Artikel

Contracteren in de cloud – ken uw risico's

K. Daniëls en P. Kits*

1. Inleiding

In de afgelopen jaren zijn particulieren en bedrijven gewend geraakt aan het gemak waarmee ICT- en internetdiensten via draagbare apparaten (*mobile devices*)[1] – mits verbonden met internet – vanaf elke plek, op elk tijdstip afgenomen kunnen worden. De tijd waarin de behoefte van gebruikers beperkt werd door de plek van een (grote) desktop-pc of door de limiet voor opslag van gegevens van een harde schijf ligt ver achter ons. Anders gezegd: gebruik 'any time, any place, by any device'. Dit geldt zowel voor zakelijk gebruik (*business-to-business*) als voor privégebruik (*business-to-consumer*). Maar ook voor *consumer-to-consumer*, immers steeds meer consumenten zijn ook aanbieders op internet, niet alleen van fysieke producten via bijvoorbeeld Marktplaats of Amazon, maar ook van, al dan niet betaalde, diensten via *apps*. Een ontwikkeling met een grote impact is de opkomst van *the internet of things*. Dit betreft de evolutie van het internet waarbij alledaagse voorwerpen zoals auto's en koelkasten zijn verbonden met het wereldwijde web (www) en gegevens kunnen uitwisselen.[2]

De vraag is wie de gewenste toegang tot en koppeling van software, apps, diensten, *computing power* (reken- en verwerkingssnelheid) en opslagcapaciteit zal verschaffen. Het antwoord op deze vraag ligt in *cloud computing*.

Waarom verdient een cloudcontract nadere aandacht? Klassieke licentie-, onderhouds- en hostingovereenkomsten werden vaak uitvoerig uitonderhandeld.[3] Dit gebeurde met het oog op de risico's die inherent zijn aan het gebruik van ICT, zoals systeemuitval, verlies of verminking van gegevens en inbreuk op rechten van derden, zoals het lekken van (bedrijfs)vertrouwelijke of persoonsgegevens. Ondanks dat deze risico's niet zijn verminderd – integendeel, de beweging naar de 'cloud' maakt effectieve controle over software en gegevens bijzonder lastig –, worden cloudoplossingen doorgaans aangeboden met – niet onderhandelbare en in hoge mate gestandaardiseerde – 'toetredingscontracten'. Niet verrassend levert dit in de praktijk financiële, operationele en juridische/compliance-problemen op.

Bij cloud computing is meestal niet duidelijk wie waarvoor verantwoordelijkheid draagt, wie welke bevoegdheden heeft of wie effectieve controle kan uitoefenen op bepaalde verwerkingen van gegevens en/of wat de rechten en plichten zijn van alle betrokken partijen in de ICT en dienstverleningsketen. De risico's en het belang van een goed contract nemen toe naarmate de controle over de ICT-activiteiten complexer wordt zodra meerdere partijen in de keten zijn betrokken.

De leverancier, een zogenoemde Cloud Service Provider (CSP), waarmee wordt gecontracteerd maakt vrijwel altijd gebruik van toeleveranciers hetzij voor de benodigde software,[4] hetzij voor serverruimte, maar ook van

* K. Daniëls is bedrijfsjurist bij Shell met een specialisatie in ICT en globale outsourcingcontracten. Dit artikel is geschreven op persoonlijke titel. P. Kits is advocaat IE, ICT & Privacy bij Holland Van Gijzen Advocaten en Notarissen en lid van de Expert Group on Cloud Computing Contracts bij de Europese Commissie.

1. In deze bijdrage staan veel Engelse termen aangezien die in de praktijk van cloudcontracten veelvuldig worden gebruikt en daarin inmiddels een bepaalde betekenis hebben. Eenduidige Nederlandse vertalingen zijn vrijwel niet mogelijk. Getracht is om anglicismen zo veel mogelijk te vermijden.
2. <www.oxforddictionaries.com/definition/english/Internet-of-things>.
3. Zie kader 'Evolutie ICT-contract naar cloudcontract'.
4. Ook wordt veelvuldig gebruikgemaakt van open source-software. Deze wordt aangeboden onder zogenoemde open source-licenties. Het kenmerkende daarvan is dat de software-eigenaar afstand doet van zijn absolute rechten op grond van het auteursrecht op openbaarmaking en verveelvoudiging. Er wordt ook wel gesproken van *copy left*. Zie ook: <http://opensource.org/licenses>.

tal van andere diensten van derden. Dit gebeurt wereldwijd. Bij het aangaan van een overeenkomst met de CSP zijn de onderliggende afspraken met deze toeleveranciers niet bekend bij de afnemer. Laat staan dat deze 'behoorlijk' zijn doorgecontracteerd (*back to back*). De toegang tot het internet en de netwerken zijn in handen van verschillende telecom- en/of netwerkaanbieders. Deze hebben onderling ook, voor de afnemer noch voor de CSP bekende, afspraken over verwerking van gegevens en *data roaming*.[5] Door toenemende virtualisatie en heet gebruik van mobile devices zoals smartphones, tablets, apps en wifi is de locatie van gegevens, de plaats van dienstverlening[6] en welke partij verantwoordelijk is voor een bepaald onderdeel van de clouddienst vrijwel niet vast te stellen.

Leveringsvoorwaarden voor clouddiensten zijn bovendien aan constante verandering onderhevig. Dit wordt veroorzaakt door de snelle technologische, juridische (met name op gebied van privacy) en marktontwikkelingen, alsmede door het feit dat de leveringsvoorwaarden van CSP's (bij zowel zakelijk als privégebruik) klakkeloos worden geaccepteerd met de daarin veelvuldig voorkomende eenzijdige wijzigingsbedingen.

Dit artikel beschrijft de belangrijkste contractuele risico's van cloud computing vanuit meerdere invalshoeken. We besteden aandacht aan het perspectief van aanbieders en afnemers, het perspectief van marktregulerende partijen (de initiatieven van de Europese en Nederlandse overheid) en het perspectief vanuit de techniek. Afgesloten zal worden met *lessons learned* uit de praktijk.

Deze bijdrage heeft een praktische insteek in aanvulling op eerder verschenen artikelen over de juridische aspecten rondom ICT-contracten en clouddiensten.[7] Om die reden zal een uitvoerige bespreking van het juridisch kader naar Nederlands recht achterwege blijven.

5. <http://nl.wikipedia.org/wiki/Roaming>.
6. Dit is relevant voor welk rechtsregime van toepassing is, maar ook voor fiscale aspecten van de dienstverlening. De context van digitale leveringen aan consumenten (*electronic services*) is van de belang in het kader van 'VAT 2015'. Vanaf 1 januari 2015 zijn de aanbieders van deze diensten niet langer verplicht het toepasselijke btw-percentage af te dragen van het land waar zij gevestigd zijn, maar in het land waar de dienst wordt afgenomen c.q. de consument verblijft: 'From 1st January 2015, this Directive (32008/8/EC) also provides that VAT on telecommunications, radio and television broadcasting and electronic services supplied by a supplier established within the Community to non-taxable persons also established within the Community will be charged in the Member State where the customer belongs.' Dit vereist, met in de EU 28 verschillende btw-regimes, significante maatregelen, zoals op het gebied van prijsstelling, maar ook bewijstechnisch en in de informatievoorziening aan en leveringsvoorwaarden voor consumenten, en via de reflexwerking voor afnemers in het midden- en kleinbedrijf. Zie hierover <http://ec.europa.eu/taxation_customs/taxation/vat/traders/e-commerce/index_en.htm>.
7. Voor een meer inhoudelijke bespreking van ICT-contracten in het algemeen, cloudcontracten en SaaS-contracten wordt verwezen naar respectievelijk: T.J. de Graaf, Pitfalls in ICT-contracten, Contracteren 2013/3, p. 99-107; K. de Vulder & A. Dierik, Contracteren in de cloud, Computerrecht 2011, p. 67; T. Burgers, Software as a Service en het huurrecht, Tijdschrift voor Internetrecht 2011, p. 107-110.

2. Risico's en aandachtspunten

In Europees verband zijn diverse onderzoeken gedaan naar de praktijk van cloudcontracten en Service Level Agreements. Hieruit kan de volgende top 10 van grootste risico's en aandachtspunten afgeleid worden:

1. beperking of uitsluiting van aansprakelijkheid en consequenties (*liabilities, remedies*);
2. service levels, inclusief beschikbaarheid (*availability of service*);
3. databeveiliging en privacy (*data location and data security*; *data disclosure and integrity*);
4. vendor lock in en exit, inclusief termijnen, beëindigingsmogelijkheden en teruggaveverplichting van gegevens bij beëindiging (*switching, data portability*);
5. eenzijdige wijzigingsbedingen van CSP's (*modification of contracts*);
6. intellectuele eigendomsrechten (*use and control of content*);
7. precontractuele informatieplicht (*pre-contractual information and presentation of information in the contract*);
8. onderzoeks-/controlebevoegdheid (*audit, reporting and monitoring*);
9. bedrijfscontinuïteit (*business continuity*);
10. rechts- en forumkeuze, toepasselijk recht, compliance (*data disclosure and integrity*).

Voordat wij hier nader op ingaan, staan wij stil bij de perspectieven van verschillende partijen in de markt.

3. Leveranciersperspectief

Door de wijze van aanbieden van clouddiensten, namelijk altijd digitaal (via websites, portals of apps), waarbij er veelal geen sprake is van voorafgaand contact is met de afnemer, laat staan van contractsonderhandelingen, zal de leverancier zorgen dat de leveringsvoorwaarden de (juridische) kern van de overeenkomst met de afnemer worden.[8] Deze leveringsvoorwaarden zijn, vanzelfsprekend, leveranciersvriendelijk en, in de regel, opgesteld voor het verlenen van diensten met een groot volume, tegen lage kosten, en voor gestandaardiseerde dienstverlening op een gedeelde infrastructuur. Daarbij wordt gebruik gemaakt of is men afhankelijk van diensten zoals telecom- en netwerkleveranciers, hostingproviders en (open source) software van derden en het open internet. De leverancier wil de kosten (en om concurrerend te kunnen blijven zijn prijs) laag houden en de risico's, zowel operationeel als juridisch, zo veel mogelijk buiten de deur houden of uitsluiten. Vanuit het stand-

8. Zie over de totstandkoming van overeenkomsten langs elektronische weg ook de in voetnoot 7 genoemde artikelen. Een verdere problematiek die hierbij in de praktijk speelt, is dat zakelijk en privégebruik van ICT-diensten zich met elkaar vermengen. Als een medewerker van een bedrijf een clouddienst afneemt via zijn smartphone, doet hij dat dan namens het bedrijf of als consument?

punt van de leverancier is het begrijpelijk dat deze liever zijn voorwaarden oplegt, en aanvoert dat gestandaarde dienstverlening voor meerdere klanten vanuit een 'shared environment' dit noodzakelijk maakt. Een dergelijke 'take it or leave it'-benadering waarmee zijn risico's drastisch worden beperkt, beoogt ongetwijfeld ook besparing van kosten en moeite. Gelijktijdig is het een gemiste kans zich te differentiëren van de concurrentie door betere en/of op de afnemer toegesneden voorwaarden te bieden. Leveranciers lijken vooralsnog niet overtuigd van (de waarde van) afwijkende afspraken, diensten en – daarmee samenhangende – onderhandelingen omtrent contractsbepalingen. Zij sluiten aansprakelijkheid voor zaken als intellectuele eigendomsinbreuken en privacy uit en eisen daarvoor, in hun leveringsvoorwaarden, (vergaande) garanties en vrijwaringen van de gebruikers van de clouddienst.

4. Afnemersperspectief

4.1 Type afnemer

Van belang is om op de eerste plaats een onderscheid te maken tussen consumenten en zakelijke afnemers/gebruikers. Consumenten vormen in aantallen de grootste groep afnemers van clouddiensten. Hierbij zijn, in vergelijking met de zakelijke markt, evenwel de contractwaarden laag. De diensten aan consumenten moeten onderverdeeld worden in betaalde en 'gratis' diensten. Dit omdat juist bij de zogenaamde gratis diensten sprake is van eenzijdige en aan constante verandering onderhevige contractsvoorwaarden. De zakelijke afnemers zijn onder te verdelen in grote afnemers, multinationals, het midden- en kleinbedrijf en vrijberoepsbeoefenaars zoals artsen, juridische dienstverleners enzovoort.

Er liggen behoorlijk wat onaangename verrassingen en risico's op de loer voor afnemers die zich laten binden aan de leverancier en daarbij zijn standaardleveringsvoorwaarden accepteren. Het is verontrustend dat alleen voor grote afnemers (multinationals) de grotere CSP's bereid lijken te zijn om afwijkende afspraken te maken. Vaak wordt gesteld dat dit slechts bij hoge uitzondering kan vanwege het kritische karakter van de cloudapplicatie voor de afnemer. Als we naar de grotere cloudleveranciers kijken, kan men stellen dat zij – grosso modo – vooralsnog vast blijven houden aan standaardleveringsvoorwaarden die veelal onnodig eenzijdig van aard zijn. Zoals aangegeven, gaan deze voorbij aan wezenlijke belangen van met name de grotere afnemers. Belangrijk is om de risico's op voorhand te kennen en te weten welke afspraken nodig en welke wenselijk zijn in het aangaan van een contract met een cloudleverancier. Immers, een duurdere cloudleverancier die juridische zekerheid biedt om de continuïteit van de dienstverlening te kunnen afdwingen, is interessanter, zeker wanneer het gaat om kritische bedrijfsapplicaties. Wat we verder zien is dat het veelal ontbreekt aan heldere communicatie vanuit de leverancier over de mogelijkheden en beperkingen van de cloudservice. Als afnemer dient men dan ook onderzoek te verrichten naar de juiste voorstelling van zaken (*caveat emptor*).

4.2 Consument

Voor consumenten lijken vooralsnog de leveringsvoorwaarden van clouddiensten geen belemmering te vormen om een dienst af te nemen. Dat blijkt uit de grote omvang van het gebruik van clouddiensten. Hierbij dient gedacht te worden aan Google (Gmail, Google+), Facebook, Microsoft Live/Outlook, YouTube, Twitter, Dropbox en de inmiddels miljoenen apps. Meestal wordt de link met algemene leveringsvoorwaarden niet eens geopend. 'I have read the terms and conditions' wordt wel beschouwd als de grootste leugen op het internet. Hoewel uit onderzoeken blijkt dat consumenten zich meer en meer zorgen maken over hun identiteit op het www en de bescherming van persoonsgegevens, blijkt van een afname in het gebruik van clouddiensten geen sprake. De vraag is of het wel redelijk is om van consumenten te verwachten dat ze over de kennis en kunde beschikken om te weten welke risico's ze lopen met het gebruik van clouddiensten. Is er überhaupt wel een mogelijkheid om het onderhandelen van de voorwaarden af te (kunnen) dwingen? Het lijkt evident dat ook voor consumenten in de 'cloud' bescherming nodig is en blijft!

4.3 Multinational

Veel multinationals lijken niet altijd even waakzaam en stemmen in de praktijk (te) snel in met de toepasselijkheid van de algemene leveringsvoorwaarden van de leverancier. Begrijpelijk, als gekeken wordt naar het gemak waarmee cloudcontracten – ook door grote afnemers – kunnen worden afgesloten. Echter, de spreekwoordelijke kleine lettertjes in deze standaardvoorwaarden/-contracten kunnen meer dan vervelende gevolgen hebben voor grotere afnemers. Een van de grote voordelen van de cloud is dat alle gegevens samen op de servers van de CSP staan en van overal vandaan toegankelijk zijn. Het lijkt dan ook logisch dat de CSP die de gegevens beheert, waarborgt dat de gegevens bij hem veilig zijn en vertrouwelijk worden behandeld. Dit lijkt evident, maar toch voorzien sommige standaard cloudcontracten in andere bepalingen. Zo zijn er voorwaarden die voorzien dat de cloudleverancier niet verantwoordelijk is om de gegevens van de gebruiker veilig of intact te houden en dat hij niet aansprakelijk is in geval van verlies van de data (de gebruiker dient zijn eigen back-ups te voorzien). Het is verontrustend dat leveranciers de verantwoordelijkheid voor de veiligheid van de gegevens bij de afnemer leggen en vooralsnog weinig bereidheid demonstreren om waarborgen ter zake te bieden. Dit is zeker het geval wanneer het een bedrijfskritische cloudapplicatie voor de afnemer betreft. Het akkoord gaan met internetvoorwaarden is zo gebruikelijk geworden dat vaak wordt vergeten dat juridische waarborgen van belang zijn en dat – net zoals met alle andere contracten – betere afspraken dienen te worden onderhandeld

met de leverancier! Niet iedere afnemer beschikt over dezelfde onderhandelingskracht; in de praktijk blijkt dat heel wat cloudleveranciers openstaan voor onderhandeling over de voorwaarden wanneer het hun wordt gevraagd en het contract voldoende belangrijk is. Multinationals zijn een voorbeeld van een groep die veelal in staat is om betere en meer op zijn belangen toegesneden voorwaarden te bedingen. Het is voor multinationals van belang om beslagen ten ijs te komen en de risico's te kennen en vooraf te weten welke afspraken nodig en welke wenselijk zijn in het aangaan van een contract met een cloudleverancier. Voor zowel leveranciers als afnemers is het cruciaal dat adequate technische, organisatorische en juridische maatregelen worden getroffen.

4.4 Midden- en kleinbedrijf

Uit de diverse onderzoeken blijkt dat in de 'kleine en middelgrote' zakelijke omgeving keuzes voor en onderhandelingen over clouddiensten met name proces- en kostengedreven zijn, en niet juridisch van aard.

Contractsbepalingen lijken hoegenaamd geen invloed te hebben op de keuze voor een bepaalde dienst of dienstverlener. Uit het onderzoek van de Universiteit van Milaan, School of Management (12 juni 2014) onder 184 bedrijven uit het midden- en kleinbedrijf[9] volgt zelfs dat 51% van de respondenten met betrekking tot de contractsbepalingen geen enkel bedrijfskritisch punt kon benoemen. Van hen gaf 44% aan de leveringsvoorwaarden van de leverancier niet eens gelezen te hebben voordat deze werden geaccordeerd. Van de respondenten bleek 3% de leveringsvoorwaarden zorgvuldig te hebben doorgenomen. Voor slechts 1% van hen was dat een reden om de dienst niet af te nemen. Als belangrijkste onredelijke contractsbepalingen werden beschouwd: de beperking van aansprakelijkheid in geval van verlies van data (37%), het recht om de dienstverlening op te schorten (29%) en de afwezigheid van enige verplichting ten aanzien van de termijn waarop door de dienstverlener actie wordt ondernomen in geval van problemen (lees: storingen) (22%).

4.5 Vrijberoepsbeoefenaars: advocatuur

In de praktijk zien we advocaten gebruikmaken van clouddiensten zoals Microsoft 360. De Nederlandse Orde van Advocaten heeft geen eigen richtlijnen voor het gebruik van clouddiensten door advocaten. De Council of Bars and Law Societies of Europe (CCBE) heeft richtlijnen opgesteld voor het gebruik van clouddiensten door advocaten.[10] In onderdeel G wordt aangegeven welke minimale onderwerpen ten minste in het contract tussen advocaat en de CSP opgenomen dienen te zijn.

4.6 Overheid[11]

De Nederlandse overheid heeft een cloudstrategie ontwikkeld. In 2011 werd door de minister van Binnenlandse Zaken en Koninkrijksrelaties in een brief aan de Tweede Kamer nog overwogen dat de nadelen van het gebruik van open cloud computing op dat moment globaal zwaarder wegen dan de voordelen. Deze argumenten hebben te maken met de onvolwassenheid van de markt en de eisen die worden gesteld aan de informatiebeveiliging.[12] De Nederlandse en Europese overheid onderzoeken de mogelijkheid om 'eigen' clouddiensten op te zetten. De Nederlandse overheid werkt samen met een aantal ICT-bedrijven aan een decentraal Dropbox-alternatief, dat bovendien veiliger moet zijn dan bestaande cloudopslagdiensten. Er wordt voor een hybride cloudomgeving gekozen. De code wordt 'open source', zodat iedereen er een eigen server mee kan opzetten. De belangenbehartiger van de Nederlandse hostingsector (DHPA) is bijzonder kritisch over dit initiatief. 'Ik durf te stellen dat het er niet om gaat waar data worden bewaard, maar om wie erop toeziet dat daar geen verkeerde dingen mee gebeuren. Dáár moet de overheid werk van maken, want nu is het toezicht versnipperd tussen CBP en Opta. Kwaliteitsstandaarden hebben we nodig, waarop een heldere kwaliteitscertificering kan worden gebouwd.'

4.7 Financiële sector

In de financiële sector wordt inmiddels veelvuldig gebruikgemaakt van cloudoplossingen. Dit gaat veelal gepaard met nauw overleg tussen de financiële instelling en de CSP. Tevens zijn de toezichthouders, zoals met name De Nederlandsche Bank (DNB), betrokken (zie par. 6). In samenspraak worden contracten op maat gemaakt, waarin de belangrijkste technische, juridische en organisatorische onderdelen van cloud computing uitvoerig worden vastgelegd.

4.8 Non-profitsector, onderwijs en zorg

4.8.1 Non-profit

In de non-profitsector is een sterke tendens waar te nemen van transitie naar de cloud. Dat heeft te maken met de aanbiedingen van enkele grote cloudaanbieders.

4.8.2 Onderwijs

Zo bieden bijvoorbeeld Microsoft[13] en Oracle[14] in het onderwijs zeer aantrekkelijke, zowel in functioneel als in financieel opzicht, cloudoplossingen aan, zoals op het gebied van het onderwijs ondersteunende apps, gegevensopslag en -uitwisseling, administratie en dergelijke. De leveringsvoorwaarden van Microsoft en Google zijn niet onderhandelbaar. Dit levert in de praktijk, bij het

9. <www.osservatori.net/dati-e-ubblicazioni/dettaglio/journal_content/56_INSTANCE_VP56/10402/1547809>.
10. <www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf>.
11. De overheid heeft meerdere rollen: regelgever, marktregulator, afnemer van clouddiensten en toezichthouder (semi-overheid). Hier bespreken we de rol van de overheid als afnemer.
12. <www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/04/20/kamerbrief-over-cloud-computing.html>.
13. <www.microsoft.com/education/ww/leaderships/Pages/SchoolLeaders.aspx>.
14. <www.google.com/edu/programs/>.

ontbreken van een duidelijk juridisch kader, en in data governance (*access management*) problemen op omdat geen garantie voor bescherming van de persoonlijke levenssfeer, betrouwbaarheid en integriteit van de gegevens en continuïteit bestaat. Tevens schuilt hier een significant risico voor een zogenoemde 'vendor lock' in. In dit verband is ook relevant om te verwijzen naar een tweetal onderzoeken. Een onderzoek van het Instituut voor Informatierecht (IVIR), *Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act*, uit september 2012[15] toont aan dat de Amerikaanse overheid kan meekijken in de cloudomgevingen van Amerikaanse CSP's met een beroep op de Patriot Act.[16] In *Met SURF in de wolken, position paper 12 juli 2011* staan voor het onderwijs elementaire onderwerpen en handvatten voor toepassing van cloudoplossingen. SurfSara biedt zelf aan het onderwijs en de wetenschap een cloudoplossing aan.[17] De Surf Cloud HPC-service wordt sinds 2011 aangeboden aan wetenschappers die behoefte hebben aan het opschalen van hun applicatie in een omgeving die zij in eigen beheer hebben.

4.8.3 Zorg

Ook in de zorg zien we het aanbod van cloudoplossingen toenemen. Zorgbestuurders zijn evenwel toch huiverig voor transitie naar de cloud met de gevoelige patiënt- en cliëntgegevens. Het ontbreekt in de zorg aan een duidelijk en concreet juridisch en technisch kader wat dit betreft. Op de website van Nictiz is geen kader voor cloud te vinden,[18] ook de Nederlandse Vereniging van Ziekenhuizen (NVZ) geeft geen richtlijnen voor het gebruik van clouddiensten.[19] Door het afketsen van het landelijk schakelpunt (LSP, in de praktijk ook het Landelijk Elektronisch Patiëntendossier genoemd) zijn op regionaal niveau diverse initiatieven ontstaan op het gebied van uitwisselen, opslaan en gebruiken van zorggegevens. Deze initiatieven worden ondersteund door diverse ICT-dienstverleners met cloudtoepassingen. De juridische vastlegging hiervan gebeurt niet en/of niet op een uniforme wijze. Overigens bestaat de ICT-infrastructuur van het LSP nog wel en wordt hiervan gebruikgemaakt. De standaarden die ten grondslag liggen aan het LSP worden beheerd door de Vereniging Zorgaanbieders voor Zorgcommunicatie.[20] Aan gebruik van het LSP door de zorgaanbieder ligt te allen tijde de toestemming van de patiënt ten grondslag. Het moet daarbij gaan om een uitdrukkelijke toestemming.[21] Deze toestemming kan bijvoorbeeld niet rechtsgeldig worden verkregen middels algemene voorwaarden in de zin van artikel 6:234 van het Burgerlijk Wetboek (BW). Op 7 juli 2014 heeft de Rechtbank Utrecht de uitwisseling van gegevens via het LSP toelaatbaar geacht.[22] De rechtbank heeft de vordering van de Vereniging van Praktijkhoudende Huisartsen om de invoering en verdere ontwikkeling van een systeem voor het elektronisch uitwisselen van medische gegevens te verbieden, afgewezen. De rechtbank oordeelde dat de manier waarop het systeem is ingericht niet in strijd is met de Wet bescherming persoonsgegevens (Wbp).

5. Europese overheid[23]

De Europese Commissie (EC) wil voorwaardenscheppend zijn om cloudgebruik en het aanbieden van clouddiensten aan te jagen: 'unleashing the power of the cloud'. Op grond van ramingen kan de Europese cloudsector in grootte uitgroeien tot 80 miljard euro in 2020 en leiden tot 3,8 miljoen nieuwe banen. Het stimuleren van vertrouwen in de 'online' wereld, het vaststellen van duidelijke rollen en redelijke afspraken zijn voorname doelstellingen van de EC. De EC wil daarbij waarborgen scheppen voor en toezien op het in acht nemen van de grondrechten van burgers, zoals het recht op privacy en consumentenbescherming.

In dat verband heeft de EC een driewegenstrategie ingezet:

1. het doorbreken van de 'jungle' van technische standaarden;
2. het vaststellen van veilige en redelijke contractsbepalingen; en
3. het opzetten van een Europese Cloud Partnership: een samenwerkingsverband van overheid en industrie met als doel het stimuleren van het gebruikmaken van cloud computing, met name ook door de publieke sector.

Tevens zijn vijf werkgroepen ingericht:

- ETSI: Cloud Standards Coordination;[24]
- Cloud Select Industry Group on Service Level Agreements (CIS SLA);
- Cloud Select Industry Group on Certification Schemes;
- Cloud Select Industry Group on Code of Conduct;

15. <www.ivir.nl/publicaties/vanhoboken/Clouddiensten_in_HO_en_USA_Patriot_Act.pdf>.
16. De Amerikaanse Patriot Act vormt onderdeel van de Amerikaanse wetgeving op het gebied van toegang tot gegevens voor justitie, politie en veiligheidsdiensten. Andere belangrijke wetgeving: de FISA (1978), de EPCA (1986) en de FAA (2008). Op 25 april 2014 heeft een Amerikaanse federale rechter bepaald dat Microsoft Amerikaanse opsporingsdiensten toegang moet verschaffen tot persoonsgegevens (lees: e-mailaccount) van een gebruiker in een datacenter in Dublin, Ierland; <www.nysd.uscourts.gov/cases/show.php?db=special&id=398>. Saillant detail was dat in de week voorafgaand aan deze uitspraak de Artikel 29 Werkgroep had aangegeven dat de Microsoft-cloudcontracten voldoen aan de hoge privacy eisen die in de EU worden gesteld: <http://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/>.
17. <www.cloud.sara.nl>.
18. <www.nictiz.nl>, expertisecentrum voor standaardisatie en e-Health levert de zoekterm cloud maar twee resultaten op.
19. <www.nvz-ziekenhuizen.nl/>.
20. <www.vzvz.nl/page/Zorgconsument/Home?>.
21. <www.vzvz.nl/page/Zorgverlener/Gebruik/Toestemming-patient>.
22. ECLI:NL:RBMNE:2014:3097; <www.rechtspraak.nl/Organisatie/Rechtbanken/Midden-Nederland/Nieuws/Pages/Elektronische-uitwisseling-van-medische-gegevens-toegestaan.aspx>.
23. Hier bespreken wij de rol van de (Europese) overheid als stimulator van clouddiensten.
24. <http://csc.etsi.org/website/home.aspx>.

– Expert Group on Cloud Contracts;
– European Cloud Partnership.

De CIS SLA[25] heeft op 24 juni 2014 een set richtlijnen uitgebracht voor de SLA–standaardisatie.[26] Deze richtlijnen zijn een aanvulling op de cloud SLA norm ontwikkeling van het ISO/IEC 19086-project.

De Expert Group on Cloud Contracts[27] heeft in de periode november 2013 tot en met april 2014 de directeur-generaal Justice en de directeur-generaal Connect geïnformeerd over de praktijk rondom cloudcontracten.[28] De input zal worden gebruikt voor een policy paper rondom cloud computing voor de (nieuwe) EC en mogelijk tot zogenoemde modelclausules, zoals de EU Model Clauses for transfer of personal data to Third Countries.[29]

6. Toezicht

6.1 Algemeen

Het toezicht op cloud computing is thans niet formeel of centraal geregeld. Noch in Nederland, noch in Europees verband. In het navolgende zullen wij kort ingaan op de in dit kader meest relevante gereguleerde onderdelen en de standpunten en het beleid van de relevante Nederlandse toezichthouders.

6.2 Privacy: CBP

Privacy en omgang met persoonsgegevens is een heikel onderwerp bij cloud computing. Op grond van de Europese en nationale privacywet- en regelgeving moeten organisaties die persoonsgegevens verwerken ('verantwoordelijken') adequate technische, organisatorische en juridische maatregelen nemen voor een rechtmatige en zorgvuldige verwerking van persoonsgegevens. Ook in geval van uitbesteding van bedrijfsprocessen of ICT blijft de verantwoordelijke hier aan gebonden en hiervoor aansprakelijk. De partij (CSP) die bepaalde gegevensverwerkingen verricht voor of in opdracht van de verantwoordelijke ('bewerker') heeft in die hoedanigheid niet of nauwelijks eigen verplichtingen in dit verband op grond van de wet- en regelgeving.

In 2012 heeft de Artikel 29 Werkgroep[30] een opinie gegeven over cloud computing.[31] In hoofdstuk 4 van zijn opinie geeft de werkgroep expliciet aan welke onderdelen minimaal zouden moeten worden vastgelegd in een cloudcontract. Op diverse punten valt dit samen met de in onderhavige bijdrage besproken belangrijkste aandachtspunten van het cloudcontract. In paragraaf 8 gaan we hier nader op in.

Eveneens in 2012 heeft het College bescherming persoonsgegevens (CBP) in een zienswijze aangegeven of en zo ja onder welke voorwaarden clouddiensten van een Amerikaanse CSP zouden mogen worden afgenomen.[32] De zienswijze gaat uit van een in Nederland gevestigde 'verantwoordelijke' die, voor verwerking van persoonsgegevens waarop de Wbp van toepassing is, gebruikmaakt van de cloud computing-diensten van een leverancier die gevestigd is in de Verenigde Staten. Het CBP gaat niet zover dat het zegt dat het gebruik van clouddiensten via servers in de Verenigde Staten niet is toegestaan. Voor de contractspraktijk is van belang dat het CBP aangeeft dat afspraken over de omgang met en beveiliging van persoonsgegevens expliciet en aanvullend in een bewerkersovereenkomst ex artikel 14 Wbp vastgelegd dienen te worden. Enkel een zogenoemde Safe Harbor-verklaring[33] van de CSP is niet voldoende. Tevens staat opgenomen dat indien de bewerker gebruikmaakt van zogeheten sub-bewerkers (hetgeen in de cloudpraktijk eerder regel dan uitzondering is*)* 'de bewerker dan wel contractueel verzekerd dient te hebben dat de sub-bewerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt'.

6.3 Mededinging, consumentenbescherming en telecom: ACM

De Autoriteit Consument & Markt (ACM), waarin de Opta, de Consumentenautoriteit en de Nederlandse Mededingingsautoriteit zijn opgegaan, heeft geen specifiek cloudbeleid. Zij houdt wel, meer in algemene zin, toezicht op de mededinging op de telecommarkt, netneutraliteit en consumentenbelangen (*e-commerce*).

6.4 Financiële sector: DNB

Financiële instellingen maken, zoals hiervoor aangegeven, in toenemende mate gebruik van cloud computing. In feite gaat het om een vorm van uitbesteding van diensten waarvoor toezichtregels gelden. Banken moeten,

25. Voor een overzicht van de leden van deze werkgroep wordt verwezen naar de annex bij de richtlijnen.
26. <https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>.
27. <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>.
28. The Expert Group was established to assist the Commission in identifying safe and fair contract terms and conditions for cloud computing services for consumers and small firms. The group shall take account of existing best market practices in terms and conditions in cloud computing contracts and the protection of individuals with regard to the processing of personal data and on the free movement of such data (as required under of Directive 95/46/EC).
29. <http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm>.
30. De Artikel 29 Werkgroep is opgericht op grond van artikel 29 van de EU Privacyrichtlijn 95/46/EC. Het is het Europese onafhankelijke adviesorgaan op het gebied van bescherming van persoonsgegevens. De taken van de werkgroep staan beschreven in artikel 30 van Richtlijn 95/46/EC en Richtlijn 2002/58/EC.
31. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>.
32. Zienswijze inzake de toepassing van de Wet bescherming persoonsgegevens bij een overeenkomst met betrekking tot cloud computing-diensten van een Amerikaanse leverancier; <www.cbpweb.nl/downloads_med/med_20120910-zienswijze-toepassing-wbp-SURFmarket-cloud-computing.pdf>.
33. <www.export.gov/safeharbor/>.

naast het 'melden' van (voorgenomen afname van) clouddiensten bij DNB, een risicoanalyse opstellen en het 'right to examine' contractueel regelen. Ook moet worden voldaan aan de eisen die worden genoemd in de Wet op het financieel toezicht. Inmiddels is door DNB met verschillende partijen, waaronder KPN, Microsoft en Salesforce.com, een 'right to examine' (onderzoeksrecht) door DNB overeengekomen. Dit 'right to examine' is standaard in de contracten opgenomen voor de Nederlandse financiële instellingen die clouddiensten bij deze partijen afnemen. Financiële instellingen kunnen daarmee voldoen aan een van de wettelijke vereisten ten aanzien van clouddienstverlening.[34] Uit eigen onderzoek (2011) is gebleken dat binnen Europa Zwitserland expliciete regelingen heeft op het gebied van cloud computing voor de financiële sector, inhoudende een verbod tot het gebruik van een *public cloud*, waarbij financiële gegevens buiten de Zwitserse landsgrenzen opgeslagen zouden kunnen worden.

7. Bespreking belangrijkste risico's en aandachtspunten

7.1 Algemeen

Er dient in de eerste plaats rekening mee te worden gehouden dat de CSP veelal niet de partij is die zelf de effectieve controle heeft over essentiële onderdelen van de dienstverlening. Het gaat dan met name over de toegang tot applicaties, de toegang tot het internet én – niet in de laatste plaats – de beschikbaarheid, integriteit en beveiliging van en toegang tot gegevens.[35] Tevens is een belangrijk punt van aandacht welk recht van toepassing is, zulks in relatie tot de locatie waar de data is opgeslagen, de CSP (of diens toeleverancier) is gevestigd en/of de dienst wordt verleend.

Dit zijn in onze ogen de belangrijkste aspecten die de kern vormen van de juridische vraagstukken rondom cloud computing. Dit zou derhalve ook de kern moeten zijn van de juridische beoordeling van en/of onderhandelingen over de inhoud van cloudcontracten. Zulks naast de afspraken die normaal gesproken in een ICT-overeenkomst (bijvoorbeeld overeenkomst van opdracht of licentieovereenkomst) worden vastgelegd.[36]

7.2 Beperking of uitsluiting van aansprakelijkheid en consequenties ('remedies')

De vergaande beperking en soms – vrijwel – volledige uitsluiting van aansprakelijkheid van CSP's voor storingen (*outages*) en gegevensverlies behoren tot de belangrijkste hordes voor potentiële afnemers van clouddiensten. CSP's doen hierbij een beroep op het feit dat zij 'commodity' services ('one to many') verlenen en zelf ook geen (directe) controle hebben over bepaalde onderdelen van de dienstverlening, zoals de beschikbaarheid (connectiviteit), gegevensverlies als gevolg van communicatie in de cloud en/of via open lijnen en dergelijke. Uit onderzoek blijkt dat in de groepen consumenten en midden- en kleinbedrijven de overgrote meerderheid de algemene leveringsvoorwaarden en daarmee deze vergaande exoneratieclausules van de CSP zonder meer accepteert. Sommige grote afnemers van clouddiensten lukt het om minder vergaande exoneraties overeen te komen; vaak staat daar wel iets tegenover, zoals het uitbreiden van de overmachtsclausule, hogere tarieven en/of het overeenkomen van minimale afname of een langere contractsduur. Dat laatste staat evenwel haaks op een van de karakteristieken van cloud computing, namelijk vergaande flexibiliteit.[37]

7.3 Service levels, inclusief beschikbaarheid

Service Level Agreements (SLA's)[38] zijn, bij gebrek aan een duidelijk definitie en standaardisatie, een voortdurende bron van discussie, zowel bij het aangaan ervan als in de uitvoeringsfase. De SLA's zijn in de praktijk namelijk vaak dermate complex en ingewikkeld opgesteld dat ze, regelmatig ook voor de CSP zelf, niet te controleren en/of te berekenen zijn. Ook is de juridische verhouding tot de hoofdovereenkomst en/of de algemene bepalingen van het contract vaak onduidelijk. Het doel van de SLA om daarmee 'iets' in handen te hebben om de afnemer de mogelijkheid te geven de CSP bij de les te houden, wordt vaak voorbijgestreefd doordat de SLA een verkapte exoneratie is. Vaak zijn de lage service credits de enige 'remedy' voor de afnemer. Die staan vrijwel nooit in verhouding tot de daadwerkelijk geleden schade. En deze beperkte 'pijn' c.q. dit beperkte risico voor de CSP is niet iets wat tot directe actie noodzaakt. Het wordt helemaal ingewikkeld in het geval de SaaS-CSP gebruikmaakt van verschillende hostingpartijen en wanneer niet duidelijk is via welke telecomprovider de verbindingen en aansluitingen worden verzorgd. Temeer nu steeds meer gebruik wordt gemaakt van allerlei *mobile devices* en Wifi. De door de SIG SLA opgestelde richtlijnen, zoals hiervoor genoemd, kunnen

34. <www.dnb.nl/publicatie/publicaties-dnb/nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-augustus-2013/dnb295744.jsp>.
35. Het kan daarbij gaan om bedrijfsvertrouwelijke gegevens en om persoonsgegevens.
36. Zie in dit verband uiteenlopende voorbeelden van ICT-contractsbepalingen in: Nederland ICT Voorwaarden 2014, <www.nederlandict.nl/?id=8307>, de Arbit voorwaarden 2014, <http://wetten.overheid.nl/BWBR0035022/geldigheidsdatum_08-04-2014#Bijlage1>, PON Model sourcing contract, <http://platformoutsourcing.nl/profiles/blogs/modelsourcingcontract-v1> en De Graaf 2013, p. 99-107.
37. Overigens biedt een exoneratieclausule een CSP niet altijd uitkomst. In de zaak KPN/Fysicas oordeelde de Rechtbank Den Haag dat via de reflexwerking de exoneratieclausule in de leveringsvoorwaarden voor een SaaS-dienst vernietigbaar was. In deze zaak was het overzetten van gegevens naar een andere omgeving mislukt, waardoor de gegevens waren verdwenen. Zie: <http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:6526>.
38. Zie ook: P. de Wit & C.E. Drion, De Service Level Agreement, een bijzondere overeenkomst, Contracteren 2005/2, p. 32-38.

een handvat zijn bij het opstellen en beoordelen van (bruikbare) en effectieve SLA's.

7.4 Databeveiliging en privacy

Databeveiliging en privacy zijn voor alle soorten gebruikers van clouddiensten 'key'. De afnemer eist van de CSP vergaande maatregelen en zekerheden, althans dat zou hij moeten doen. De CSP kan deze veelal niet geven. Dit komt doordat de gegevens zich veelal in de public cloud bevinden en daarmee uit het zicht en de controle van de CSP zijn. Veel CSP's weten niet eens om welke data het gaat (met name op PaaS- en IaaS-niveau. Ook is er sprake van steeds wisselende situaties. De data is in beweging (*data in motion*), in gebruik (*data in use*) of in ruste (*data at rest*). Ook hebben anderen dan medewerkers van de CSP toegang tot de gegevens, zoals bijvoorbeeld 'system integrators' en hostingpartijen. Aan de andere kant kan worden gesteld dat data beter beveiligd en privacy beter gewaarborgd zijn in een goed beveiligde en 'anonieme' omgeving dan bijvoorbeeld op een niet of nauwelijks beveiligde server op de locatie van de afnemer. Ten aanzien van de eisen aan het cloudcontract op het gebied van databeveiliging en privacy vormen de opinie 05/2012 van de Artikel 29 Werkgroep en de zienswijze van het CBP goede handvatten. Ook bieden de richtlijnen en publicaties van het ENISA[39] een goed kader, zoals in dit verband het rapport *Security risks and benefits of cloud computing*.[40] Tevens kan worden verwezen naar de in 2013 gepubliceerde richtsnoeren Beveiliging persoonsgegevens van het CBP.[41] In de zomer van 2014 heeft de International Standardization Organization (ISO) een nieuwe norm vastgesteld die ziet op verwerking van de persoonsgegevens in de cloud: ISO 27018. Deze norm is een aanvulling op de bestaande informatiebeveiligingsnormen, zoals ISO 27001 en ISO 27002. In tegenstelling tot de laatstgenoemde normen is de ISO 27018-norm specifiek gericht op clouddiensten en de eerste privacyspecifieke internationale standaard voor de cloud. ISO 27018 regelt met name onderwerpen zoals het vertrouwelijk houden van klantinformatie en het voorkomen dat persoonsgegevens verder worden verwerkt dan het doel waarvoor zij zijn verkregen, zoals data-analyses en adverteren. De norm is een directe reactie op de oproep van de Europese Commissie voor een controleerbaar auditraamwerk voor CSP's, teneinde het vertrouwen in online omgevingen te vergroten en het gebruik en aanbieden van clouddiensten aan te jagen.

Voor de goede orde zetten wij hierbij de handvatten van de Artikel 29 Werkgroep voor cloudcontracten op een rij:

a. Transparantie richting betrokkene: aan betrokkene dient te worden aangegeven dat zijn gegevens in de cloud worden verwerkt.
b. Transparantie richting ICT-leverancier aan cloudgebruiker: De CSP dient kenbaar te maken welke derden (onderaannemers) worden betrokken bij de dienstverlening, waar de datacentra zijn gelokaliseerd (binnen of buiten de EU), welk recht van toepassing is, op welke wijze rechtsgeldige gegevensuitwisseling met zogenoemde 'derde landen' zonder 'passend beschermingsniveau' is geregeld: via de EU Model Clauses, Binding Corporate Rules of anderszins. Ook dient de CSP direct kenbaar te maken wanneer een gezagshandhavende instantie inzage in persoonsgegevens heeft geëist, tenzij dit in het kader van strafrechtelijke geheimhouding niet is toegestaan.
c. Wederkerig geheimhoudingsbeding.
d. Teruggave gegevens: in het cloudcontract dienen de afspraken en voorwaarden te worden gespecificeerd voor het teruggeven van persoonsgegevens bij het einde van de overeenkomst.
e. Beveiligingsmaatregelen: de door de CSP te nemen beveiligingsmatregelen dienen expliciet te zijn gespecificeerd. De maatregelen die worden getroffen dienen in verhouding te staan tot de risico's ten aanzien van de verwerking van de soort persoonsgegevens.
f. Scope en duur: er dient een duidelijke omschrijving te zijn van soort, doel en wijze van verwerking van de persoonsgegevens, alsmede de duur van de clouddienst.
g. Technische en functionele specificaties/SLA: in een SLA dienen de technische en functionele specificaties van de clouddienst te zijn opgenomen. De SLA dient objectieve en meetbare criteria te bevatten met betrekking tot: beschikbaarheid, integriteit, vertrouwelijkheid, transparantie, beperkingen, inmenging van derden, interoperabiliteit, toerekening en controle. Tevens moeten de gevolgen van het niet halen van service levels zijn opgenomen.
h. Medewerkingsplicht: de CSP moet verplicht worden gesteld om op eerste verzoek medewerking te verlenen in geval van een beroep op inzage, correctie of verwijdering van persoonsgegevens door een betrokkene.
i. Verbod tot doorgifte aan derden: in het cloudcontract dient een expliciet verbod tot doorgifte van persoonsgegevens te staan, tenzij is overeengekomen dat onderaanneming is toegestaan.
j. Informatieplicht bij inbreuk: de verplichtingen van de CSP in geval van een datalek (lees: inbreuk op verlies, beschadiging of diefstal van persoonsgegevens).[42]

39. European Network and Information Security Agency.
40. <www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment>.
41. <www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf>.
42. <www.rijksoverheid.nl/documenten-en-publicaties/wetsvoorstellen/2012/11/01/wijziging-wet-bescherming-persoonsgegevens-meldplicht-datalekken>. Het wetsvoorstel bevat een regeling voor de meldplicht bij geconstateerde inbreuken op beveiligingsmaatregelen voor persoonsgegevens, uitbreiding van de bevoegdheid tot het opleggen van een bestuurlijke boete door het College bescherming persoonsgegevens en enige onderwerpen die voortvloeien uit de evaluatie van de Wet bescherming persoonsgegevens en het rapport van de Adviescommissie veiligheid en de persoonlijke levenssfeer. Deze maatregelen hebben tot doel de naleving van de wet te verbeteren.

k. Onderzoeks-/controlerecht: de afnemer dient het recht te hebben om zich inzicht te verschaffen in de activiteiten en beveiligingsmaatregelen van de CSP en om zijn onderaannemers te controleren; zij moeten verplicht zijn hier aan mee te werken.[43]
l. Voldoen aan wet- en regelgeving: in het cloudcontract dient voor de CSP een algemene verplichting te worden opgenomen om te voldoen aan de nationale wet- en regelgeving op het gebied van verwerking van persoonsgegevens.
m. Informatieplicht bij wijziging in dienstverlening: de CSP moet verplicht worden gesteld om de gebruiker te informeren over relevante wijzigingen in de clouddienst, waaronder implementatie van additionele functies en aanvullende bevoegdheden.[44]
n. Continuïteit: expliciet dient te worden vastgelegd welke maatregelen zijn genomen in verband met continuïteit, zoals het voorkomen van storingen en onderbrekingen en het verlies of verminking van gegevens.
o. Interoperabiliteit: de afnemer moet nagaan of de CSP een interoperabel bestandsformaat hanteert. Dit teneinde 'vendor lock ins' tegen te gaan.
p. Vendor lock in en exit, inclusief termijn, beëindigingsmogelijkheden en teruggaveverplichting van data bij beëindiging en escrow.

Afspraken over beëindiging en medewerking aan het overdragen van gegevens bij beëindiging van de relatie met een CSP staan vaak niet of uiterst summier in de leveringsvoorwaarden. Voordat een clouddienst wordt afgenomen, dient de afnemer zich ervan te vergewissen dat de benodigde gegevens beschikbaar blijven en op verzoek worden overgedragen of overdraagbaar zijn naar zichzelf of derden bij het einde van de relatie met de CSP. Daarbij is er in Nederland de laatste tijd, na het Nebula–arrest,[45] aandacht voor de noodzaak van een escrow-overeenkomst bij clouddienstverlening.[46] Daarbij gaat het om het gebruik en de gebruiksrechten van/op de applicatie die wordt gebruikt. Vooralsnog lijkt de beste oplossing de overdracht van de IE-rechten aan een separate entiteit. Voor consumenten en het midden- en kleinbedrijf is dit een brug te ver. Dit biedt kansen voor de CSP's zelf om een dergelijke voorziening aan te bieden of voor ondernemers die in dit gat in de markt springen.

7.5 Eenzijdige wijzigingsbedingen van CSP's;

In vrijwel alle onderzochte cloudcontracten c.q. gestandaardiseerde cloudleveringsvoorwaarden staan zogenoemde eenzijdige wijzigingsbedingen. Zulks al dan niet met de mogelijkheid voor de afnemer om de dienst, in geval van wijziging, met inachtneming van een opzegtermijn te beëindigen. De leveranciers geven aan dat dit noodzakelijk is gelet op de snelle ontwikkelingen in de techniek, op de markt en juridisch.

Enkele voorbeelden:

> '[CSP] may modify the general conditions and terms of service at any time. Customer may terminate the contract within 30 days. By continuing to use the service customer will be bound by the modified terms.'

> 'The service specifications are subject to change at [CSP]'s discretion.'

> '[CSP] may modify the general conditions and terms upon written notice of 60 days.'

Er zijn inmiddels diverse voorbeelden van doorgevoerde wijzigingen in leveringsvoorwaarden, waarbij de gebruiker, ineens, meer rechten moest prijsgeven dan de bedoeling was, zonder dat de gebruiker daar feitelijk en juridisch iets tegen kan inbrengen.

Naast contractsbepalingen die de kern van de dienst weergeven (kernbedingen) en algemene voorwaarden (art. 6:231 BW) wordt door CSP's ook veelvuldig gebruikgemaakt van zogenoemde AUP's (Acceptable Usage Policies). De juridische status van dergelijke policies is niet duidelijk, maar in de praktijk kan een CSP, indien naar zijn discretie hij van mening is dat in strijd met 'acceptabel gebruik' de dienst wordt gebruikt, de dienst geheel of gedeeltelijk, definitief of tijdelijk opschorten. Deze AUP's zijn ook veelvuldig aan eenzijdige wijzigingen onderhevig.

7.6 Intellectuele eigendomsrechten (use and control of content);

In de digitale wereld bestaat veel onduidelijkheid over de eigendom van intellectuele eigendomsrechten en -gegevens (data). Daarbij gaat het met name om auteursrechten op afbeeldingen, foto's, video's, geluidsfragmenten, software, api's, teksten en databanken. Met de snelheid van het licht worden deze gedeeld, bewerkt, openbaar gemaakt, toegeëigend enzovoort. Wat mag een leverancier met de intellectuele eigendommen van zijn klanten? In diverse cloudcontracten komen we tegen dat de klant aan de leverancier een onbeperkt, niet exclusief gebruiksrecht verschaft op openbaarmaking, verveelvoudiging en hergebruik, al dan niet in gewijzigde vorm, ervan.

43. Omdat dit in de praktijk niet of nauwelijks uitvoerbaar is, wordt gebruikgemaakt van zogenoemde TPM's (Third Party Mededelingen), zoals bijvoorbeeld gebaseerd op de ISAE 3402 (voorheen SAS70). Een lacune is thans nog dat dit met name ziet op het aanwezig zijn van een informatiemanagementsysteem en niet op de inhoud daarvan of op de kwaliteit van de getroffen beveiligingsmaatregelen en ook niet op de rechtmatigheid van verwerking van persoonsgegevens.
44. Denk hierbij aan het zichzelf toestaan van het koppelen van verschillende gegevensbestanden en data-analyses (Big Data-toepassingen).
45. HR 3 november 2006, NJ 2007/155 (Nebula). Hierin bepaalde de Hoge Raad, kort gezegd, dat het voortbestaan van een wederkerige overeenkomst als zodanig niet beïnvloed wordt door het faillissement van een van de partijen, maar dat zulks niet automatisch inhoud dat de schuldeiser zijn rechten kan uitoefenen alsof er van een faillissement geen sprake zou zijn. Volgens de Hoge Raad geldt dit ook voor de gevallen waarin de gefailleerde niet (langer) verplicht is een prestatie te verlenen, maar het gebruik van een aan hem in eigendom toebehorende zaak moet dulden. In de praktijk is vervolgens discussie ontstaan of een curator zich met succes kan verzetten tegen toegang en gebruik van software en broncodes die toebehoren aan de failliet.
46. Zie hierover: E.J. Louwers & P.M. de Laat, Continuïteit in de cloud, Computerrrecht 2014/4, p. 216-221.

Enkele voorbeelden:

> '[CSP] does not claim ownership of the materials you provide to [CSP] (including feedback and suggestions) or post, upload, input or submit to any Website Services or its associated services for review by the general public, or by the members of any public or private community, (collectively "Submissions"). However, by posting, uploading, inputting, providing or submitting your Submission you are granting [CSP], its affiliated companies and necessary sub licensees permission to use your Submission in connection with the operation of their Internet businesses (including, without limitation, all [CSP] Services), including, without limitation, the license rights to: copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate and reformat your Submission; to publish your name in connection with your Submission; and the right to sublicense such rights to any supplier of the [CSP service] Website.'

> 'Some of our Services allow you to submit your content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.
> When you upload or otherwise submit content to our Services you give [CSP] (and those we work with) a worldwide license to use, host, store, reproduce, modify, create, communicate, publish, publicly perform, publicly display and distribute such content. (…) The license continues even if you stop using our Service. (…) Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.'

> 'When you use our Services, you provide us with things like your files, content, email messages, contacts and so on ("Your Stuff"). Your Stuff is yours. These Terms don't give us any rights to Your Stuff except for the limited rights that enable us to offer the Services.
> We need your permission to do things like hosting Your Stuff, backing it up, and sharing it when you ask us to. Our Services also provide you with features like photo thumbnails, document previews, email organization, easy sorting, editing, sharing and searching. These and other features may require our systems to access, store and scan Your Stuff. You give us permission to do those things, and this permission extends to trusted third parties we work with.'

Het behoeft geen betoog dat dergelijke bepalingen een kritische benadering vereisen bij het beoordelen van cloudcontracten.

7.7 Precontractuele informatieplicht

Op 25 oktober 2011 is Richtlijn 2011/83 betreffende consumentenrechten tot stand gekomen. De richtlijn voegt twee eerdere richtlijnen, te weten Richtlijn 97/7/EG betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten en Richtlijn 85/577/EEG betreffende de bescherming van de consument bij buiten verkoopruimten gesloten overeenkomsten, samen tot één nieuwe richtlijn. De richtlijn beoogt de bestaande Europese regels over overeenkomsten die zijn gesloten tussen consumenten en handelaren te actualiseren, te vereenvoudigen en te verbeteren en door de realisatie van een hoog niveau van consumentenbescherming bij te dragen aan een goede werking van de interne markt. Het toepassingsgebied van de richtlijn ziet op alle overeenkomsten die tussen handelaren en consumenten zijn gesloten:

a. op afstand;
b. buiten verkoopruimten; en
c. overeenkomsten anders dan op afstand en buiten verkoopruimten gesloten.

De informatieplicht van de verkoper/CSP is een belangrijk onderdeel van de nieuwe wetgeving. De CSP is verplicht om bepaalde informatie aan de consument te verschaffen voordat de overeenkomst tot stand komt. Enkele voorbeelden zijn: de naam van de verkoper, de prijs van het product of dienst, de kosten voor verzenden van het product en de manier waarop betaald kan worden. Deze informatie moet door middel van een 'duurzame gegevensdrager' aan de consument worden verstrekt. E-mail valt onder de nieuwe regelgeving overigens ook onder de definitie duurzame gegevensdrager. De Europese Commissie werkt aan een set van standaardiconen die door CSP's gebruikt kunnen worden (niet verplicht) om aan hun informatieverplichtingen te voldoen.

7.8 Onderzoeks-/controlebevoegdheid (audit);

Om meerdere redenen dienen in een cloudcontract afspraken over onderzoeks- en controlemogelijkheden te worden vastgelegd. Een dergelijke bepaling geeft de afnemer, op de eerste plaats, de mogelijkheid om de CSP te kunnen afrekenen op nakoming van zijn verplichtingen en fungeert als 'sturingsmiddel' in de relatie met hem. Een controle-/auditbevoegdheid kan derhalve bewijs opleveren voor een stelling van de afnemer. Afnemers hebben daarnaast ook diverse verplichtingen op grond van fiscale, administratief-financiële en privacywet- en regelgeving. Op grond van artikel 47 van de Algemene wet inzake rijksbelastingen (AWR) bijvoorbeeld, dient eenieder op verzoek van de belastinginspecteur gegevens, boeken en bescheiden te overleggen waarvan de raadpleging van belang kan zijn voor de

vaststelling van de belastingheffing.[47] Deze verplichting geldt tot en met zeven jaar na creatie van het desbetreffende gegeven/document. De administratief-financiële verplichtingen rondom opslag en bewaring komen voort uit het Burgerlijk Wetboek (Boek 2 en Boek 3) en uit accountancystandaarden zoals IFRS. In het vorenstaande zijn wij reeds uitgebreid ingegaan op de verplichtingen op grond van de privacywet- en regelgeving. Teneinde te kunnen aantonen dat de afnemer aan de hier bedoelde eisen voldoet, dient hij concrete afspraken te maken met de CSP of zich er, voor het afnemen van de dienst, van te vergewissen dat dit door middel van controle kan aantonen. Zonder vastlegging in de overeenkomst kan de afnemer dit niet afdwingen en kan hij ook niet aantonen dat hij aan de op hem rustende dwingendrechtelijke verplichtingen voldoet.

Omdat dergelijke controles in cloudomgevingen praktisch welhaast onmogelijk en/of kostbaar zijn, wordt in de praktijk – door CSP's – gebruikgemaakt van zogenoemde Third Party Mededelingen (vergelijk voetnoot 43). Er zijn inmiddels diverse certificeringsschema's op het gebied van databeveiliging voorhanden, zowel technisch als organisatorisch georiënteerde. Voorbeelden zijn: SOC/ISAE 3402 / SSAE16, Cloud Industry Forum Code of Practice, ISO 27001, Cloud Security Alliance – Open Certification Scheme. Echter, deze worden beschouwd als 'standaarden', maar slechts een enkeling voldoet aan de behoeften die bestaan in en eisen die worden gesteld aan een (veilige en betrouwbare) cloudomgeving. Ten aanzien van bescherming van persoonsgegevens zijn er nog geen certificeringsschema's die als standaard worden beschouwd. Via ETSI (vergelijk voetnoot 24) streeft de Europese Commissie ernaar om tot duidelijke en bruikbare standaarden te komen, op basis waarvan gecontroleerd en waartegen gecertificeerd kan worden.

7.9 Bedrijfscontinuïteit

De vraag is hoe bedrijfscontinuïteit in de cloud is te realiseren. Daarbij gaat het om beschikbaarheid en integriteit van de bedrijfsgegevens. In de praktijk zorgen CSP's voor meerdere back-ups, ook al is dit contractueel niet overeengekomen. Dit om aansprakelijkheid te voorkomen (zie ook voetnoot 37). Sommige CSP's wijzen uitdrukkelijk op de medeverantwoordelijkheid van de clouddienstafnemer: indien de gegevens of de 24/7-beschikbaarheid van een softwareapplicatie of de data dermate belangrijk zijn, is de aangeboden clouddienst dan wel de meest aangewezen oplossing voor die afnemer? CSP's geven ook geregeld aan dat zij een dienstverlener en geen verzekeringsmaatschappij zijn en dat het de afnemer vrijstaat om eigen back-ups te maken.

7.10 Rechts- en forumkeuze, toepasselijk recht, compliance

Niet altijd wordt voldoende aandacht besteed aan de keuzes voor toepasselijk recht en adequate geschillenbeslechting, en ook niet aan welk recht op bepaalde verwerkingen of in relevante jurisdicties van toepassing is. Bijvoorbeeld Duitse financiële gegevens mogen niet buiten de Europese Economische Ruimte worden gebracht. In die gevallen moet het contract onder het recht van een lidstaat van de Europese Economische Ruimte worden gebracht, omdat dit anders niet afdwingbaar is. Dit is het domein van internationaal privaatrecht in het geval de partijen hier niets over hebben bepaald. Dat is, gelet op de complexiteit van cloud computing, een ongewenste situatie. Ten aanzien van adequate geschillenbeslechting is van groot belang dat beslissingen van het scheidsgerecht ook bindend zijn voor bijvoorbeeld sub-bewerkers/onderaannemers.

Ten aanzien van compliance zijn in het voorgaande reeds enkele aandachtspunten aan de orde gekomen, zoals op het gebied van privacy, fiscaliteiten en administratieve en financiële bewaarverplichtingen. Uiteraard zijn er in diverse sectoren nog specifieke bewaarverplichtingen van toepassing. Hier melden wij nog de verplichting die rust op zowel de afnemer als de CSP om mee te werken aan opsporingsonderzoeken van justitiële en andere opsporingsautoriteiten. In cloudcontracten dient een bepaling te zijn opgenomen dat CSP's verplicht zijn om verzoeken van opsporingsautoriteiten aan de afnemer te melden. In februari 2013 is het rapport *Misdaad en opsporing in de wolken* van het Wetenschappelijk Onderzoek- en Documentatiecentrum gepubliceerd[48]. De belangrijkste constatering van de auteurs is dat de meest gebruikte methoden om digitale gegevens te verzamelen (doorzoeking, vorderen van gegevens en onderscheppen van gegevens) beperkingen hebben bij gegevens die in de cloud liggen opgeslagen of wanneer via de cloud wordt gecommuniceerd. De voornaamste beperking daarbij vormen de territoriale grenzen waaraan de Nederlandse opsporing is gebonden. Slechts met rechtshulpverzoeken kunnen buitenlandse cloudaanbieders worden verzocht de gegevens aan te leveren.

8. Lessons learned

Ervaring 1: Laat je niet misleiden. Niet alles is 'standaard' aan clouddiensten. Het omgekeerde is veelal het geval. Probeer de risico's op voorhand te kennen en te onderkennen en deze af te wegen tegen de voordelen die de specifieke clouddienst kan bieden. Het kan goed zijn

47. Art. 47 AWR: 'Ieder is gehouden desgevraagd aan de inspecteur: a. de gegevens en inlichtingen te verstrekken welke voor de belastingheffing te zijnen aanzien van belang kunnen zijn; b. de boeken, bescheiden en andere gegevensdragers of de inhoud daarvan – zulks ter keuze van de inspecteur – waarvan de raadpleging van belang kan zijn voor de vaststelling van de feiten welke invloed kunnen uitoefenen op de belastingheffing te zijnen aanzien, voor dit doel beschikbaar te stellen. Ingeval de belastingwet aangelegenheden van een derde aanmerkt als aangelegenheden van degene die vermoedelijk belastingplichtig is, gelden, voor zover het deze aangelegenheden betreft, gelijke verplichtingen voor de derde.'

48. B.J. Koops e.a., Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing, Den Haag: WODC 2013.

dat voor niet-kritische diensten vanuit juridisch oogpunt in principe veilig kan worden overgeschakeld op de cloud en de algemene leveringsvoorwaarden te accepteren. Als blijkt dat afwijkende afspraken noodzakelijk zijn, dient de afnemer volhardend te zijn naar de CSP en een 'maatwerk'-contract uit te onderhandelen.

Ervaring 2: Waar mogelijk is het maken van sectorspecifieke afspraken, zoals bijvoorbeeld in de financiële sector in samenwerking tussen DNB, financiële instellingen en enkele CSP's succesvol is gedaan, efficiënt als krachtenbundeling naar de aanbieders van clouddiensten. In andere, ook minder gereguleerde sectoren zouden de handen ineengeslagen kunnen worden.

Ervaring 3: Benader een cloudproject niet enkel vanuit technisch en informatiebeveiligingsoogpunt. Bij de afweging van de voordelen van cloudoplossingen voor een afnemer (dynamisch gebruik, gebruiksgemak) tegen de verhoogde risico's (zoals de gebrekkige controle over gegevens en dienstverlening door leverancier en voor hem werkzame derden) dienen andere aspecten, zoals commerciële (zoals de methodiek waarmee de prijs wordt berekend en aangepast), juridische en/of compliance-aspecten, meegenomen te worden. Hanteer een multidisciplinaire aanpak naar het project toe, zowel binnen de klantorganisatie als samen met de CSP en steeds vanuit een geïntegreerd juridisch, technisch en organisatorisch perspectief. De hele keten dient op de een of andere manier inzichtelijk en gebonden (lees: aangesproken) te kunnen worden gemaakt. Eventueel kunnen de rollen en verantwoordelijkheden van de diverse betrokkenen vastgelegd worden in een RACI–matrix.[49]

Ervaring 4: Hanteer een datacentrische benadering voor effectieve risicobeoordeling. Draag zorg voor zorgvuldige en consistente dataclassificatie om te (kunnen) bepalen welke gegevens en applicaties bedrijfskritisch zijn en derhalve voor keuzes omtrent welke aanbieder het meest geschikt is. Belangrijk is om de risico's die verband houden met het overbrengen van de data en de controle daarover naar systemen van de CSP op voorhand nauwkeurig in kaart te brengen en te kennen. Dit betekent dan ook dat er op voorhand al rekening gehouden dient te worden met het *legal & regulatory* perspectief en de risico's die verband houden met de opslag, overdracht en bewerking van gegevens van de afnemer. Daarbij dienen voordelen (zoals gebruiksgemak, efficiëntie, kosten ('pay per use')) te worden afgewogen tegen de risico's (zoals de gebrekkige controle over gegevens en dienstverlening). Ter waarschuwing: het gemak waarmee een relatie met een CSP min of meer automatisch tot stand komt, mag geen excuus zijn om belangrijke juridische aspecten te negeren.

Ervaring 5: Voorkom vendor lock in! Een goed cloudcontract begint met overeenstemming over de exitbepalingen. Beding nadrukkelijk en expliciet wat er gebeurt in geval van een exit. De afnemer dient (in beginsel) de rechthebbende te zijn en blijven over alle gegevens (inclusief afgeleide gegevens zoals bijvoorbeeld metadata) die de leverancier onder zijn hoede heeft. Voorkom dat er intellectuele en/of industriële eigendomsrechten zijn die de afnemer (kunnen) verhinderen in geval van een (voortijdige) beëindiging gegevens terug te krijgen.

Ervaring 6: Maak een rechts- en forumkeuze bepaling op maat. Gelet op de complexiteit van cloud computing volstaat een zogenoemde 'boiler plate'-clausule niet. Er zijn immers vaak meerdere rechtsstelsels die toepasselijk kunnen zijn op de systemen en/of gegevens (in 'rest' en in 'motion'). Dit betekent in de 'klein en middelgrote' zakelijke praktijk dat de opsteller of beoordelaar van een cloudcontract zich geen agnostische houding kan permitteren! Immers, zonder te begrijpen (vanuit het projectteam) wat de clouddienst en de CSP beogen te doen met de gegevens, is een risico-inventarisatie weinig zinvol. Het is noodzakelijk om onder de motorkap te kijken… cloudoplossing en cloudcontract zijn verweven vanuit een risicoperspectief!

Wat is cloud?

De meest geaccepteerde en meest gangbare definitie van cloud computing is de zogenoemde NIST-definitie.[50] Hierin wordt cloud computing beschreven als: een model voor eenvoudig en *on demand* netwerk toegang tot een gedeelde omgeving van ICT-bronnen, zoals netwerken, servers, opslag, applicaties en diensten. Clouddiensten en -oplossingen kunnen snel ingezet en geleverd worden met minimale inspanning van het management van de afnemer of de dienstverlener. Het model is opgebouwd uit vijf essentiële karakteristieken, drie dienstverleningsmodellen en vier soorten toepassingen.

De essentiële kenmerken zijn: *on demand* zelfservice, brede (lees: vrijwel onbeperkte) netwerktoegang, *resource pooling*, flexibiliteit en meetbare dienstverlening. De dienstverleningsmodellen zijn: Software as a Service, Platform as a Service en Infrastructure as a Service. De toepassingsgebieden zijn: private cloud, community cloud, public cloud en hybrid cloud (zie figuur 1).

In figuur 2 wordt de NIST-definitie schematisch weergegeven.

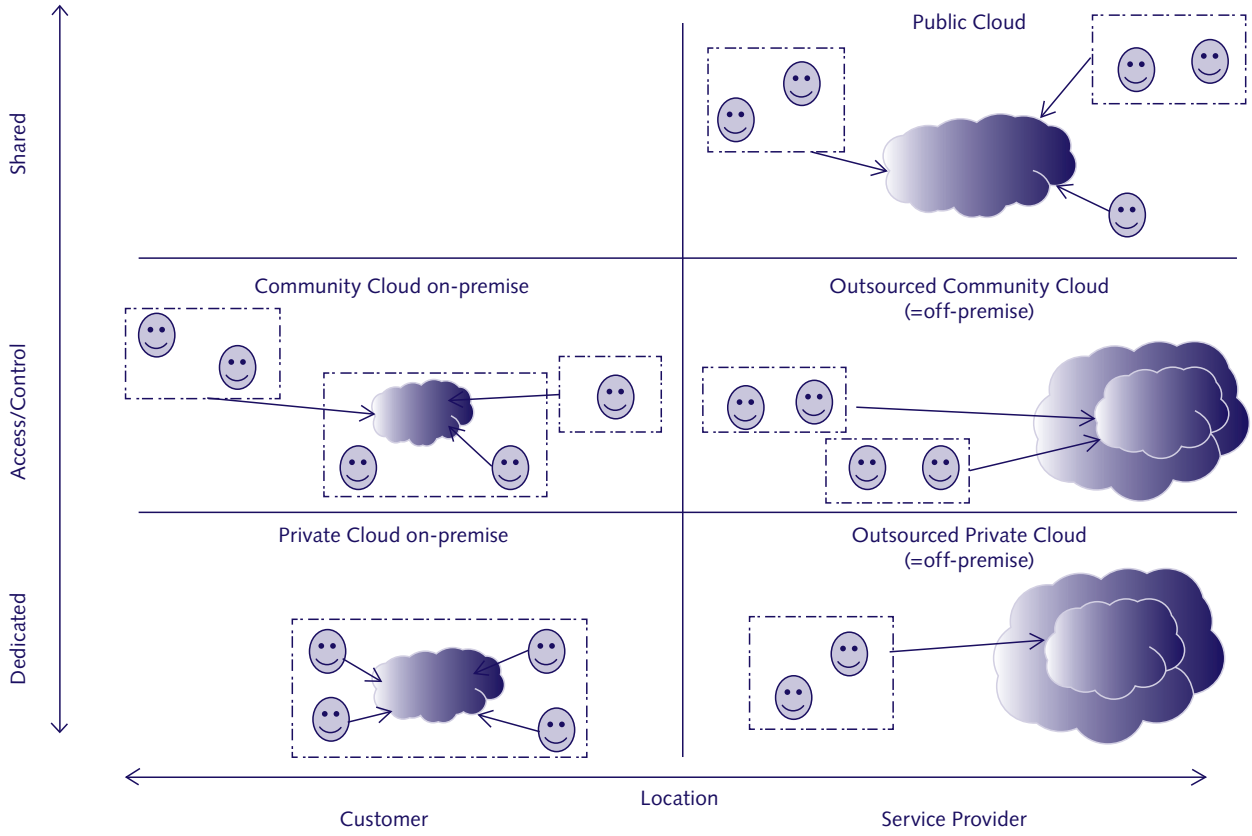
Cloud broker: Als je de risico's niet kent of niet de resources hebt om dit te onderzoeken, maak dan gebruik van een broker. Een opkomende vorm van dienstverlening die bepalend aan het worden is in de businessmodellen van cloud computing[51] is de zogeheten cloud broker. Er bestaat nogal wat onduidelijkheid over wat dit model precies inhoudt. Een gangbare definitie is dat het een

49. <http://nl.wikipedia.org/wiki/RACI-model>.

50. National Institute of Standards and Technology, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

51. <www.werken20.nl/nieuws-over-nieuwe-werken/technologie/32288/cloudbrokers-gaan-cloud-computing-vormgeven/>.

Figuur 1



professionele partij betreft die verantwoordelijkheid draagt voor de levering en beschikbaarheid van de clouddiensten aan een afnemer. De broker leidt bijvoorbeeld de selectie, onderhandelingen en relaties met cloudleveranciers en draagt verantwoordelijkheid voor het sluiten van adequate cloudcontracten met ieder van hen, daaronder begrepen de juridische aspecten en risicoafwegingen die verband houden met de gegevens van de afnemer. Cloud brokers richten zich veelal op het midden- en kleinbedrijfsegment en op multinationals en helpen hen hun bedrijfsprocessen in de cloud beter in te richten, nieuwe toepassingen te ontwikkelen en systemen te integreren waarbij het hebben van adequate controlepunten en de kwaliteitsbewaking daarover van vitaal belang zijn. Voor het midden- en kleinbedrijf is de broker bijvoorbeeld op zoek naar de beste manier om zich te abonneren op SaaS-applicaties. Voor grote ondernemingen zoekt de broker naar specifieke en gelijkwaardige 'enterprise-wide' cloudoplossingen waarbij veiligheidsstandaarden 'gekoppeld' worden aan type data/classificatie. In een NIST Standards Roadmap (2013) wordt dit model nader uitgewerkt.[52]

52. <www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf>.

Evolutie van ICT-contract naar cloudcontract

In verreweg de meeste gevallen waar software in licentie werd verkregen, draaide deze op eigen servers, hetzij binnen het bedrijf of organisatie, hetzij bij de privégebruiker thuis. Deze software werd via een schijf (floppydisk of cd-rom op de pc geïnstalleerd). Het gebruiksrecht was vastgelegd in een licentieovereenkomst.[53] Door de professionele afnemer werd in de regel met de software-eigenaar[54] een doorlopende onderhouds- en supportovereenkomst gesloten. Op basis hiervan had de licentienemer gedurende de contractsperiode recht op gebruiksondersteuning en nieuwe versies en updates van de software. Opslag van gegevens gebeurde op de eigen server/pc.

In geval van ICT-uitbesteding werden de software en de gegevens van de eigen servers verhuisd naar een andere locatie, te weten de servers van de beheer- en hostingpartij, met welke partij een beheer- en hostingovereenkomst werd geslo-

53. <www.iusmentis.com/computerprogrammas/licenties/bindendheid/>, met daarin ook een beschrijving van de zogenoemde *shrink wrap licentie*. Deze vorm van contracteren komt overeen met de vorm waarmee in de cloudomgeving wordt gecontracteerd, aangezien veelal met een 'muisklik' de leveringsvoorwaarden van de CSP worden geaccepteerd voordat toegang wordt verkregen tot de clouddienst.

54. Wij spreken hier bewust over de software-eigenaar, omdat de leverancier in de praktijk vaak een VAR (value added reseller)/distributeur betrof.

ten. Dit was vrijwel altijd een andere partij dan de software-eigenaar. De eerstgenoemde licentie-/onderhouds- en supportrelatie (en contracten) bleven daarbij veelal in stand. De software-eigenaar stemde dan in met de verhuizing.[55]

Als er iets mis was met de software, kon de afnemer zich wenden tot de software-eigenaar. Als er een probleem was met de hosting of toegankelijkheid van gegevens of applicaties kon de afnemer zich, met een beroep op de hosting- en beheerovereenkomst, wenden tot de hostingpartij. De software-eigenaar kon *bugs* in zijn software verhelpen. De hostingpartij wist waar de applicatie draaide en waar de gegevens waren opgeslagen en kon eenvoudig de oorzaak van het probleem vinden en herstellen. In deze situatie gaven de namen van de contracten ook duidelijk aan wat de aard van de afspraken of dienstverlening was.

In de beginperiode van ICT-outsourcing was er vaak ook sprake van zogenoemde *dedicated servers*, dat wil zeggen servers in eigendom van of exclusief aangehouden voor een specifieke afnemer. Als gevolg van soms grote pieken en dalen in belasting (reken- en verwerkingscapaciteit) en benodigde opslagruimte[56] kwam er in de loop der jaren behoefte aan samenwerking en het delen van computerkracht (reken- en verwerkingskracht en opslagruimte. De zogenoemde *shared server omgevingen* deden hun intreden. Diverse servers werden met elkaar gekoppeld. Leveranciers konden hierdoor goedkoper ICT, met name beheer- en hostingdiensten aanbieden. Vaak wisten de afnemers toen al niet met welke andere partijen zij de serverruimtes deelden. Maar dit gebeurde nog vrijwel uitsluitend binnen een fysieke locatie van de hostingpartij. Software werd al lang niet meer via schijven geïnstalleerd, maar via downloads.[57]

Met de opkomst van het internet en de mogelijkheden tot virtualisatie[58] via *software clients* zoals 'Citrix' of 'VM ware' werden de mogelijkheden letterlijk eindeloos. Hierdoor konden en kunnen in feite alle computers, netwerken en servers met elkaar gekoppeld worden en gebruikmaken van elkaars rekenkracht, verwerkingscapaciteit en opslagruimte (zie figuur 1). En hierdoor kan iedereen gebruikmaken van de vele mogelijkheden die het internet biedt, zowel voor bedrijven als voor consumenten, de overheid en non-profitorganisaties, zonder daarvoor grote investeringen in ICT te hoeven doen of licenties te hoeven aanschaffen en/of licentievoorwaarden te accepteren. Na een 'tussenperiode' waarin contracten werden aangeduid met termen als Application Service Provider-, Co Location- en Managed Internet Services-contracten en dergelijke, wordt nu vaak slechts nog gesproken over een cloudcontract.

55. In diverse standaardlicentievoorwaarden van grote softwareleveranciers staat dat het verhuizen van softwareapplicaties naar servers van derden is toegestaan, mits maar aan de licentievoorwaarden werd voldaan (zoals bijvoorbeeld het maximaal aantal gebruikers van de software).
56. Ter voorbeeld: een pensioenuitvoerder heeft in de maand december de grootste piek in benodigde computercapaciteit (reken- en verwerkingscapaciteit). Dat is de maand dat premies worden berekend, vastgesteld en voor alle pensioengerechtigden de uitkeringen worden berekend. In het geval de behoefte voor de maand december op '100' wordt gesteld, is de benodigde capaciteit, in vergelijking, voor de overige elf maanden maximaal '10' per maand. Om in de maand december niet in de problemen te komen kocht de organisatie capaciteit voor, zekerheidshalve, '105' in, zulks terwijl zij dergelijke capaciteit maar voor één maand per jaar nodig heeft. Hierbij werden derhalve veel onnodige kosten gemaakt en bleef veel capaciteit langere tijd ongebruikt. Via een shared omgeving kan dit opgevangen en beter verdeeld worden.
57. Zie bijvoorbeeld: <www.oracle.com/technetwork/indexes/downloads/index.html> en <www.adobe.com/nl/downloads/.html>.
58. Bij virtualisatie kunnen meerdere besturingsprogramma's worden opgestart, naast elkaar draaien en met elkaar communiceren, waarbij in de 'oude' situatie per harde schijf maar één besturingsprogramma kon draaien. Door bepaalde computerprogramma's kunnen naast het hoofdbesturingsprogramma één of meerdere andere besturingsprogramma's worden ingeschakeld. Deze programma's doen zich voor als een tweede of derde computer, maar het betreft in feite een gedigitaliseerde omgeving, vandaar de naam virtulisatie.

Figuur 2