

ICT-DIENSTEN

Juridische aspecten van cloud computing

Steeds meer organisaties en instellingen maken gebruik van 'cloud computing' of overwegen hier gebruik van te maken. Maar wat houdt dit fenomeen in? En welke juridische aspecten kleven hieraan? In dit artikel wordt ingegaan op een aantal belangrijke kenmerken van 'cloud computing'. Daarnaast bespreekt de auteur een aantal juridische do's en dont's bij het contracteren over de voorwaarden.



Mirjam Elferink

Inleiding

Zoals gezegd brengen steeds meer organisaties hun data naar de cloud. De cloud kan allerlei voordelen opleveren op het gebied van kostenbesparingen en eenvoudiger beheer van software en data. De 'cloud' staat symbool voor het internet. Cloud Computing is een volwassen techniek die het mogelijk maakt om via het internet computerkracht of -ruimte en applicaties snel en veilig te gebruiken, zonder dat de gebruikers deze zelf op de computer hebben staan of onderhouden.¹ Het begrip 'cloud computing' is in feite een paraplu-begrip voor allerlei vormen van ICT-dienstverlening via het internet. Denk bijvoorbeeld aan het gebruik van Gmail, Google Apps of andere clouddiensten.

Deze nieuwe techniek brengt mee dat er een nieuwe leveringswijze van ICT-diensten plaatsvindt. Dit brengt op zijn beurt juridische vraagstukken met zich, zoals hoe voorkomt u dat u de grip verliest op uw eigen data? En wie is er eigenlijk verantwoordelijk als er privacy gevoelige en / of bedrijfsinformatie wordt gelekt? Welk recht is van toepassing als de data verspreid over de wereld worden opgeslagen? En wat gebeurt er met deze informatie als de provider bijvoorbeeld failliet gaat? Een andere valkuil die op de loer ligt is dat u afhankelijk wordt van de leverancier. Dit wordt ook wel een zogenaamde vendor lock-in genoemd. Hoe kunt u het ontstaan hiervan voorkomen? Voor dat ik aan de bespreking hiervan toekom, zal ik allereerst ingaan op een aantal kenmerken en vormen van cloud computing.

Kenmerken

Kenmerkend voor cloud computing is dat het beheer van ICT diensten en het beheer van data wordt uitbesteed aan derden. Hierdoor worden data verspreid over verschillende

locaties opgeslagen. Vaak is daarbij niet duidelijk op welke locatie welke data staan. Een ander belangrijk kenmerk is dat de data toegankelijk zijn via het internet. Bij cloud computing wordt vaak onderscheid gemaakt tussen vier soorten cloud-omgevingen: de public cloud, de community cloud, de private cloud en de hybrid cloud.²

In een public cloud worden generieke diensten aangeboden voor algemeen gebruik. In die gevallen heeft de gebruiker vrijwel geen invloed op of controle over de wijze waarop de dienst wordt geleverd (bijvoorbeeld Google, Microsoft of Dropbox).

In een community cloud is sprake van gemeenschappelijke diensten voor een groep (community) organisaties met een gedeeld belang.

Daarnaast kennen we de private cloud. Hierbij is de infrastructuur van de clouddiensten uitsluitend bestemd voor een specifieke organisatie of gebruiker.

Tenslotte bestaat nog de hybrid cloud. Een hybrid cloud is een combinatie van de private cloud voor bijvoorbeeld kritieke data zoals medische gegevens en een public cloud voor minder gevoelige data.

Privacy aspecten

Cloud computing staat soms op gespannen voet met Europese privacyregelgeving. Op de geautomatiseerde verwerking van persoonsgegevens is namelijk de Wet Bescherming Persoonsgegevens (Wbp) van toepassing. Onder het begrip persoonsgegevens wordt verstaan: alle gegevens die te herleiden zijn tot een (natuurlijk) persoon, waaronder naam, adres, woonplaats, e-mailadres, maar ook foto's en in sommige gevallen ook IP-adressen. De Wbp legt een aantal algemene verplichtingen op bij verwerking van persoonsgegevens. Het

gebruik van clouddiensten brengt met zich mee dat persoonsgegevens in de cloud worden opgeslagen. Een eerste belangrijke vraag die daarbij rijst is wie verantwoordelijk is voor de verwerking van persoonsgegevens in de cloud.

Daarvoor is het van belang te kijken naar de begrippen in de wet. De verantwoordelijke is degene die doel en middelen van de verwerking vaststelt. Dit betekent in de regel dat de organisatie die bijvoorbeeld haar kantoorautomatisering naar de cloud brengt verantwoordelijk is voor de persoonsgegevens die in de cloud worden opgeslagen. Dit terwijl die organisatie materieel gezien niet bij de gegevens kan en de facto ook niets te maken heeft met de opslag hiervan. Deze zaken worden nu juist uitbesteed. Toch is de organisatie en/of instelling zelf verantwoordelijk voor de persoonsgegevens. Het komt er dus op aan hier goede afspraken met de leverancier over te maken.

De cloud leverancier die de persoonsgegevens ten behoeve van zijn afnemers opslaat wordt door de Wbp aangemerkt als bewerker. De Wbp schrijft voor dat er een bewerkersovereenkomst wordt gesloten tussen de verantwoordelijke en de bewerker. Hierin worden de in de Wbp genoemde zelfstandige verplichtingen van de bewerker nader geconcretiseerd en contractueel vastgelegd. Denk hierbij onder meer aan de zorg voor een adequate beveiliging van persoonsgegevens.

Degene op wie de persoonsgegevens betrekking hebben worden in de wet aangeduid als betrokkenen. Ook betrokkenen hebben een aantal rechten, zoals het recht op toegang tot de eigen gegevens, het recht deze aan te passen, te wissen, af te schermen of verwerking te weigeren. In de regel zullen betrokkenen dergelijke verzoeken richten tot de verantwoordelijke. Omdat deze de facto niet bij de opgeslagen gegevens kan, heeft hij hiervoor de medewerking van de bewerker nodig. In het kader van de persoonsgegevenbescherming is verder van groot belang te weten hoe de leverancier met de gegevens om zal springen. Zorgt de leverancier ervoor dat deze niet zomaar gedeeld worden met derden? Hoe lang en op welke wijze worden ze bewaard?

Leg uw rechten en plichten goed vast

Omdat bij cloud computing vaak standaard diensten worden geleverd, is het meestal niet eenvoudig om over de voorwaarden van

het contract te onderhandelen. Toch is het raadzaam om goed op te letten waarvoor u eigenlijk tekent. Welke dingen zou u in ieder geval moeten regelen in een cloud computingcontract? Ik noem - naast het hiervoor behandelde onderwerp privacy - nog enkele aspecten.

1. Intellectuele Eigendom

Zorg ervoor dat de intellectuele eigendom van beschermde werken en het databankenrecht op de gegevensverzameling die ontstaat bij u blijft berusten.

2. Service Level Agreement (SLA)

Maak in het contract goede afspraken over het dienstenniveau, bij voorkeur in een Service Level Agreement (SLA). In een SLA kunnen bepalingen worden opgenomen over de beschikbaarheid van de dienstverlening alsmede over de betrouwbaarheid, vertrouwelijkheid en het gebruiksgemak. Denk ook aan een goede back up regeling.

3. Aansprakelijkheid

Regel wie waarvoor aansprakelijk is. Denk daarbij in ieder geval aan de aansprakelijkheid met betrekking tot het verlies van data en/of datalekken, want dit vormt een van de grootste risico's bij cloud diensten. Denk aan de kwestie Diginotar.

4. Meldplicht datalekken

Wees u ervan bewust dat er in de (nabije) toekomst op u als verantwoordelijke een meldplicht komt te rusten voor datalekken. Zowel op nationaal als op Europees niveau zijn hieromtrent een aantal wettelijke ontwikkelingen gaande. Voor aanbieders van telecommunicatiediensten (openbare elektronische communicatiediensten) geldt sinds juni dit jaar al een meldplicht. Anticipeer daarop – waar mogelijk – in uw contracten met de cloudleverancier en/of bewerker, omdat u ook voor dit aspect afhankelijk bent van hun informatie.

5. Continuïteit van de dienstverlening

Regel een aantal zaken waardoor de continuïteit van de dienstverlening gewaarborgd blijft, zoals ondersteuning van de leverancier van migratie van bestaande ICT-oplossingen en het leggen van koppelingen met andere systemen en / of diensten. Voorkom een 'vendor lock-in': zorg ervoor dat de data ook beschikbaar zijn na het einde van de overeenkomst (waaronder faillissement, verhuizing naar een andere leverancier). Vergewis u ervan op welke locatie de data worden opgeslagen.

6. Toepasselijk recht

Kijk welk recht van toepassing wordt verklaard in de contracten. Omdat de cloud per

definitie niet grensgebonden is, is het niet ondenkbaar dat u met buitenlandse partijen contracteert. Het is dan wel van belang om te weten op grond van welk recht eventuele geschillen zullen worden beslecht. Voor wat betreft persoonsgegevens geldt bovendien dat u ervoor moet waken dat de gegevens in landen buiten de Europese Unie worden opgeslagen. Dat mag namelijk niet zonder meer.

Conclusie

In dit artikel heb ik een aantal aspecten die van belang zijn bij cloudcontracten kort aangestipt. Vanzelfsprekend is dit geen uitputtende opsomming. Bedenk dat cloud diensten veelal bestaan uit een keten van verschillende leveranciers en toeleveranciers. Dit maakt dat scherp onderhandelen over de juridische voorwaarden geboden is. Het is immers beter en goedkoper om zaken vooraf contractueel te regelen dan achteraf te moeten repareren!

Mirjam Elferink

Advocaat te Enschede

Mr. dr. M.H. Elferink is werkzaam in Enschede bij het advocatenkantoor KienhuisHoving in de praktijkgroep Technologie, Media en Entertainment (TME). Zij is sinds jaren gespecialiseerd in Intellectuele Eigendom en ICT en publiceert en doceert regelmatig over deze onderwerpen. De praktijkgroep TME van KienhuisHoving is als kennispartner verbonden aan het Centre4Cloud, mede opgericht door de Universiteit Twente. Het Centre4Cloud is een nationaal kenniscentrum op het gebied van cloud computing.

Meer weten? www.fenedexpress.nl, zoek op Cloud computing, ICT-diensten

Voetnoten

1. Zie: <http://www.centre4cloud.nl>
2. Zie voor een overzicht van de verschillende vormen: <http://www.centre4cloud.nl/nl/kennis-ontwikkeling/definition-cloud-computing/deployment-models/>. Verder kan worden onderscheiden in verschillende typen cloud diensten, zoals Software as a Service (SaaS), Infrastructure as a Service (IaaS) en Platform as a Service (PaaS). Het voert in het kader van dit artikel te ver om dit nader uit te leggen. Zie voor meer informatie: <http://www.centre4cloud.nl/nl/kennis-ontwikkeling/definition-cloud-computing/service-models/>