstige bezwaren stootten.” Frank Demonie kijkt met een goed gevoel terug op de samenwerking met de NBB: “Men beseft dat de evolutie op dit vlak een marktgegeven is en stelt zich constructief op. Misschien hebben we het pad al wat geëffend voor andere bancaire instellingen, maar daarom zal de NBB zich terecht niet minder risicoalert opstellen.”

#### BELANGRIJKE CLAUSULES

Hoewel zowel de interne als externe risicoanalyses dus een positief advies gaven wat betreft de verderzetting van het project, kwamen ook wat aandachtspunten naar boven waar men als dienstafnemer geen antwoord op kan bieden. Demonie: “Elk outsourcingproject brengt onze zekerheid mee. In dit geval hebben we zelf geen zicht op het intern functioneren van onze service provider. Uiteindelijk stoppen we onze data in een 'zwarte doos'.” De marktrepucie van de aanbieders en externe audits konden deze twijfels deels adresseren, maar het voornaamste hier blijkt voldoende beschermings- en controle clausules te onderhandelen in het contract met de service provider.

Hoewel KBC als klant gezien haar omvang en reputatie in ieder geval wat autoriteit geniet in contractbesprekingen, geeft de CTO de contractuele flexibiliteit van de providers aan als belangrijkste beslissingsfactor in het selectieproces. “We verspreidden een RFI (Request for Information) bij de drie grote partijen. Een

“De NBB beseft dat de evolutie op dit vlak een marktgegeven is en stelt zich constructief op.”

eerste uitsluiting gebeurde op basis van de garantie die kon gegeven worden omtrent de locatie van onze data. Deze willen we namelijk absoluut in Europa hebben. Later deden we een interne test met 200 gebruikers.”

#### STANDAARD

De setup vandaag is vrij standaard. “Waar KBC uitdrukkelijk een afwijking heeft ingevoerd, is bij de authenticatie van gebruikers. De validatie gebeurt normaalgezien in Office zelf, maar bij ons moet men eerst ingelogd zijn in het eigen platform alvorens toegang te krijgen tot de tools en gegevens die in de cloud zijn ondergebracht.” Met het oog op maximale bescherming van de bedrijfsgegevens heeft KBC heel wat policies in werking gesteld. Sommige data bevinden zich daarom in de eigen datacenters van KBC, zonder enige connectie of interface met de cloud.

#### MIGRATIES IN HET WEEKEND

Dit verhaal is alleszins nog niet op z'n einde. Gedurende een aantal weekends werden er telkens groepen van om en bij 3500 gebruikers gemigreerd, en dit met een succesratio van 99,6%. Frank Demonie toont zich tevreden over het verloop: “We hebben een zevental maanden gespendeerd om deze migratie – die zowel op pc's als mobiele toestellen gebeurt - tot in de puntjes voor te bereiden. Een degelijke technische voorbereiding is noodzakelijk als je wil slagen. De uitdaging is om de gebruiker er niets van te laten merken.” KBC werkte met een aantal externe partijen om onder meer de migratie uit te voeren en trainingsmateriaal op te stellen. Maar verder was het vooral een interne realisatie. Het implementatietraject kwam tot stand door een intensieve samenwerking tussen IT, Business en HR. Die laatste was samen met het communicatiedepartement ook sterk betrokken in het change management traject, dat vooral bestond uit het geven van opleidingen en het efficiënt leren gebruiken van de nieuwe tools in een KBC omgeving.

Globaal gezien raadt Demonie de gekozen cloud-opzet zeker aan, maar waarschuwt ook meteen. “Je moet er aan beginnen met een positieve mindset, focus op de voordelen, en niet op wat niet meer kan in de nieuwe omgeving. Maar ook de keerzijde van de medaille moet zeer degelijk bekeken worden, mede aan de hand van een grondige risicoanalyse.” ■