

CONTINUÏTEITSRISICO'S IN DE CLOUD

Donkere wolk

Wat doe je als de *cloud provider* failliet gaat of er anderszins mee stopt? Kun je dan nog wel bij je gegevens? En hoe zorg je dan dat je kunt blijven doorwerken? In afwachting van wetgeving zoeken juristen de oplossing in goede contracten en een calamiteitenfondsje.

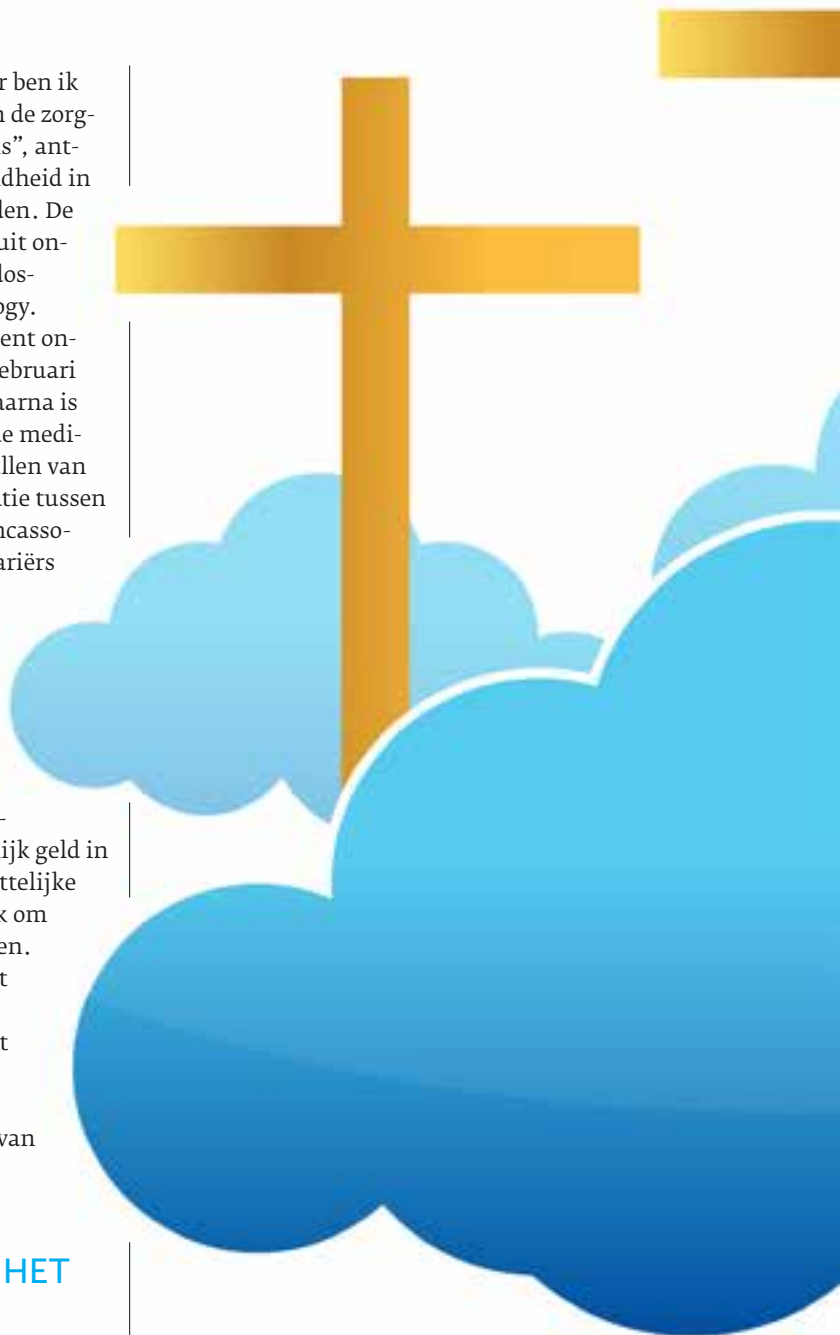
TEKST: LEX VAN ALMELO | BEELD: DREAMSTIME

"Gelet op de uitspraken van de curator ben ik van mening dat de continuïteit van de zorgverlening voldoende gewaarborgd is", antwoordt de minister van Volksgezondheid in maart 2011 op vragen van ongeruste Kamerleden. De ongerustheid betreft het lot van de gegevens uit ongeveer twee miljoen elektronische patiëntendossiers die op de servers staan van Info Technology. Deze *application service provider* uit Hillegom bedient ongeveer tweehonderd huisartsen. Totdat op 8 februari 2011 het faillissement wordt uitgesproken. Daarna is het voor de Kamerleden de vraag wat er met de medische gegevens gaat gebeuren. Over de lotgevallen van het systeem voor de uitwisseling van informatie tussen huisartsen en fysiotherapeuten en voor het incassosysteem SmartCash bekreunen de parlementariërs zich overigens niet.

CURATOR BEPAALT

Het antwoord van de bewindsvrouwe onderstreept hoe zeer de afnemers van cloud-diensten afhankelijk zijn van de curator als de cloud of SaaS (Software as a Service) provider failliet gaat. De belangrijkste verantwoordelijkheid van de curator is zoveel mogelijk geld in de boedel zien te krijgen en dat volgens de wettelijke rangorde te verdelen. Het is dan aantrekkelijk om hardware en/of gegevensbestanden te verkopen. Dat zal een curator met patiëntendossiers niet doen. Maar bij commercieel aantrekkelijke adressenbestanden is het al gebeurd. De klant van een cloud provider kan dus maar het best bij voorbaat voor een noodverband zorgen. Temeer omdat de curator zich in een situatie van

'JE KUNT DE CURATOR MAAR HET BESTE VOOR ZIJN DOOR EEN GOEDE EXIT-REGELING AF TE SPREKEN MET DE CLOUD PROVIDER.'



'BIJ SOMMIGE PROVIDERS ZIJN GEGEVENS ALLEEN TE BEWERKEN IN HET PROGRAMMA VAN DE PROVIDER ZELF.'

PRIVACYBESCHERMING

Volgens de Digitale Agenda van Eurocommissaris Neelie Kroes moet er een Europees raamwerk komen voor billijke contractvoorwaarden bij cloud computing. Erg concreet is dat vrijblijvende raamwerk nog niet. Het *vendor-lock-in*-probleem wordt er voorlopig niet mee opgelost. Vincent Wellens (Nauta Dutilh) verwacht dat de Europese Verordening Gegevensbescherming invloed zal hebben op de *best practices* voor cloud-contracten. De bepalingen van deze verordening zijn direct bindend in alle lidstaten en geven burgers het recht om te weten waar hun gegevens worden verwerkt.

Als de gegevens worden verwerkt buiten de Europese Unie, bijvoorbeeld in India of de Verenigde Staten, moeten cloud providers de privacybescherming goed regelen.

Wouter Dammers (ICTRecht): "Zij mogen alleen persoonsgegevens verwerken als het bedrijf zich houdt aan de *safe harbor principles* en de betrokken personen toestemming hebben gegeven. Amazon.com en Microsoft houden zich aan die privacy-principes, maar hun klanten moeten dus nog wel akkoord gaan met de verwerking van hun gegevens."

faillissement niets hoeft aan te trekken van contracten. In 2006 zei de Hoge Raad (LJN AX8838) bijvoorbeeld dat het economisch eigendom van een pand na het faillissement van de juridisch eigenaar weliswaar doorloopt, maar het gebruiksrecht van dat pand vervalt. De curator hoeft dat contract dus niet na te komen.

EXIT-REGELING

Om te voorkomen dat de leveranciers van de cloud provider hun leveringen staken, neemt een curator over het algemeen snel een aantal forse maatregelen, zonder daarbij altijd de belangen van alle betrokkenen zorgvuldig af te wegen. Hij zal dan niet per se willen investeren in de continuïteit van de dienstverlening. Elke uitgave gaat tenslotte ten koste van de boedel zo niet ten koste van zijn honorarium. "Een curator mag alles doen in het voordeel van de failliete boedel. Je kunt de curator dus maar het beste voor zijn door een goede exit-regeling af te spreken met de cloud provider", zegt Wouter Dammers van juridische advieskantoor ICTRecht.

Klanten van een cloud provider kunnen bijvoorbeeld een *active escrow*-bepaling opnemen in het contract, waarmee wordt gegarandeerd dat de dienst na faillissement nog een aantal maanden door blijft draaien. Verder is het handig om af te spreken dat je als klant de data uit de cloud mag halen als de dienstverlening van de SaaS-provider om wat voor reden dan ook stopt. De klant kan de gegevens dan overbrengen naar een andere provider.

VENDOR-LOCK-IN-PROBLEEM

In de praktijk stuit dat nogal eens op technische problemen. "Bij sommige providers zijn de gegevens alleen te bewerken in het programma van de provider zelf. Dan kun je dus niets meer met jouw gegevens als de leverancier stopt", zegt Elly Stroo Cloeck van de NBA.

'VENDOR-LOCK-IN-PROBLEEM KUN JE CONTRACTUEEL ONDERVANGEN DOOR TE BEPALEN DAT DE LEVERANCIER OPEN STANDAARDEN MOET GEBRUIKEN.'

Dit zogenoemde *vendor-lock-in*-probleem kun je volgens Dammers contractueel ondervangen door te bepalen dat de leverancier open standaarden moet gebruiken. Zoals XBRL voor online-boekhoudprogramma's. De kans dat de curator de contractuele exit-regeling om budgettaire redenen naast zich neerlegt, kan volgens Dammers tot nul worden gereduceerd door bij het sluiten van het contract 'een continuïteitsstichting' op te richten. Deze stichting heeft een bankrekening waar geld op staat om de gegevens van de klanten veilig over te brengen naar een nieuwe *host*. Een micro-rampenfondsje dus.

LUXEMBURG

Hoewel Luxemburg als toevluchtsoord voor fiscale asielzoekers een slechte reputatie heeft, kan het groot-hertogdom als lichtend voorbeeld gelden voor wetgeving op cloud-gebied. In het kielzog van de financiële industrie, die van oudsher sterk geautomatiseerd is, richt het land zich ook op e-commerce. Het dwergstaatsje heeft de ambitie op korte termijn elk adres aan te sluiten op het glasvezelnet. Dankzij de technische infrastructuur hebben bedrijven als Amazon, e-Bay en Skype hun hoofdzetels al naar Luxemburg verplaatst. Het Luxemburgse parlement is nu druk bezig met de aanleg van de juridische infrastructuur.

In oktober 2012 is een wetsvoorstel ingediend dat de klanten van een cloud provider of andere dienstverleners het recht geeft om hun gegevens terug te eisen. Bij betalingsproblemen of faillissement kan de curator de servers en de *server racks* dus niet zo maar verkopen, zegt Vincent Wellens, die verbonden is aan de Luxemburgse vestiging van advocatenkantoor NautaDutilh. Om gegevens terug te kunnen vorderen, schrijft het wetsvoorstel voor dat data van verschillende klanten gescheiden moet kunnen worden. Dat terugvorderen kan lastig zijn als marketingdiensten in de cloud zitten

NBA KENNISGROEP ZOEKT EXPERTS

De NBA zoekt voor de Kennisgroep Cloud vrijwilligers met 'een bovengemiddelde kennis en belangstelling' voor cloud computing. De kennisgroep wil kennis bundelen en verspreiden en een vraagbaak zijn voor NBA-leden. De kennisgroep zal zich naast de continuïteitsproblemen als een cloud provider failliet gaat ook buigen over risico's rond toegang, data integriteit en privacy. Meer informatie: e.stroocloeck@nba.nl.

'LUXEMBURG KAN GELDEN ALS LICHTEND VOORBEELD VOOR WETGEVING OP CLOUD-GEBIED.'

en de provider de klantgegevens van verschillende opdrachtgevers verrijkt heeft met eigen en andere informatie. Dan is er één grote omelet ontstaan, waarvan je geen eieren meer kunt maken.

BOTTE BIJL

Een minpuntje in het Luxemburgs wetsvoorstel vindt Wellens dat de klant moet opdraaien voor de kosten om de gegevens te herstellen. "De wetgever gaat ervan uit dat de partijen het contractueel regelen als zij iets anders willen. Maar dat vind ik niet zo goede opmerking als je bezig bent met een wettelijke regeling." Misschien draait de wetgever nog bij, het is tenslotte nog maar een wetsvoorstel.

In het wetsvoorstel ontbreekt een fonds om de continuïteit te waarborgen. De Luxemburgse financiële toezicht-houder heeft die optie wel gesuggereerd voor financiële instellingen die werken met cloud-toepassingen.

Ondanks deze minpuntjes vindt Wellens cloud-wetgeving nuttig. "Je weet dan dat het geregeld is en dat ook een curator zich er aan moet houden. Want soms gaat die er met de botte bijl door."

Bij cloud computing kunnen de gegevens praktisch overal ter wereld worden verwerkt. De servers van een Nederlandse provider kunnen dus heel goed in het buitenland staan. Als de gegevens in Luxemburg worden verwerkt, kan een Nederlandse klant straks een beroep doen op de Luxemburgse wetgeving. □