VanDoorne Advocaten • Notarissen • Fiscalisten

RAND EUROPE

VERDONCK KLOOSTER & ASSOCIATES

CLOUD COMPUTING, FUNDAMENT OP ORDE

Eindrapportage

CLOUD COMPUTING, FUNDAMENT OP ORDE

Eindrapportage

André Hendriks, Erik Mark Meershoek met bijdragen van Van Doorne (Kees Stuurman et al) en RAND Europe (Neil Robinson, Jonathan Cave)

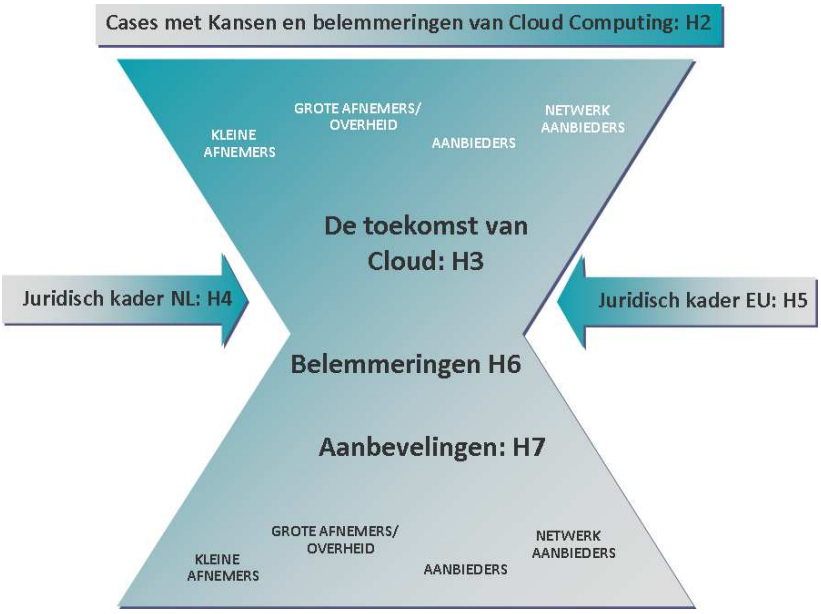
STATUS Definitief
VERSIE 1.1
PROJECTNUMMER 20110472

LEESWIJZER

Dit rapport start met een Management Samenvatting, gevolgd door een inleidend hoofdstuk waarin wordt ingegaan op het begrip Cloud Computing. Wat verstaan we er onder en wat is er, in vergelijking met de ontwikkeling die de IT de afgelopen 20 jaar heeft doorgemaakt, nu eigenlijk "nieuw" aan Cloud Computing?

De overige hoofdstukken in dit rapport zijn ingedeeld in drie delen:
DEEL I Hoofdstuk 2 en 3: Cases, ontwikkelingen en (toekomst)scenario's
DEEL II Hoofdstuk 4 en 5: Wet- en Regelgeving – Bijdrage Van Doorne en RAND
DEEL III Hoofdstuk 6 en 7: Belemmeringen en aanbevelingen

In onderstaand schema zijn de verschillende hoofdstukken afgebeeld. Afhankelijk van de invalshoek van de lezer, kunnen de verschillende delen los van elkaar worden gelezen.



Figuur 1 Leeswijzer

Deel I – Hoofdstuk 2 beschrijft een aantal cases rondom het gebruik van Cloud Computing. De voordelen van Cloud Computing, maar ook mogelijke bezwaren of belemmeringen van Cloud Computing worden vanuit het perspectief van een ondernemer beschreven. Lezers die al goed vertrouwd zijn met Cloud Computing kunnen dit hoofdstuk overslaan.
Deel 1 – Hoofdstuk 3 beschrijft een aantal ontwikkelingen en toekomstscenario's rondom Cloud Computing.

Het tweede deel van het rapport bevat een bijdrage van Van Doorne en RAND en gaat dieper in op de juridische aspecten van Cloud Computing. Dit deel is redelijk omvangrijk, enerzijds omdat een

groot aantal van de geconstateerde belemmeringen zich in het juridische domein bevinden, anderzijds omdat EL&I van nature verbonden is met het thema wetgeving.

In het derde deel van het rapport worden de huidige en verwachte belemmeringen van Cloud Computing samengevat (Deel III – Hoofdstuk 6). Deze belemmeringen zijn verdeeld in een vijftal categorieën. Vanuit deze belemmeringen worden in Deel III – Hoofdstuk 7 aanbevelingen gedaan om belemmeringen te verminderen of weg te nemen.

Voor de bronnen die bij de totstandkoming van dit rapport zijn gebruikt wordt verwezen naar bijlage A. In de tekst wordt naar deze bronnen verwezen als [R-xx], waarbij R-xx is terug te vinden in de lijst met referenties in bijlage A.

MANAGEMENT SAMENVATTING

CLOUD COMPUTING; HET FUNDAMENT OP ORDE

Zowel op Europees niveau als in Nederland bestaat er vanuit de overheid veel belangstelling voor Cloud Computing[1]. Eurocommissaris Kroes heeft diverse keren aangegeven dat zij Europa "Cloud-actief" wil maken. Kroes geeft daarbij aan dat Cloud Computing een belangrijke ontwikkeling is voor innovatie en economische groei in Europa. In lijn hiermee stelt ook de Nederlandse Digitale Agenda.nl dat Cloud Computing een belangrijke ontwikkeling is om efficiënter en flexibeler te werken en kan bijdragen aan productiviteitsgroei[2].

Het ministerie van Economische Zaken, Landbouw en Innovatie (EL&I) onderzoekt hoe zij kan bijdragen aan het wegnemen van belemmeringen en het stimuleren van het (veilig) toepassen van Cloud Computing. Ter ondersteuning van dit onderzoek schreef Verdonck, Klooster & Associates, in samenwerking met Van Doorne en RAND, het voorliggende rapport "Cloud Computing; fundament op orde". Vanuit bestaande onderzoeken en een beperkt aantal aanvullende gesprekken met diverse stakeholders, verschaft het rapport inzicht in effecten, belemmeringen en randvoorwaarden van Cloud Computing, worden conclusies getrokken en aanbevelingen aan EL&I[3] gedaan.

Het fenomeen Cloud Computing is volop in ontwikkeling en bevindt zich nog op de weg naar volwassenheid. Zowel voor aanbieders als afnemers biedt Cloud Computing een platform voor innovatie. Dit geldt voor zowel kleine als grote organisaties en de overheid als gebruiker van IT-middelen. Nieuwe ontwikkelingen volgen elkaar in hoog tempo op. Tegen deze achtergrond van een zich snel ontwikkelende, innovatieve en nog relatieve jonge markt, is het van belang dat de overheid waar mogelijk zorgt voor een goede voedingsbodem voor groei en verantwoord gebruik van Cloud Computing, zonder dat innovatie en marktwerking negatief worden beïnvloed. Met andere woorden, zorg dat het fundament op orde is! Met een stevig fundament kan groei van het aanbod en gebruik van Clouddiensten tot stand komen. Tegelijkertijd moeten aanbieders en afnemers ruimte krijgen om op dit fundament naar eigen inzicht te bouwen.

DE TOEKOMST VAN CLOUD COMPUTING

Diverse marktonderzoeken wijzen op een evolutionaire groei van Cloud Computing de komende jaren. Deze groei komt mede voort uit een aantal trends waarmee Cloud Computing nauw verweven is zoals Het Nieuwe Werken, keteninformatisering, consumerization en schaarste aan IT-experts. Ondanks de hoge verwachtingen rondom de groei van Cloud Computing in de komende

[1] Cloud Computing is een vorm van IT waarbij de toepassingen en/of IT-resources (zoals opslag- en verwerkingscapaciteit) als dienst via een netwerk (meestal het Internet) wordt afgenomen zonder dat de afnemer in eigen apparatuur en software hoeft te investeren. Een Clouddienst is daardoor overal toegankelijk en vanaf elk type randapparatuur met internettoegang te gebruiken.

[2] De gestelde produktiviteitsgroei is in dit onderzoek als aanname gehanteerd en niet nader onderzocht.

[3] Hierbij is ook aandacht besteed aan de rol van EL&I als wetgever, haar verantwoordelijkheid voor de Telecommunicatiewet in het bijzonder.

jaren, zal in 2015 de wereldwijde uitgave aan publieke Clouddiensten naar verwachting echter nog beperkt zijn tot een "single digit" percentage van de totale besteding aan IT. IT-aanbieders verwachten volgens onderzoek van ICT~Office in 2015 ruim 40 procent van hun ICT-diensten en -infrastructuur op basis van Cloud Computing te leveren. Uit ander onderzoek door Intertic blijkt dat wanneer een snelle adoptie van Cloud Computing kan worden bereikt er potentieel in Europa de komende 5 jaar tienduizenden nieuwe MKB's en tussen de 300.000 en 1,5 miljoen nieuwe banen kunnen ontstaan.

De voorspellingen rondom Cloud Computing zijn nog met veel onzekerheden omgeven. Technologische ontwikkelingen gaan snel en (onverwachte) gebeurtenissen kunnen van grote invloed zijn. Twee uiterste scenario's in dit kader: I) gebruik van Cloud Computing stagneert (of daalt) bijvoorbeeld als gevolg van grote (veiligheids)incidenten met persoonsgegevens, of II) door het succes van Cloud Computing krijgen één of meer aanbieders een belangrijk marktaandeel waardoor deze Clouddiensten wellicht aangemerkt moeten worden als "vitale infrastructuur", omdat uitval van de betreffende dienst leidt tot discontinuïteit bij een grote verscheidenheid aan organisaties met in het ultieme geval economisch en/of maatschappelijke schade voor Nederland.

Bij de totstandkoming van de aanbevelingen is, naast de twee genoemde, met verschillende scenario's rekening gehouden. Dat laat onverlet dat de onzekerheden en snelle ontwikkelingen rondom het onderwerp Cloud Computing maken dat EL&I op periodieke basis de gekozen beleidslijn met betrekking tot dit onderwerp tegen de actuele ontwikkelingen opnieuw zal moeten toetsen.

BELEMMERINGEN BIJ HET AFNEMEN VAN CLOUDDIENSTEN

Naast de vele voordelen die het gebruik van Cloud Computing biedt zijn er ook nadelen die een snellere groei en acceptatie van Cloud Computing in de weg staan. De meer dan 50 belemmeringen zijn onder te verdelen in vijf clusters. De clusters (in veel gevallen voor zowel aanbieder als afnemer) zijn:

- Zorg over de mate waarin wordt voldaan aan vigerende wetgeving. Zowel WBP als TW.
- Zorg rondom de beveiliging van en controle over data.
- Zorg over de beschikbaarheid/continuïteit van de dienst.
- De onvolwassenheid van Cloud Computing in het algemeen waardoor enerzijds voor veel organisaties nog geen passend aanbod beschikbaar is, en anderzijds sprake is van een gebrek aan transparantie in het aanbod van Clouddiensten (welk beveiligingsniveau wordt geboden en hoe is dit gewaarborgd? Wat is het service niveau en hoe wordt hierover gerapporteerd? Is continuïteit van dienstverlening gegarandeerd? Etc.).
- Zorg over dataportabiliteit en interoperabliliteit

In combinatie met negatieve publiciteit over incidenten die zich met Clouddiensten voordoen en al of niet terechte zorg over toegang tot informatie door andere overheden, hebben genoemde (clusters van) belemmeringen geleid tot een breed gedeelde zorg rondom het vertrouwen dat kan worden gesteld in Clouddiensten. Niet alleen vergen nog een aantal belemmeringen meer ontwikkeling om grootschalig gebruik van Cloud Computing (ook voor kritieke bedrijfstoepassingen) mogelijk te maken, ook dient aandacht besteed te worden aan het

verbeteren van het vertrouwen in Clouddiensten. Gebleken is dat percepties over voor- en nadelen niet altijd zijn gebaseerd op de feitelijke situatie.

De bijdrage die EL&I kan leveren aan het geheel of gedeeltelijk oplossen van de belemmeringen is vertaald in een viertal thema's met aanbevelingen.

THEMA 1: HET BEVORDEREN VAN TRANSPARANTIE EN VOLWASSENHEID

Uit het onderzoek blijkt dat de markt voor Clouddiensten nog volop in beweging is en nog niet het stadium van volwassenheid heeft bereikt, zeker daar waar het gaat om toepassingen ter ondersteuning van kritieke bedrijfsprocessen. Het aanbod is veelal nog onvoldoende afgestemd op de vraag. Dit geldt voor de markt voor (Openbare) Clouddiensten in het algemeen, maar bijvoorbeeld ook voor de specifieke markt voor Clouddiensten gericht op de overheid.

Behalve volwassenheid vormt het gebrek aan transparantie van de markt in het algemeen, en van individuele Clouddiensten in het bijzonder, een belemmerende factor voor snelle groei. Voor afnemers is het lastig vast te stellen welke Clouddiensten passen bij het gewenste service niveau, en hoe deze diensten in werkelijkheid presteren. Relatief eenzijdig opgestelde en ondoorzichtige voorwaarden dragen verder bij aan de ondoorzichtigheid. En dat terwijl het een complexe markt betreft met veel dienstverleningsaspecten die voor organisaties van groot belang zijn (beveiliging, responsetijd, beschikbaarheid, support etc.). Het gebrek aan transparantie leidt tot verschillen in perceptie en werkelijkheid, onzekerheid over de kwaliteit van de aangeboden dienst en een gebrek aan vertrouwen in de Cloud.

Meer transparantie, en de verdere ontwikkeling van Clouddiensten richting volwassenheid, zijn belangrijke voorwaarde voor het succes van Clouddiensten.

Aanbevolen wordt om het bevorderen van transparantie en volwassenheid als algemeen uitgangspunt te hanteren en nader uit te werken hoe EL&I hier, in samenwerking met de markt, concreet invulling aan kan geven.

Hoewel primair een verantwoordelijkheid van aanbieders en afnemers van Clouddiensten, kan het ministerie van EL&I bijdragen aan het proces van totstandkoming van meer transparantie. Hierbij kan worden gekeken naar initiatieven als certificering, voorlichting, vraagarticulatie en ontwikkeling en gebruik van (open) standaarden. Gelet op de snelle ontwikkelingen en het innovatieve karakter van Clouddiensten, wordt geadviseerd terughoudend te zijn met het fors inzetten van beleidsinstrumenten met een meer juridisch karakter. Door in te zetten op het stimuleren van de eigen verantwoordelijkheid van de aanbieders kan de markt, zo is de verwachting, zelf doorgroeien naar een volgend volwassenheidsniveau.

Om dit thema inhoud te geven volgen hieronder een aantal voorstellen voor vervolgacties.
Noot: Bij de onderstaande aanbevelingen wordt steeds aangegeven op welke doelgroepen de aanbevelingen het meest betrekking hebben. Met andere woorden, welke (groep van) actor(en) kan het meest bijdragen aan het wegnemen van belemmeringen binnen dit thema.

Aanbeveling 1.1 (afnemers klein). Steun en stimuleer brancheorganisaties en koepels bij a) sectorgerichte voorlichting gericht op het MKB, en b) sector- of branchegerichte vraagarticulatie en contractering.

Aanbeveling 1.2 (afnemers groot / overheid). Onderzoek in samenwerking met BZK de mogelijkheden om standaard voorwaarden voor (overheids) aanbestedingen op te stellen ter bevordering van de transparantie van Clouddiensten, en b) hoe ervaringen met Clouddiensten binnen de overheid structureel verzameld, vastgelegd en inzichtelijk gemaakt kunnen worden.

Aanbeveling 1.3 (aanbieders van Clouddiensten). Steun en stimuleer de totstandkoming van een breed gedragen certificering, keurmerk of erkenningsregeling in Nederland, of in EU verband.

THEMA 2. DUIDELIJKE EN GEHARMONISEERDE WET- EN REGELGEVING

Bij zowel afnemers als aanbieders bestaan veel zorgen over de mate waarin/wijze waarop zij voldoen aan vigerende wet- en regelgeving, bijvoorbeeld op het gebied van privacy. Hoewel Cloud Computing goed in het huidige juridische kader is in te passen; is op een aantal punten wel aanpassing gewenst. Aanbieders (en grote afnemers) van Clouddiensten hebben baat bij geharmoniseerde wet- en regelgeving tussen landen. In ieder geval tussen de landen binnen de EU, maar ook met de Verenigde Staten. Dit geldt zeker ook voor Nederland als land met een sterke internationale oriëntatie. Verder blijkt uit de inventarisatie voor dit rapport dat naast harmonisering ook behoefte bestaat aan verduidelijking van bestaande wetgeving, bijvoorbeeld de toepassing van de Telecomwet. Een helder onderscheid tussen de verschillende rollen bij de totstandkoming van een Clouddienst kan hierbij helpen.

Aanbevolen wordt om (in EU verband) de harmonisatie van regelgeving te bevorderen en zorg te dragen voor eenduidige wetgeving, rekening houdend met de opkomst van Cloudaanbieders in aanvulling op de al jaren bekende aanbieders van netwerkdiensten.

Opgemerkt wordt dat bij de aanbeveling om in EU verband de harmonisatie van regelgeving te bevorderen, ook hoort het voorkomen, of in ieder geval minimaliseren, van afwijkende of aanvullende regelgeving in Nederland zelf.

Om dit thema inhoud te geven volgen hieronder een aantal voorstellen voor vervolgacties.

Aanbeveling 2.1 (EU / Internationaal) Zet in op aanpassing, harmonisatie van wet- en regelgeving met betrekking tot privacy en andere relevante aspecten en monitor de ontwikkelingen in dit domein.[4]

[4] Toelichting: Met geharmoniseerde wet- en regelgeving wordt het voor aanbieders en afnemers duidelijker op welke manier met privacy-gevoelige informatie wordt omgegaan. Huidige onduidelijkheid voor aanbieders hoe om te gaan met de eisen van het land waaruit de gegevens afkomstig zijn wordt weggenomen doordat dit in alle landen dezelfde eisen zijn. In het onlangs uitgelekte ontwerp voor de nieuwe privacyverordening wordt duidelijke dat de Europese Commissie werkt aan een verordening en niet aan een nieuwe Richtlijn waardoor er geen nationale implementatievoorstellen meer nodig zijn.

Aanbeveling 2.2 (ministerie EL&I) Verduidelijk en of licht de relevante wetgeving en begrippenkader toe.[5]

Aanbeveling 2.3 (ministerie EL&I) Zet in Brussel de belangen van bedrijfsleven en met name die van het MKB op de agenda.

THEMA 3. DE ZORG VOOR CONTINUÏTEIT

Een belangrijke zorg met betrekking tot Clouddiensten is continuïteit. Het niet, of slecht, bereikbaar zijn van Clouddiensten kan direct gevolgen hebben voor de bedrijfsvoering bij afnemers, en misschien zelfs voor een hele sector of een deel van de Nederlandse economie. Het maken van een risicoafweging ten aanzien van uitval van een Clouddienst of –aanbieder is primair een verantwoordelijkheid van iedere individuele afnemer. Echter, de verzameling netwerken en systemen waaruit de Cloud is opgebouwd vraagt om een bredere kijk op continuïteit.

Daarnaast raakt continuïteit aan aspecten als dataportabiliteit. Continuïteit, gezien vanuit de afnemer van Clouddiensten, is gebaat bij de mogelijkheid voor afnemers om te allen tijde, snel en in een bruikbaar (standaard) formaat, over de eigen gegevens te kunnen beschikken.

Aanbevolen wordt de zorg voor continuïteit als algemeen uitgangspunt bij beleidsvorming te hanteren en nader uit te werken hoe EL&I hier concreet invulling aan kan geven.

Om dit thema inhoud te geven volgen hieronder een aantal voorstellen voor vervolgacties.

Aanbeveling 3.1 (aanbieders van Clouddiensten). Stimuleer aanbieders tot het nemen van continuïteitsmaatregelen.

Aanbeveling 3.2 (aanbieders van Clouddiensten) Monitor de mate waarin Clouddiensten vitaal zijn, of in de toekomst kunnen worden, en besluit op basis van de uitkomst van dit onderzoek over eventuele vervolgstappen, in nationaal en internationaal verband.

Aanbeveling 3.3 (aanbieders van Clouddiensten). Onderzoek op welke wijze in internationaal verband dataportabiliteit verder kan worden gestimuleerd.

Aanbeveling 3.4 (ministerie EL&I). Monitor (op termijn) of de huidige regelgeving met betrekking tot netneutraliteit (in de toekomst) geen belemmering vormt voor de groei van Clouddiensten.

[5] Toelichting: Onderzoek of het begrippenkader in de TW kan worden aangepast aan nieuwe ontwikkelingen zoals Cloud Computing, en streef naar duidelijkheid in wetgeving: op wie is de wet van toepassing en wat wordt verwacht? Een harmonisatie van basisbegrippen met betrekking tot netwerken, datatransport, Internet, Cloud Computing etc, helpt bij het vaststellen en toelichten van wettelijke kaders voor bijvoorbeeld de WBP, TelecomWet (inclusief de nieuwe meldplicht) en opsporingsmogelijkheden.

THEMA 4. STIMULEREN VAN HET GEBRUIK VAN CLOUD COMPUTING

Door een aantal andere landen wordt actief beleid gevoerd ter bevordering van het gebruik van Cloud Computing. Ook het ministerie van EL&I kan actief beleid voeren om het gebruik van Cloud Computing te stimuleren ter bevordering van de productiviteit en innovatiekracht van het Nederlandse bedrijfsleven. Hiermee wordt tevens de vooraanstaande positie van Nederland op het gebied van de (elektronische) infrastructuur versterkt. Nederland heeft één van 's werelds grootste internetknooppunten en is al jaren koploper in breedbandaansluitingen. Ook zijn Nederlanders in vergelijking met andere landen zeer actief op het Internet.
In een recent onderzoek van Roland Berger wordt de relatie gelegd met de topsectoren: Voor verschillende van de zogenaamde topsectoren is IT een belangrijke sleutel tot succes. In de topsectoren logistiek, tuinbouw, media en in de gezondheidszorg is het nu noodzaak sectorspecifieke systeemplatformen te creëren.

Eén van de belangrijkste sterktes van Nederland op het gebied van IT is zonder meer de aanwezige infrastructuur. Ons land is, dankzij uitstekende binnenlandse netwerken en internationale verbindingen, nu al de Digital Gateway to Europe op niveau van het fysieke netwerk. Met de vorming van sectorspecifieke systeemplatformen zet Nederland de volgende stap en breidt het haar positie uit van fysieke 'platte' digital gateway tot een virtuele 'intelligente' digital gateway. Het systeemplatform vormt de schakel tussen de sterke infrastructuur en de betreffende sector. (Roland Berger, Van een fysieke naar een intelligente Digital Gateway to Europe)

Aanbevolen wordt actief beleid te voeren dat is gericht op het stimuleren van het aanbieden en gebruiken van Clouddiensten.

Om dit thema inhoud te geven volgen hieronder een aantal voorstellen voor vervolgacties.

Aanbeveling 4.1 (aanbieders Clouddiensten). Stimuleer de ontwikkeling van aanbod en afname van Clouddiensten, zodat Nederland optimaal gebruik maakt van de positie die Nederland heeft (vestigingsklimaat, internetknooppunt.)

Aanbeveling 4.2 (afnemers en aanbieders Clouddiensten). Community Clouds bieden mogelijkheden voor sectoren om de belemmeringen van Openbare Clouddiensten weg te nemen of te verminderen Start met belanghebbenden een discussie over de (verdere) inzet van Community Clouds, bijvoorbeeld in sectoren Zorg, Onderwijs en Overheid.

- Topsectoren logistiek, tuinbouw, media en gezondheidszorg worden in onderzoeken als kansrijk genoemd

Aanbeveling 4.3 (aanbieders Clouddiensten). Stimuleer Nederlandse organisaties gebruik te maken van het door de EU beschikbaar gestelde budget voor onderzoek naar Cloud Computing.

- Uit onderzoek blijkt dat Nederland nog relatief weinig gebruik maken van het door de EU beschikbaar gestelde budget voor onderzoek naar Cloud Computing.

Aanbeveling 4.4 (afnemers groot/overheid). Geef als overheid het voorbeeld door meer van Clouddiensten gebruik te maken, en maak hierbij eventueel gebruik van ervaring opgedaan door overheden in andere landen.

Tot slot

De markt voor Cloud Computing is nog volop in ontwikkeling. Op weg naar meer volwassenheid zullen aanbieders van Clouddiensten zich in de toekomst steeds beter aanpassen aan klantwensen. Huidige belemmeringen rondom bijvoorbeeld contractvoorwaarden, transparantie, standaarden en integratie zullen door de marktwerking afnemen. Uitspraken in (proef)processen zullen gaan bijdragen aan een juridisch kader dat aanbieders en afnemers meer houvast biedt.

Ondanks de grote rol voor de markt in dat proces ligt er voor EL&I ook zeker een kans. Wanneer EL&I een impuls kan geven aan het wegnemen van een aantal belemmeringen rondom het aanbieden of gebruiken van Cloud Computing, ontstaat in Nederland een stevig fundament voor Cloud Computing. Dit vergroot de kans dat de markt voor Cloud Computing versneld volwassen wordt. Wanneer bovendien de aan Cloud Computing gekoppelde productiviteitsgroei realiteit wordt, zal de gehele Nederlandse economie een stap vooruit zetten. Wij zien voor EL&I een kans om met de gedane aanbevelingen die impuls ook vorm en inhoud te geven.

INHOUDSOPGAVE

1 INLEIDING

De afgelopen jaren is het fenomeen Cloud Computing[6] volop in de belangstelling komen te staan. Er wordt veel verwacht van Cloud Computing: meer flexibiliteit en schaalbaarheid van IT, lagere kosten en initiële investeringen en snellere ontwikkeling van nieuwe diensten. Tegenover de hoge verwachtingen staan de risico's die verbonden zouden zijn aan het gebruik van Cloud Computing. In de praktijk blijken de (vermeende) risico's voor veel organisaties een belemmering te zijn om van Cloud Computing gebruik te maken.

Om Cloud Computing te laten bijdragen aan de productiviteitsverbetering en innovatie van de BV Nederland en overheid, onderzoekt het ministerie van Economische Zaken, Landbouw en Innovatie (hierna afgekort tot EL&I) hoe zij kan bijdragen aan het wegnemen van belemmeringen en het stimuleren van het (veilig) gebruik van Cloud Computing. Daarnaast kijkt EL&I ook naar de ontwikkeling van Cloud Computing vanuit haar rol als wetgever (Telecommunicatiewet).

Scope van dit rapport
Dit rapport beschrijft de belemmeringen die aanbieders en (potentiële) afnemers van Cloud Computing diensten ervaren, en geeft inzicht in de rol die EL&I kan vervullen bij het wegnemen of verminderen van deze belemmeringen. De belemmeringen hebben in het algemeen betrekking op de Clouddiensten die voor meerdere organisaties toegankelijk zijn (Openbare Clouddiensten). In het kader van dit rapport is overigens geen nader onderzoek gedaan naar de relatie tussen het gebruik van Cloud Computing en productiviteitsverbetering en/of innovatie.

Dit rapport richt zich op organisaties (aanbieders en afnemers) van Clouddiensten en niet op de consument. De inhoud van het rapport kan dan ook niet één op één op consumenten van toepassing worden verklaard, al gelden verschillende bevindingen en conclusies geheel of gedeeltelijk ook voor consumenten.

1.1 Wat verstaan we onder Cloud Computing

De meest gehanteerde definitie van Cloud Computing is opgesteld door het US National Institute of Standards and Technology (NIST) [R-1] en luidt:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

VKA hanteert voor Cloud Computing de volgende definitie:

[6] We gebruiken de Engelse term Cloud Computing in plaats van de Nederlandse begrippen Wolkwebben (EU Digitale Agenda) of Wolkensysteem (Minister Donner in een AO rondom ICT-projecten bij de Rijksoverheid, 22/3/2011), en sluiten hiermee aan bij de gebruikte terminologie in de Nederlandse Digitale Agenda.nl.

> "Cloud Computing is een model voor het snel beschikbaar stellen van on-demand netwerktoegang tot een gedeelde pool van configureerbare IT-middelen (zoals netwerken, servers, opslag, applicaties en diensten), met een minimum aan managementinspanning of interactie met de aanbieder." [R-2]

Kenmerkend voor Cloud Computing is dat IT als dienst wordt afgenomen, deze dienst via het netwerk overal toegankelijk is en gebruik maakt van internetstandaarden waardoor de dienst vanaf elk type randapparatuur met internettoegang te gebruiken is.

Deze kenmerken gelden voor de meest zuivere vorm van Cloud Computing. Er bestaan echter verschillende vormen van Cloud Computing, waardoor niet altijd sprake is van gebruik van internetstandaarden of van toegankelijkheid vanaf "elk type" randapparatuur. Voor een uitgebreide beschrijving van de eigenschappen van Cloud Computing wordt verwezen naar bijlage B. Hierin worden ook de begrippen Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) en de verschillende vormen van Cloud Computing (Openbare/Public, Private, Community en Hybrid) toegelicht.

In dit rapport worden Cloud Computing diensten afgekort tot Clouddiensten. Wanneer wordt gesproken over, bijvoorbeeld, opslag "in de Cloud", wordt feitelijk bedoeld, opslag in systemen van een aanbieder van Clouddiensten, of Cloudaanbieder. De term Cloud verwijst naar het concept van een wolk. Dit concept wordt vaak gebruikt om te illustreren dat je niet precies weet hoe en waar jouw dienst tot stand komt en hoe die bij jou als afnemer wordt afgeleverd. De afnemer heeft alleen zicht op de "buitenkant" van de wolk, en kent niet de exacte inhoud en structuur daarbinnen.

De term Cloud Computing voor een breed scala aan IT-diensten gebruikt. De meeste van de geïdentificeerde belemmeringen hebben betrekking op Publieke Clouddiensten en niet op Private Clouddiensten. Wanneer we dus in het algemeen spreken over de belemmeringen van Cloud Computing, wordt al generaliserend een groter deel van de IT-uitbestedingsmarkt (ook die van de Openbare Clouddiensten) in de discussie betrokken, dan strikt noodzakelijk. Het oplossen van deze meer semantische problematiek is niet betrokken in de scope van de opdracht.

1.2 Voorbeelden van Cloud Computing

Hieronder een kort overzicht van veel gebruikte Clouddiensten:

- Opslag (storage): het bij een Cloudaanbieder opslaan van data. Bekende voorbeelden zijn Dropbox, KPN's back-up online of Microsoft's Skydrive;
- (web)Hosting: het bij een Cloudaanbieder opslaan van webpagina's zodat die middels het Internet bereikbaar worden;
- Internetbellen: het gratis communiceren via een Cloudaanbieder zonder tussenkomst van een traditionele telecomaanbieder. Het bekendste voorbeeld is Skype;

- Kantoorautomatisering: het afnemen van klassieke toepassingen zoals tekstbewerking en rekenbladen. Veel gebruikte toepassingen in dit kader zijn Google Apps en Microsoft's Office 365;
- Email: het afnemen van e-maildiensten (mailadres, opslag). Yahoo mail (310 miljoen gebruikers), Microsoft's Hotmail (350 miljoen gebruikers) en Google's Gmail (260 miljoen gebruikers) zijn bekende voorbeelden [R-3]. Microsoft levert haar voor veel organisaties/gebruikers bekende e-mailprogramma Exchange/Outlook ook via derde partijen als Clouddienst onder de noemer Hosted Exchange;
- CRM: het afnemen van diensten rondom het beheren van klantrelaties (CustomerRelationshipManagement). Het Amerikaanse bedrijf Salesforce.com startte in het jaar 2000 met het aanbieden van online diensten. Medio 2011 heeft het bedrijf bijna 100.000 organisaties als klant, met ruim 2 miljoen gebruikers;
- HR: het afnemen van diensten rondom het Human Resources of personeelsbeleid. Het Amerikaanse bedrijf SuccessFactors maakt op Cloud Computing gebaseerde HR-diensten. SuccessFactors heeft meer dan 3.500 klanten, met meer dan 15 miljoen abonnees in 168 landen;
- Social networking: diensten voor het vinden van mensen en delen van persoonlijke profielen met relaties en vrienden. Bekende voorbeelden zijn LinkedIn (gericht op zakelijke relaties), Hyves (gericht op Nederlandse burgers), Facebook (gericht op wereldburgers).

Er is een snel groeiend aantal toepassingen in de Cloud te vinden. Van Enterprise Resource Planning (ERP) tot Business Intelligence en boekhouden, van fotobewerking tot het ontwerpen van websites en van projectmanagement tot samenwerkingsruimten. In hoofdstuk 2 passeren aan de hand van cases een aantal typische Clouddiensten.

1.3 Stand van zaken

In 2009 is door Intertic, een internationale denktank, een economisch model ontwikkeld waarmee de economische impact van de adoptie van Cloud Computing is doorgerekend. Uit het model blijkt dat wanneer een snelle adoptie kan worden bereikt er potentieel in Europa de komende 5 jaar tienduizenden nieuwe MKB's en tussen de 300.000 en 1,5 miljoen nieuwe banen kunnen ontstaan [R-4]. In hoeverre Europa eind 2011 "op schema" ligt is niet bekend. KPMG geeft aan dat het marktaandeel van Cloud Computing in het totale IT-portfolio op dit moment nog marginaal is (<4%) [R-5]. Wel is duidelijk dat Cloud Computing op dit moment veel aandacht krijgt.

In de Europese Digitale Agenda is als actie opgenomen dat lidstaten voorzien in voldoende financiële steun voor een EU-strategie voor “wolkwebben” (Cloud Computing), met name ten bate van de overheid en wetenschap [R-6]. Eurocommissaris Kroes heeft diverse keren aangegeven dat zij Europa niet zozeer Cloud-vriendelijk wil maken, maar juist Cloud-actief. Kroes geeft daarbij aan dat Cloud Computing een belangrijke ontwikkeling is voor innovatie en economische groei in Europa [R-7].

In lijn hiermee beschrijft de Nederlandse Digitale Agenda (Digitale Agenda.nl [R-8]) dat Cloud Computing een belangrijke ontwikkeling is om efficiënter en flexibeler te werken en kan bijdragen aan productiviteitsgroei:

Om de potentie van Cloud Computing te benutten wordt een programma 'Productiviteit en Cloud Computing' gestart, in lijn met het voornemen om te komen tot een Europese Cloud Strategie. Dit programma heeft als doel na te gaan wat Cloud Computing de komende jaren gaat betekenen voor economische groei en productiviteit en inzicht te geven in de rol van de overheid, onder meer wat betreft het regelen van randvoorwaarden zoals standaardisatie (via open standaarden), continuïteit van dienstverlening, veiligheid en privacy. Qua toepassing van Cloud Computing zal de focus liggen op de overheid zelf en het MKB. [R-8].

1.4 Wat is nu eigenlijk nieuw aan Cloud Computing

Is Cloud Computing werkelijk een nieuw verschijnsel of is het, zoals wel wordt gezegd "nieuwe wijn in oude zakken". Na bestudering van diverse bronnen (bijlage A1) en het voeren van gesprekken met onder andere aanbieders van Clouddiensten, aanbieders van openbare communicatienetwerken en afnemers (bijlage A2) komt het volgende beeld naar voren: Vaak wordt Cloud Computing gezien als een volgende (logische) stap in de ontwikkeling die IT doormaakt. Nadat aanvankelijk organisaties voornamelijk alles zelf deden (middelen in eigendom, zelf beheer uitvoeren, en alles op de eigen locatie, ook wel "on-premise"), volgde de periode waarin meer en meer werd uitbesteed. Vaak werd uiteindelijk de complete IT-infrastructuur uitbesteed en fysiek op locatie van de beheerder ondergebracht. Met Cloud Computing schuift de grens verder op: de fysieke locatie waar de IT-middelen staan opgesteld kan zich nu in principe overal bevinden en de onderliggende infrastructuur wordt door de beheerder zodanig ingericht dat meerdere afnemers van dezelfde infrastructuur gebruik kunnen maken.

De volgende vier kenmerken onderscheiden Cloud Computing van de manier waarop organisaties tot voor kort IT toepasten;

- Delen van IT-middelen. Hard- en software wordt gedeeld door meerdere organisaties.
- Locatie onafhankelijk. Verwerking en opslag van informatie kan overal plaatsvinden.
- Dynamisch versus statisch. IT-middelen worden op verzoek (automatisch) dynamisch toegewezen of vrijgegeven waardoor de IT-infrastructuur en de manier waarop toepassingen daarvan gebruik maken continu in beweging zijn.
- Huur van diensten in plaats van investeren in IT.

Uiteindelijk leidt dit tot een fundamenteel andere manier van de inzet van IT; IT wordt een "commodity" en is eenvoudig in gebruik, vergelijkbaar met de afname van elektriciteit of water.

Opgemerkt wordt dat dit voornamelijk van toepassing is op een Openbare en in mindere mate Community Cloud. Op een Private Cloud zijn deze kenmerken niet, of slechts in heel beperkte mate, van toepassing. De verschillen tussen een Private Cloud en de manier waarop organisaties nu IT toepassen zijn klein, met name omdat organisaties al jaren Cloud Computing technieken toepassen. Het zogenaamde virtualiseren van servers vindt al op grote schaal, ook in de eigen IT-omgeving plaats.

Zoals aangegeven is de ontwikkeling richting Cloud Computing meer een stapsgewijs proces (evolutie) dan een revolutie die zich in een paar jaar volledig gaat voltrekken. De ontwikkeling is al langer gaande. Salesforce en Hotmail zijn voorbeelden van Clouddiensten die al jaren bestaan.

Door de opkomst van smartphones, tablets en social media zijn vooral consumenten de afgelopen jaren in toenemende mate opgeschoven naar de Cloud. Consumenten worden, vaak onbewust, verleid gebruik te maken van Clouddiensten. Een goed voorbeeld hiervan is de lancering van iCloud door Apple waardoor de grote groep van Apple gebruikers min of meer automatisch gebruik gaat maken van de (Openbare) Cloud. Organisaties worden hiermee geconfronteerd omdat consumenten de eigen middelen, zoals smartphones, tablets en toepassingen als Google Docs en Dropbox mee de organisatie in nemen.

1.5 Relevantie voor het MKB

Voor grotere organisaties is de stap van uitbesteden van IT-middelen naar het gebruik van Clouddiensten wellicht niet heel groot. Uitbesteden van IT-diensten was echter voor het MKB in veel gevallen nog erg ingewikkeld. Dit verandert wel door de opkomst van Cloud Computing. Zelfs een ZZP'er kan zich door het afnemen van Clouddiensten voor wat betreft zijn kantoorautomatisering goed meten met organisaties van vele tienduizenden medewerkers.

Grote organisaties kunnen waarschijnlijk vergelijkbare schaalvoordelen realiseren als Cloudaanbieders. Voor het midden- en kleinbedrijf, of beter bescheiden afnemers van Clouddiensten, geldt dit niet. Een startende ondernemer kan echter door het afnemen van Clouddiensten met een paar eenvoudige handelingen "state-of-art" IT-middelen tot zijn beschikking krijgen, tegen prijzen die moeilijk zijn te evenaren. Hiermee draagt Cloud Computing bij aan innovatie en verhoging van productiviteit bij het MKB.

Roland Berger concludeert in een studie ten behoeve van de OPTA [R-9] dat de kleinzakelijke klant met name lijkt te zoeken naar de mogelijkheden uit de publieke Cloud: *Veel van de behoeften van de kleinzakelijke klant zijn redelijk standaard en zijn kwaliteitseisen liggen lager dan in het grootzakelijke segment. Daarnaast is deze klant iets minder bezorgd over veiligheid, privacy en juridische complicaties dan de grootzakelijke klant. De grootzakelijke klant draait vaak al Remote Housing en Hosting-oplossingen voor relatief simpele diensten zoals e-mail en CRM en databeheer en zal zijn applicaties met name in een private cloud-omgeving willen plaatsen.*

Ondanks dat MKB bedrijven soms iets minder bezorgd lijken over enkele nadelen van Cloud Computing, zijn er voldoende belemmeringen die de afname van Clouddiensten door MKB bedrijven remt. Ook blijkt het "iets minder bezorgd zijn" nog wel eens een gevolg van

onwetendheid over de risico's die zijn verbonden aan het gebruik van Clouddiensten. Dit rapport gaat onder andere in op de ondersteuning die aan MKB bedrijven kan worden gegeven om verantwoord gebruik van Clouddiensten te stimuleren.

DEEL I:
CASES, ONTWIKKELINGEN EN (TOEKOMST)SCENARIO'S

2 CASES

Dit hoofdstuk beschrijft een aantal fictieve cases rondom het gebruik van Cloud Computing. De bedoeling is om met de cases een fors deel van de redenen om wel, en de belemmeringen om niet over te stappen op Cloud Computing te introduceren. Bij iedere case zijn twee items opgenomen:
- "Kansen die Cloud creëert" beoogt aan te geven welke impuls Clouddiensten kunnen geven aan economische activiteiten van de bedrijven uit de cases.
- " *Drempels voor het gebruik van de Cloud* " beschrijft een aantal geïdentificeerde belemmeringen.

2.1 Case 1: Klein reclame bureau

Deze case gaat over een klein bedrijf in de creatieve sector. Het betreft iReclame, een reclame bureau met vijf medewerkers. Voor dit bedrijf is IT is een middel dat medewerkers helpt in hun primaire proces: het bedenken van reclame campagnes. Daarnaast is het belangrijk dat de IT past bij het trendy imago van dit reclamebureau.

Bedrijf: creatief en veel contacten
Het ontwikkelen van reclame campagnes gebeurt iteratief in nauwe samenwerking met klanten en leveranciers. De medewerkers van iReclame zijn het creatieve brein van de campagne, ze gebruiken hun computer om concepten te visualiseren. Tegelijkertijd is de medewerker de organisatorische koppeling tussen de klant en de diverse leveranciers uit de traditionele en online reclamewereld. Daartoe communiceren medewerkers veel met klanten en leveranciers, op locatie en online.

Medewerkers: jong, trendy, Cloud minded
Het personeel is relatief jong en vanuit hun privé-omgeving gewend te werken met diensten vanuit de Cloud, zoals e-mail (Gmail), social media (Facebook, LinkedIn, Twitter), streaming media (Spotify), online foto's opslaan en delen (Picasa), online bestanden delen (Dropbox). Apple is zeer in trek bij de medewerkers van dit bedrijf. Deze IT fabrikant is vanuit haar historie sterk vertegenwoordigd in de grafische sector, maar heeft sinds enkele jaren een sterke marktpositie in de top van de consumentenmarkt. Apple's producten (MacBook, iPhone, iPad) zijn in hoge mate geïntegreerd met Apple's eigen Clouddiensten (iTunes, iCloud).

Huidige IT: persoongebonden apparaten met diensten uit de Cloud
iReclame biedt elke medewerker een laptop (MacBook) en een smartphone (iPhone). Op het bedrijfskantoor zijn geen servers en computers. De laptop is persoonlijk en wordt meegenomen naar klanten, leveranciers en naar huis. Op de laptop zijn, naast de min of meer standaard kantoorautomatiseringsoftware, een aantal pakketten geïnstalleerd die gebruikt kunnen worden voor het visualiseren van concepten. Hierbij spelen drie argumenten een rol. Ten eerste heeft iReclame vanwege de hoge interactiviteit en grote hoeveelheden data nog geen geschikt alternatief in de Cloud kunnen vinden. Ten tweede werkt er op een bepaald moment steeds maar één medewerker aan een bepaalde opdracht, waardoor een lokaal pakket geen beperkingen

oplevert voor het delen van informatie. Voor de uitwisseling onderling worden marktstandaarden gebruikt. Ten derde verliep de installatie van het pakket eenvoudig. Centrale applicaties (administratie pakket, intranet) worden online betrokken of elders gehost. Voor iReclame is het niet voor de hand liggend om haar eigen IT middelen aan te schaffen. In eerste plaats is er binnen het bedrijf is geen technische kennis aanwezig voor het installeren van servers. Daarnaast geven de eigenaren de voorkeur aan betaling per maand boven investeringen voor bedragen boven € 5.000. Bijkomend voordeel van deze Clouddiensten is dat het gebruik niet aan één locatie gebonden is, de administratie kan dus ook vanaf huis of andere locaties worden bijgewerkt.

Kansen die de Cloud creëert:
Indien iReclame tijdelijk een aantal extra mensen inhuurt, dan kan zij daarvoor een abonnement afsluiten voor alle Clouddiensten die iReclame gebruikt. Het gebruik van deze diensten vergt geen extra investering in licenties of hardware, bovendien zijn ze maandelijks opzegbaar.

Clouddiensten zorgen voor lagere investeringslasten en flexibilisering van IT kosten.

iReclame kan haar concepten gemakkelijk delen met leveranciers en klanten. Hiervoor kan bijvoorbeeld gebruik gemaakt worden van Google Docs of Dropbox. Veel gebruikers hebben al een account bij deze of een soortgelijke Clouddienst en anders kunnen ze eenvoudig en kosteloos een account aanmaken. Het voordeel van het delen van documenten via daarvoor ontworpen Clouddiensten, in plaats van bijvoorbeeld e-mail, is dat de laatste versie altijd centraal toegankelijk is voor iedereen en dat anderen daar op voort kunnen bouwen.

Clouddiensten verbeteren samenwerking over de grenzen van organisaties heen.

Drempels voor het gebruik van de Cloud:
iReclame maakt gebruik van meerdere Clouddiensten. Voor nagenoeg elke dienst is er een eigen wachtwoord nodig. De wachtwoorden worden op de laptop opgeslagen en soms automatisch ingevuld. Toch ergeren medewerkers zich aan alle wachtwoorden, met name bij incidenteel gebruik vanaf andere computers of bij het periodiek wijzigen van het wachtwoord.

De veelheid aan wachtwoorden voor Clouddiensten wordt door gebruikers als lastig ervaren.

Medewerkers van iReclame werken veel onderweg, bij klanten of bij leveranciers. Voor de verbinding met Internet zijn ze daar waar geen wifi is aangewezen op UMTS. Daarbij lopen ze aan tegen beperkte dekking van UMTS binnen kantoorpanden en de onvoorspelbaarheid van kosten/snelheid die gerelateerd zijn aan het op grote schaal gebruik maken van UMTS. Zeker bij gebruik in het buitenland lopen de kosten van dataverkeer snel op.

Beperkingen (locatie, tijd, geld) voor internettoegang remt de groei van Cloud.

Recentelijk bleek dat de gratis intranetsite die iReclame gebruikt, vanaf volgende maand geld gaat vragen voor haar dienstverlening. iReclame heeft andere gratis alternatieven gevonden, maar het

overzetten van de gegevens van de oude naar de nieuwe intranetsite bleek zoveel tijd te kosten, dat iReclame besloten heeft de huidige intranetsite tegen betaling voort te zetten.

Gebruikte standaarden of contractuele beperkingen zorgen in sommige gevallen voor een vendor lock-in.

Cloud economics:
Wat betreft de financiën heeft de directeur bij zijn besluit om mail uit de Cloud te betrekken een rekensommetje gemaakt op het "achterkant van een bierviltje". Hij was er snel uit dat e-mail als Clouddienst een stuk goedkoper is dan de inzet van eigen IT-middelen.

Cloud	*Zelf doen*
• *5 x zakelijk mail account bij Cloudaanbieder voor € 4 per maand per persoon*	• *Aanschaf server: 1 x € 1.000 voor 5 jaar, per jaar afschrijving € 200* • *Stroom (100 watt): € 200 per jaar* • *Licenties mailserver: € 500 per jaar* • *Support: 4 x 1 uur à € 50 per jaar* • *Backup: 1x € 100 voor externe disk + 15 minuten per week beheer*
Totaal per jaar: € 240,-	*Totaal: € 1.120 per jaar + 13 uur beheer per jaar*

2.2 Case 2: Middelgroot advocaten kantoor

Hendriks & Van Geest Advocaten (H&G Advocaten) is een advocatenkantoor met honderd medewerkers. Binnen de rechtspraak wordt nog veel gewerkt met papieren dossiers. H&G Advocaten zet IT in daar waar de toegevoegde waarde ervan bewezen is. De IT moet vooral betrouwbaar en niet te ingewikkeld zijn.

Bedrijf:onderdeel van een papieren keten
Binnen de rechtspraak worden dossiers uitgewisseld op papier. Officiële brieven worden van rechtswege vaak op papier verspreid. Informatie over wetgeving en jurisprudentie is elektronisch toegankelijk. Relaties met klanten zijn duurzame en langdurige van aard, persoonlijke binding is daarbij belangrijk.

Medewerkers: senior en traditioneel
Het bedrijf kent een aantal senior medewerkers (advocaten) die bepalend zijn voor de manier van werken binnen het bedrijf. Contacten met cliënten, rechtbanken en andere advocatenkantoren verloopt uit hun naam. De advocaten hebben vele jaren ervaring in de advocatuur. Zij zijn gewend

te werken met papieren dossiers. Elk van de advocaten binnen het kantoor kan rekenen op secretariële ondersteuning en een aantal juridische medewerkers die stukken voorbereiden.

Huidige IT:
De papieren dossiers vormen de brongegevens. In de kelder van het kantoor bevindt zich een archief dat te allen tijde compleet wordt gehouden. Documenten die tevens elektronisch voorhanden zijn worden wel bewaard, maar het elektronisch dossier is verre van compleet.

H&G Advocaten beschikt over een eigen server voor e-mail en opslag van bestanden. De IT apparatuur is eigendom van het advocatenkantoor en staat in een aparte ruimte in het kantoor. Het beheer is uitbesteed aan een lokale IT-dienstverlener die zich richt op het MKB. Eén van de partners van H&G Advocaten kent de directeur van de IT-dienstverlener persoonlijk, daarnaast heeft H&G Advocaten ooit een zaak gevoerd voor deze dienstverlener. De IT-dienstverlener zit in de buurt, dus als er iets niet werkt, dan zijn ze snel ter plaatste om het op te lossen.

Voor het bijhouden van de cliënt gegevens, de status van de dossiers en de registratie van gewerkte uren heeft het advocatenkantoor in het verleden software gekocht. De software bestaat uit een applicatie die geïnstalleerd is op één van de servers van het advocatenkantoor en cliënt-applicaties die geïnstalleerd zijn op de computers in het kantoor. De pakketten zijn aan het einde van hun levensduur. De IT-dienstverlener heeft aangegeven dat uit continuïteitsoogpunt gezocht moet worden naar een opvolger, omdat de huidige leverancier geen support meer verleent.

Uit beveiligingsoverweging is de IT van H&G Advocaten maar beperkt toegankelijk vanaf een locatie buiten het kantoor. Uit juridisch oogpunt (onder andere de Wet op Bescherming Persoonsgegevens) houdt H&G Advocaten de servers met informatie over cliënten het liefst binnen de muren van het kantoorpand[7].

Kansen die de Cloud creëert:
Internationale aanbieders van Clouddiensten hebben doorgaans een schaalgrootte waarbij de meerkosten van 7x24 uur beheer per week en redundante voorzieningen beperkt zijn. Hierdoor kunnen Clouddiensten vaak een betere beschikbaarheid bieden voor hetzelfde geld, dan wanneer een kleine of middelgrote onderneming zelf deze hoge beschikbaarheid zou willen regelen.

Clouddiensten bieden een hoge beschikbaarheid.

Grote aanbieders van Clouddiensten ondervinden veel imago schade wanneer een beveiligingslek in hun systemen publiek bekend wordt. Zij hebben daardoor alle belang bij een goede beveiliging van hun systemen. Dankzij de schaalgrootte die zij hebben, is het voor hen relatief gemakkelijker om actuele beveiligingskennis in huis te halen.

[7] Onder bepaalde voorwaarden is het mogelijk om ook gegevens die vallen onder de WBP op te slaan bij aanbieders (ook in het buitenland). Zie verder hoofdstuk 4 voor een beschrijving van de voorwaarden.

Leveranciers van Clouddiensten hebben veel belang bij een goede beveiliging en hebben de schaalgrootte om beveiliging ook goed te regelen.

Drempels voor het gebruik van de Cloud:
Officiële correspondentie wordt op papier ondertekend en (aangetekend) verzonden. Een belangrijk bezwaar tegen verzending per e-mail is het ontbreken van een breed gedragen en geaccepteerde manier voor het rechtsgeldig elektronisch ondertekenen. Er zijn, mede door ontwikkelingen vanuit de overheid, diverse rechtsgeldige systemen voor elektronische uitwisseling van gegevens (bijvoorbeeld eHerkenning als beoogd systeem tussen overheid en bedrijfsleven). Maar het gebruik en de acceptatie ervan halen het nog niet bij de handtekening op papier. Het digitaliseren van alle inkomende en uitgaande documenten en de archivering van het ondertekende origineel op papier, werkt belemmerend in de digitalisering van de keten. Maar ook standaarden voor documentuitwisseling binnen de keten zijn nog nauwelijks tot stand gekomen.

Het ontbreken van een breed ondersteunde en geaccepteerde rechtsgeldige elektronische handtekening belemmert de digitalisering binnen ketens.

H&G Advocaten wil geen gegevens over klanten opslaan bij bedrijven met hun hoofdkantoor in de Verenigde Staten. Deze bedrijven kunnen middels de USA PATRIOT Act verplicht worden gegevens ter beschikking te stellen aan de Amerikaanse overheid. Het advocatenkantoor vindt dit een onacceptabel risico voor de betrouwbaarheid van de naam die zij heeft opgebouwd. Dit punt ligt met name gevoelig bij haar klandizie binnen de overheidssector.

Juridische kaders voor de opslag van gegevens belemmeren het gebruik van Clouddiensten door bedrijven en instellingen.

2.3 Case 3: Horeca

Deze case gaat over café Chez Martin. Dit café in het historische centrum van Delft moet het vooral hebben van haar grote terras. Als service naar haar klanten biedt Chez Martin gratis draadloos internettoegang.

Bedrijf: voel je thuis bij Chez Martin
Chez Martin wil een fris en gezellig café zijn waar gasten zich thuis voelen. Het publiek is divers; jonge volwassenen, jonge gezinnen, vijftigers komen graag langs om er wat te drinken. Het personeel is vriendelijk en informeel.

Medewerkers: jong en flexibel
De meeste personeelsleden zijn jonger dan 24 jaar, veelal studenten die als bijbaan in de horeca werken. Zij zijn goedkoper dan oudere werknemers en flexibel inzetbaar. Er is een kleine kern van meer ervaren vaste krachten, die al jaren bij het bedrijf werken.

Huidige IT:
Chez Martin heeft sinds kort een nieuw kassasysteem. Met dit systeem kan het personeel bestellingen op het terras invoeren met behulp van een applicatie op een smartphone. De bestellingen worden automatisch doorgezet naar een scherm achter de bar, waar ze worden klaargezet. Zo kunnen ze snel worden uitgeserveerd. Afrekenen kan bij de kassa binnen in het café of bij een mobiele kassa op het terras. Alle gegevens worden bewaard bij de leverancier van het kassasysteem en zijn online te raadplegen. Deze online omgeving biedt naast het raadplegen gegevens over de omzet ondermeer koppelingen met een dienst voor kostprijscalculatie, een aantal bestelsystemen en administratiediensten. In de toekomst is het de bedoeling dat gasten de mogelijkheid krijgen om via hun eigen smartphone bestellingen op te geven en te betalen.
Het personeel kan een smartphone van de zaak gebruiken voor het opnemen van bestellingen. De meeste personeelsleden kiezen er echter voor om hun eigen smartphone te voorzien van de bestelapplicatie. Ze krijgen daarvoor een vergoeding van 10 euro in de maand van hun werkgever.

Kansen die de Cloud creëert:
De seizoensarbeiders die Chez Martin in de zomermaanden inhuurt om het terras te bemannen, kunnen eenvoudig worden toegevoegd aan het kassasysteem. Omdat het kassasysteem grotendeels in de Cloud werkt, kunnen middelen gedeeld worden en hoeft er enkel betaalt te worden voor de middelen die gebruikt worden. Dit betekent dat de extra abonnementskosten die in de zomer nodig zijn, in de winter weer kunnen worden afgebouwd.

Clouddiensten schalen mee met wisselende mate van gebruik, hierdoor ontstaat flexibilisering van IT kosten.

Clouddiensten zijn toegankelijk vanaf standaard randapparatuur, dit biedt mogelijkheden om zelfbediening verder te vergroten. Zelf-scan-kassa's in de supermarkt zijn al niet meer ongewoon, in deze case kunnen die dankzij gebruik van standaard randapparatuur ook doordringen in de horeca.

Clouddiensten vergroten mogelijkheden voor zelfservice.

Bij Clouddiensten wordt functionaliteit aangeboden vanaf centrale platformen. Waar vroeger nog installatie van nieuwe software nodig was, inclusief integratietesten met andere software, komt nieuwe functionaliteit bij Clouddiensten automatisch ter beschikking. Bij Clouddiensten wordt de functionaliteit centraal bepaald door de dienstverlener.

Clouddiensten verlagen de barrière voor gebruik van nieuwe functionaliteit.

Drempels voor het gebruik van de Cloud:
Voor het gebruik van Clouddiensten is toegang tot Internet noodzakelijk. Wanneer Clouddiensten worden toegepast in het primaire proces (voor de horecabranche is dit bijvoorbeeld het bestellen van een drankje), dan wordt het primair proces afhankelijk van de beschikbaarheid van internettoegang. Dit stelt hoge eisen aan de beschikbaarheid daarvan.

Clouddiensten verhogen de eisen voor beschikbaarheid van internettoegang.

Hierboven is geschetst dat bij het afnemen van Clouddiensten eenvoudig nieuwe functionaliteit kan worden toegevoegd. De keerzijde hiervan is wel dat er voor een individuele afnemer veel minder mogelijkheden bestaan om individueel maatwerk op de Clouddienst te (laten) ontwikkelen. Bovendien kan de huidige functionaliteit ook op enig moment door de aanbieder onnodig worden aangepast of zelfs verwijderd.

Clouddiensten bieden minder mogelijkheid voor individueel maatwerk.

Cloud economics:
De eigenaar heeft besloten zijn personeel € 10,- per maand (bruto) te geven wanneer zij hun eigen smartphone gebruiken in plaats van die van de zaak. Zo hoeft hij minder smartphones aan te schaffen. Bovendien heeft hij minder omkijken naar kapotte smartphones die zijn personeel per ongeluk heeft laten vallen, waar drank overheen is gegaan of die ergens op een tafel zijn blijven liggen.

Afweging voor eigenaar	
Zakelijk gebruik privé smartphone	*Smartphone van de zaak*
• *Vergoeding zakelijk gebruik privé smartphone: € 10,- per maand*	• *Aanschaf smartphone: € 300,-* • *Levensduur: 1 jaar* • *Geen abonnement nodig*
Kosten per jaar: € 120,- per personeelslid	*Kosten per jaar: € 300,- per personeelslid*

Voor het personeel is de vergoeding een leuk extraatje. Zij hebben doorgaans al een smartphone en het zakelijk gebruik leidt niet tot extra kosten. Dat komt omdat de communicatie verloopt via het draadloos netwerk van het bedrijf en niet via het netwerk van de telecomaanbieder.

Afweging voor personeel	
Zakelijk gebruik privé smartphone	*Smartphone van de zaak*
• *Geen extra kosten door meergebruik van privé smartphone* • *Vergoeding zakelijk gebruik van privé smartphone: € 10,- per maand bruto* • *Belasting: min € 4,- per maand*	• *Geen kostenbesparing op privé smartphone* • *Geen vergoeding*
Extra inkomen: € 72,- netto per	*Extra inkomen: € 0,- per jaar*

Afweging voor personeel

jaar

Het gebruik van Clouddiensten op basis van standaard randapparatuur, levert in dit geval dus voordeel op voor werkgevers én werknemers.

2.4 Case 4: Grote multinational

Deze case gaat over een grote internationale organisatie dat zich heeft gespecialiseerd in de productie en verkoop van koffie en thee: Nu-age Systems. Het wereldwijde kantoor bevindt zich in Europa en de koffie en thee wordt op diverse productielocaties ontwikkeld en gemaakt. In 132 landen worden de koffie en thee via een nationaal of regionale importeur, via groothandelaren bij de verkooppunten gebracht. Er werken wereldwijd ongeveer 50.000 mensen bij het bedrijf.

Bedrijf: groot en internationaal
Nu-age is groot maar daardoor ook zichtbaar en kwetsbaar voor bijvoorbeeld reputatieschade. Anderzijds is de koffie- en theehandel de afgelopen jaren steeds verder onder druk komen te staan en zijn de marges dun geworden. Nu-age probeert in haar productie- en distributiesystemen operational excellence na te streven. Het IT-beleid is gericht op het creëren van stabiele voorzieningen, maar ook op het verlagen van de Cost of Ownership.

Medewerkers: internationaal
De medewerkers van Nu-age hebben heel veel verschillende achtergronden. Niet alleen hun nationaliteit is anders, maar ook de cultuur, de leeftijd en mate van ervaring met IT-systemen zijn anders. Op het hoofdkantoor en de landenorganisaties werken relatief veel hoogopgeleiden. Op de productielocaties werken juist veel laagopgeleiden.

Huidige IT:
De landenorganisatie hebben relatief veel vrijheid rondom de inrichting van de IT-systemen. Wel moeten zij een aantal systemen verplicht afnemen: het centrale systeem voor Identiteit en Toegang (Identity and Access Management), het centrale systeem voor personeelsbeheer en het centrale systeem voor planning en productie. De laatste 2 systemen werken op basis het Server Based Computing concept. Vanuit het eigen datacenter van het hoofdkantoor, wordt voor duizenden gebruikers wereldwijd het systeem beschikbaar gemaakt. Door een kleine applicatie op de individuele werkplek te installeren kunnen de twee centrale applicaties benaderd worden. Door de omvang van de organisatie kan voor de eigen IT-middelen al veel schaalvoordeel worden bereikt. Het serverpark is geoptimaliseerd en leveranciers zijn bereid fikse kortingen te leveren wanneer Nu-age zich als klant meldt.

Kansen die de Cloud creëert:
Verschillende landen hebben in het verleden verschillende keuzes gemaakt rondom IT. Het ene land is gestandaardiseerd op Apple's MacOS, de ander op Microsoft's Windows XP en weer een ander op Microsoft's Windows Vista. Daarbinnen zijn weer allerlei verschillende keuzes voor de internetbrowser gemaakt.

Clouddiensten zijn veelal toegankelijk door gebruik te maken van standaard webbrowsers. Het feit dat verschillende gebruikers wereldwijd gebruik maken van verschillende platformen en browser doet nauwelijks meer ter zake. Het is nog niet helemaal gestandaardiseerd, maar het wordt voor Nu-age wel eenvoudiger om naast bestaande systemen ook andere toepassingen zoals Document Management of Customer Relationship Management snel een eenvoudig wereldwijd uit te rollen.

Clouddiensten werken veelal onafhankelijk van het gebruikte platform of browser. Dit maakt het standaardiseren van het gebruik van applicaties eenvoudiger.

Nu-age heeft soms te maken met grote internationale marketingcampagnes. Door spotjes op radio en televisie worden geïnteresseerden naar de website van Nu-age geleid. De impact van zo'n campagne op systemen kan enorm zijn. In enkele dagen stijgt het aantal bezoekers van de website naar miljoenen.
Daar waar in het verleden de webpagina's en eventuele webtoepassingen nog in het eigen datacenter draaiden, kiest men nu steeds vaker voor de inzet van gespecialiseerde bureaus die snel capaciteit kunnen op- en afschalen. Investeringen in het eigen datacenter zijn nu veel gericht op het opvangen van enorme pieken, waardoor uiteindelijk minder investeringen nodig zijn.

Clouddiensten zorgen voor lagere investeringslasten en flexibilisering van de inzet van IT-middelen.

Nu-age is zuinig op haar imago en kan het zich niet permitteren dat haar website niet bereikbaar is, of wellicht nog erger gehacked wordt. Door haar schaalgrote kan Nu-age redelijk goed zorgen voor deskundig personeel dat voorkomt dat de site gehacked kan worden. Toch ziet ze dat het steeds lastiger wordt om alle kennis in continuïteit beschikbaar te maken.

Clouddiensten kunnen zich specialiseren waardoor zij meer en actuele kennis rondom beveiliging in huis kunnen halen.

Drempels voor het gebruik van de Cloud:
Nu-age overweegt het gebruik van Clouddiensten voor personeelsgegevens en een systeem voor Customer Relationship Management (CRM),
Om dit moment is Nu-age nog terughoudend om de persoonlijke en privacygevoelige personeelsgegevens centraal op te slaan. Er is door een aantal juristen naar de mogelijkheden gekeken, maar men stuitte toch snel op veel verschillende eisen in verschillende landen, waardoor steeds per land bijvoorbeeld middels vergunningen toestemming aan de bevoegde autoriteiten moest worden gevraagd.

Het als werkgever in Clouddiensten (Openbaar of Privaat) opslaan van privacygevoelige informatie vanuit diverse landen is mogelijk, maar vraagt steeds per land een nader onderzoek naar het regelgevend kader en mogelijk per land een andere oplossing.

Bij de overweging om Clouddiensten in te zetten voor CRM zag Nu-age in eerste instantie twee grote belemmeringen in de standaardvoorwaarden van de Cloudaanbieder: 1) De aanbieder wilde niet aansluiten op het door Nu-age gebruikte (standaard)systeem voor Identiteits- en toegangsbeheer en 2) de aanbieder wilde niet ingaan op de eis van Nu-age om een back-up van de klantgegevens wekelijks op een externe locatie te plaatsen.

De standaardvoorwaarden van Cloudaanbieders zijn vaak eenzijdig. Cloudaanbieders zijn niet snel bereid hun standaardvoorwaarden op maat van de afnemer te maken.

Door haar omvang en hoog "showcase" karakter van Nu-age bleken de Cloudaanbieders uiteindelijk bereid in te gaan op de eisen van Nu-age. Gebruikers worden nu via het eigen systeem voor Identiteits- en toegangsbeheer doorgeleid naar de systemen van de aanbieder.

Noot: in de praktijk blijkt het mogelijk voor grote afnemers om afwijkende functionaliteit en/of afwijkende voorwaarden te bedingen. Zo heeft SURF bedongen dat verschillende diensten van Google worden ontsloten via SURFfederatie, het authenticatieplatform voor hoger onderwijs en onderzoek.

Een andere overweging om voorlopig af te zien van het opslaan van privacy-gevoelige gegevens in een centrale toepassing lag in de technische architectuur van de Cloudaanbieder. Het systeem dat Nu-age in overweging had draaide op een platform waarbij op grote schaal gebruik werd gemaakt van virtualisatie-technologie. Concreet betekende dit dat op een fysieke server van de aanbieder niet alleen toepassingen van Nu-age zouden kunnen draaien, maar ook toepassingen van andere organisaties. Hoewel de aanbieder beschikte over diverse certificaten (bijvoorbeeld SAS 70 en ISO 27001) en de goede beveiliging steeds benadrukte, was Nu-age van mening dat het gedeeld gebruik een toename van het risico op inbreuk op de gegevens betekent. De zorgen van Nu-age rondom haar eigen imago maakt haar terughoudend bij dergelijke risico's.

Door het delen van IT-middelen door aanbieders van Clouddiensten ontstaan, terecht of onterecht zorgen over de veiligheid van de gegevens.

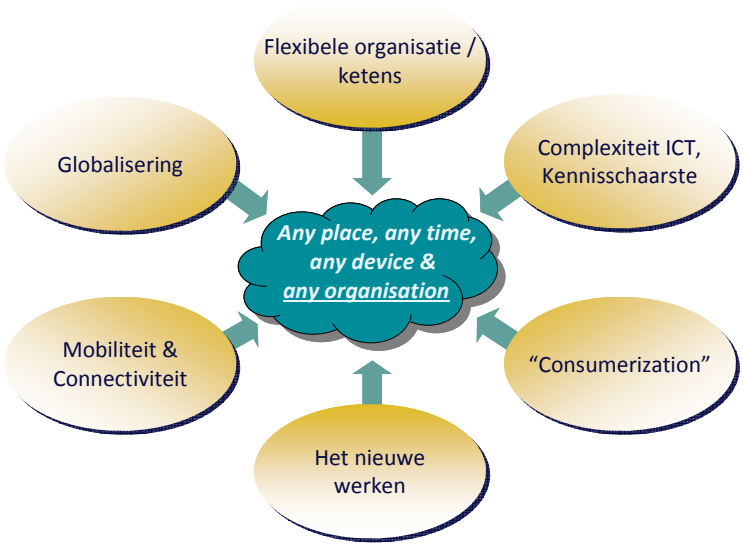
3 DE TOEKOMST VAN CLOUD COMPUTING

De ontwikkelingen in het IT-domein volgen elkaar al decennia lang in hoog tempo op. Nieuwe technologieën of producten die aanslaan worden in steeds kortere tijd door vele miljoenen gebruikers (wereldwijd) toegepast. Bekende voorbeelden zijn de opkomst van de smartphone en recent de tablet. Technologieën of producten kunnen daarentegen ook mislukken of na een periode van succes snel weer uit de belangstelling raken. Second Life is hiervan een goed voorbeeld. In de jaren 2007-2009 was dit een zeer populair dienst rondom een virtuele wereld. Bedrijven, politici en popsterren stortten zich in die tijd massaal op dit nieuwe medium. In 2011 is er nauwelijks nieuws meer rondom Second Life.

Tegen deze achtergrond is het moeilijk te voorspellen hoe de toekomst voor Cloud Computing er uit ziet. Toch is het voor een goed begrip van de belemmeringen (en de daarmee samenhangende maatregelen) voor het gebruik van Clouddiensten, relevant om inzicht te hebben in een aantal trends en (mogelijke) toekomstscenario's met betrekking tot Cloud Computing.

3.1 Cloud Computing in relatie tot andere trends

Cloud Computing is geen op zichzelf staande ontwikkeling, maar een die samenhangt met een aantal andere trends. De eigenschappen van Cloud Computing sluiten nauw aan bij de gevolgen die deze trends hebben voor het toepassen van IT. Flexibilisering en kostenverlaging zijn waarschijnlijk de belangrijkste voorwaarde voor het succes van Cloud Computing, zeker in deze economische onzekere tijden.



Figuur 2 Cloud Computing in relatie tot andere trends

- Flexibele organisaties / ketens / netwerken. IT-toepassingen blijven steeds minder beperkt tot de grenzen van de eigen organisatie. Toenemende ketensamenwerking en inzet van flexibele arbeidskrachten (toename ZZP'ers) vraagt om IT-toepassingen die hierop aansluiten. Clouddiensten zijn eenvoudiger over de grenzen van een organisatie toe te passen. Daarnaast

zorgt de schaalbaarheid van Clouddiensten er voor dat ZZP'ers en MKB'ers toegang krijgen tot IT-toepassingen die voorheen alleen voor grote organisaties beschikbaar waren.

- Complexiteit van IT en schaarste aan kennis. Ondanks de economisch mindere tijden is er sprake van schaarste van IT-specialisten [R-10]. Door IT-infrastructuren en –toepassingen te delen, kan efficiënter gebruik worden gemaakt van schaarse IT-kennis, bijvoorbeeld op het gebied van de beveiliging van IT.
- "Consumerization". De grens tussen zakelijk en privé vervaagt. Privé beschikken mensen vaak over de nieuwste middelen en wordt van (gratis) Clouddiensten gebruik gemaakt. Deze middelen (bijvoorbeeld de eerdergenoemde smartphones en tablets) en toepassingen neemt de consument mee naar het werk. De werknemer verwacht de eigen middelen ook voor zakelijke toepassingen te kunnen gebruiken ("Bring Your Own Device"). Gaten in het IT-aanbod van de werkgever vult de werknemer zelf op door gebruik te maken van Clouddiensten. Bijvoorbeeld Dropbox om gegevens te delen of "mee te nemen" of Google Docs om met collega's snel en eenvoudig te kunnen samenwerken.
- Het nieuwe werken en mobiliteit. Steeds vaker wordt werknemers de mogelijkheid geboden werk te doen onafhankelijk van locatie en tijd. Werknemers krijgen meer ruimte om zelf te bepalen wanneer en waar wordt gewerkt. Voor de werkgever levert het vaak een besparing op in benodigde kantoorruimte en mogelijk IT-beheerkosten. Voor de medewerkers kan het leiden tot een hogere tevredenheid. Clouddiensten zijn inherent tijd- en locatieonafhankelijk. Ook speelt Cloud Computing een rol bij de opkomst van mobiele randapparatuur dat wordt gebruikt om locatieonafhankelijk te kunnen werken (smartphones, tablets).
- Connectiviteit en Open Data. Steeds meer informatie komt via de Cloud beschikbaar. Niet alleen omdat organisaties (ruwe) gegevens ter beschikking stellen aan iedereen die hier gebruik van wil maken (Open Data), maar ook omdat een steeds grotere verscheidenheid aan objecten met het Internet in verbinding staat ("Internet-of-things"). Informatie over filevorming, komst van regenbuien, tracking van goederen etc. wordt door sensoren, camera's en andere technologieën verzameld en via de Cloud beschikbaar gemaakt voor Clouddiensten.

In deze economisch moelijke tijd, waarbij het voor bedrijven lastig is kapitaal aan te trekken als gevolg van beperktere kredietverstrekking door banken, biedt Cloud Computing mogelijk financiële voordelen. Er zijn geen (/weinig) initiële investeringen in IT nodig en de kostenstructuur van de onderneming kan door gebruik van Clouddiensten meer in lijn worden gebracht met de (onzekere toekomstige) omzet waardoor het financiële risico afneemt.
Zowel de druk op kostenverlaging/-flexibilisering als de hiervoor geschetste trends zetting zich naar verwachting de komende jaren voort. Verwacht mag worden dat hiermee ook de aandacht voor Cloud Computing voorlopig blijft bestaan.

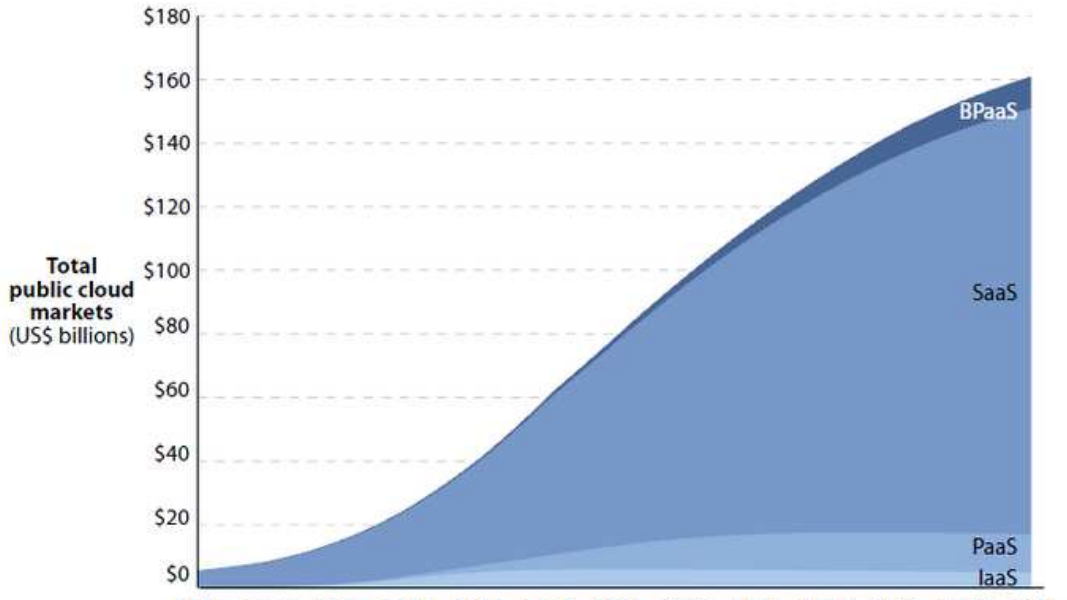
3.2 Groeiverwachtingen

Door analisten en marktonderzoek-organisaties worden regelmatig groeicijfers voor Clouddiensten gepubliceerd. De afgelopen jaren is gebleken dat deze cijfers regelmatig weer worden bijgesteld. Ook zijn niet alle cijfers op basis van volledig onafhankelijk onderzoek tot stand gekomen. Enige voorzichtigheid is dus geboden bij de interpretatie van groeicijfers voor Clouddiensten, met name die cijfers die worden gepubliceerd door de Cloudaanbieders zelf. Echter, de cijfers geven wel richting aan en verwoorden ook de verwachting die de markt heeft van Clouddiensten.

- Gartner [R-11]: in 2011 wordt wereldwijd $89 miljard besteed aan publieke Clouddiensten (was $74 miljard in 2010, ofwel 2% van de totale uitgave aan IT). Naar verwachting groeit de uitgave aan Clouddiensten vier keer sneller dan de groei in de totale uitgave aan IT. Dit resulteert in een wereldwijde besteding aan publieke Clouddiensten in 2015 van $177 miljard (5% van de totale uitgave aan IT). Wordt alleen gekeken naar de SaaS-markt dan verwacht Gartner dat in 2015 organisaties 15% van de uitgave aan bedrijfstoepassingen besteden aan SaaS-diensten ($20 miljard).

- Onderzoek ICT~Office: IT-bedrijven verwachten in 2015 ruim 40 procent van hun ICT-diensten en -infrastructuur op basis van Cloud Computing te leveren [R-12].

- Forrester [R-13]: de wereldwijde markt voor Cloud Computing, inclusief de Openbare en Private Cloud, zal groeien van $40,7 miljard in 2011 naar meer dan $241 miljard in 2020. Van de $40,7 miljard komt $25,5 miljard van publieke Clouddiensten.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
BPaaS ($)	0.15	0.23	0.35	0.53	0.80	1.26	1.95	2.93	4.28	6.00	7.66	9.08	10.02
SaaS ($)	5.56	8.09	13.40	21.21	33.09	47.22	63.19	78.43	92.75	105.49	116.39	125.52	132.57
PaaS ($)	0.05	0.12	0.31	0.82	2.08	4.38	7.39	9.80	11.26	11.94	12.15	12.10	11.91
IaaS ($)	0.06	0.24	1.02	2.94	4.99	5.75	5.89	5.82	5.65	5.45	5.23	5.01	4.78

Figuur 3 De groeiverwachtingen rondom Cloud Computing volgens Forrester [R-13]

Ook Roland Berger concludeert in een studie ten behoeve van de OPTA [R-9] dat er sprake is van een toename in Clouddiensten (in het rapport gevat onder de noemer Remote Housing & Hosting), al wordt daarbij opgemerkt dat volgens onderzoek van Forrester 80% van de ondernemingen nu

geen gebruik maakt van Openbare Clouddiensten in verband met zorgen over de gegevensbeveiliging. Roland Berger en SAP verwachten dat de wereldwijde verkoop van Cloud Computing in 2015 50 miljard euro oplevert [R-14].

3.3 Cloud Computing en Apps

De introductie van smartphones en tablets in het IT landschap hebben in hun kielzog nieuw leven ingeblazen in een al wat ouder fenomeen, de Appstore. Op Linux systemen is de Appstore al tien tot vijftien jaar oud en heet het ' repository'. Apple heeft met de introductie van de iPhone de Appstore succesvol in de markt gezet en het grote publieke bekend gemaakt met het concept. Andere aanbieders volgden, zoals Google met de Market voor Android apparatuur.
In het algemeen zijn Apps zogenaamde front-end toepassingen die zorgen voor een gebruiksvriendelijke interface die past bij het type randapparaat, en gebruik maken van de specifieke mogelijkheden die het apparaat in zich heeft (bijvoorbeeld locatiebepaling of Bluetooth communicatie mogelijkheden). Aan de achterkant zijn Apps vaak gekoppeld aan, en afhankelijk van, Clouddiensten. Voorbeelden van dergelijke Apps zijn Booking.com en Skyscanner. Hoewel veel Apps aan de achterkant communiceren met (open) webstandaarden, zijn de Apps zelf en daarmee ook de Appstores, afhankelijk van een enkel platform (bijvoorbeeld de platformen iOS of Android). Daarmee is een tegenbeweging in gang gezet die door zijn populariteit niet te stuiten lijkt, maar waarmee organisaties zich (toch) weer binden aan die nieuwe platformen.
Platformonafhankelijke 'Apps' zijn mondjesmaat in opkomst met de introductie van HTML5. HTML5 wordt door elke browser en daarmee tablet en smartphone ondersteund. Een voordeel voor ontwikkelaars van diensten is dat HTML5 platform onafhankelijk is terwijl Apps voor elk platform opnieuw ontwikkeld moeten worden. De toekomst zal uitwijzen of Apps of HTML5 de overhand krijgt of dat beide naast elkaar zullen bestaan.

3.4 Leveranciers investeren in Clouddiensten

De mate waarin leveranciers van IT oplossingen zich achter het concept van de Cloud scharen is een belangrijke succesfactor voor Clouddiensten. Om hiervan een indruk te krijgen kan worden gekeken naar de investeringen die leveranciers doen in Clouddiensten:

- Verizon investeert in de overname van Terremark ($1,4 miljard) en CloudSwitch [R-15];
- Microsoft claimt 90% van het R&D budget te investeren in Clouddiensten [R-16].
- In december 2011 werd Succesfactors voor 3,4 miljard dollar door het Duitse SAP overgenomen [R-17].
- Een aantal snel groeiende IT-bedrijven hebben het succes te danken aan de Cloud en investeren voornamelijk in Clouddiensten (Google, Amazon, Salesforce).
- 's Werelds grootste fabrikant van IT, Apple, investeert in Clouddiensten. Dit jaar is de dienst iCloud geïntroduceerd en biedt Apple onder andere muziekdiensten aan vanuit de Cloud. Dit is een verschuiving van iTunes dat lokaal op het apparaat draait.

Steeds meer leveranciers hebben, gelet op de investeringen die worden gedaan, een groot belang bij een doorbraak in het gebruik van Clouddiensten. Door hybride toepassingen te leveren wordt de afnemer, bewust of onbewust, meegenomen de Cloud in.

In de volgende paragrafen worden een aantal scenario's geschetst waarin de consequenties van de geschetste trends worden beschreven. De scenario's verkennen een denkbeeldig spectrum van succes tot falen van Cloud Computing.

3.5 Scenario 1: Ontwikkeling van Clouddiensten tot vitale infrastructuur

Niet uitgesloten kan worden dat één of meer Clouddiensten zich ontwikkelen tot een "vitale" infrastructuur. Dat wil zeggen, het niet, of gedeeltelijk, beschikbaar zijn van de dienst leidt tot significante maatschappelijke en/of economische schade. De volgende twee eigenschappen van Clouddiensten liggen hieraan ten grondslag:

- Eén enkele Clouddienst, dit kan zijn een toepassing (SaaS), platform (PaaS) of infrastructuur (IaaS), wordt door meerdere afnemers gedeeld. Uitval van één enkele dienst kan direct gevolgen hebben voor alle afnemers die van deze dienst gebruik maken.
- Clouddiensten zijn in veel gevallen verbonden met, en afhankelijk van, weer andere (onderliggende) Clouddiensten. SaaS-diensten draaien op een platform dat is ingekocht als PaaS-dienst. Voor de opslag van de data wordt weer gebruik gemaakt van een IaaS-dienst. Naarmate de verwevenheid van diensten groter wordt neemt het gevaar toe op een sneeuwbaleffect als één de diensten niet of slecht beschikbaar is;

Er kan een vergelijking gemaakt worden met telecommunicatie-infrastructuren, waarbij voor sommige van deze infrastructuren geldt dat uitval kan leiden tot ontwrichting van maatschappij en economie. In publicaties wordt soms zelfs al gesproken over Clouddiensten zoals Facebook die mogelijk uitgroeien tot een nutsvoorziening [R-18].

Tijdens de totstandkoming van dit rapport kwam Zweden in de publiciteit vanwege grootschalige uitval van IT-diensten met vergaande gevolgen voor veel organisaties. Het persbericht meldde [R-19]:

"STOCKHOLM - Zweden is getroffen door een enorme datastoring die sinds vrijdagavond veel belangrijke organisaties het werk lastig of onmogelijk maakt. Dat bevestigden verscheidene Zweedse organisaties maandag. Veel apotheken kunnen patiënten geen medicijnen op recept meer geven, het ambtenarenapparaat van gemeenten als hoofdstad Stockholm ligt plat, een groot deel van de autokeuringen kan niet volgens plan plaatsvinden, een belangrijke leenbank (SBAB) kan niets uitschrijven en ook de nationale studiefinancieringautoriteit is getroffen."

Een punt van aandacht in relatie tot vitale infrastructuren is aansprakelijkheid. Bij Clouddiensten is sprake van een overeenkomst tussen aanbieder en afnemer van de dienst. Hierin is de (mate van) aansprakelijkheid op individueel niveau vastgelegd. Echter, veroorzaakt een storing in de Cloud of in het netwerk een sneeuwbaleffect dat leidt tot verstoring van een (groot) aantal Clouddiensten met economische of maatschappelijke schade tot gevolg, dan kan de aansprakelijkheidsvraag moeilijk te beantwoorden zijn. Er is geen verantwoordelijke voor het totale stelsel.

3.6 Scenario 2: terugslag Clouddiensten door beveiligingsincidenten

Uitval van veel gebruikte Clouddiensten, of het verlies van (persoons)gegevens of toegang hiertoe door onbevoegden, komt regelmatig in de publiciteit. Een recent voorbeeld is de inbraak op het

systeem van Sony Playstation,waarbij persoonsgegevens van 77 miljoen gebruikers in handen van hackers is gevallen (waarna het Playstation netwerk dagen lang niet beschikbaar was). Ook op de site van Cheapticket.nl werd eerder dit jaar ingebroken met als gevolg dat onbevoegden toegang hebben gekregen tot persoonsgegevens van 715.000 klanten van Cheapticket.nl.

Het is onwaarschijnlijk dat genoemde incidenten de laatste zijn. Wanneer zich in de toekomst een aantal incidenten op rij voordoen met grote aanbieders van Clouddiensten, dan kan dit het imago van Clouddiensten schaden ("de Cloud is niet veilig"), met als gevolg een terugslag in de groei van Clouddiensten. Aanbieders van Clouddiensten zullen extra maatregelen nemen en langzaam het vertrouwen van de afnemer weer terug moeten winnen.

Het verlies van persoonsgegevens als gevolg van een inbraak ("hack") is niet alleen een probleem voor de klanten van de betreffende Clouddienst. Ook de aanbieders van Clouddiensten ondervinden snel de nadelige gevolgen van een inbraak in hun systemen. Afnemers maken gebruik van Clouddiensten omdat er een zekere mate van vertrouwen is in de aanbieder van de Clouddienst. Valt dit vertrouwen weg, bijvoorbeeld door verlies van persoonsgegevens, dan kunnen afnemers besluiten over te stappen op een andere dienst, met directe gevolgen voor de omzet/winst van de getroffen aanbieder. De sterke opkomst van sociale media (bijvoorbeeld Facebook, Twitter) zorgt er bovendien voor dat een slechte ervaring met een Cloudaanbieder snel breed bekend wordt.

3.7 Scenario 3: de Cloud redt het niet en sterft uit

Paragraaf 3.6 beschrijft een terugslag in de afzet van Clouddiensten als gevolg van een aantal serieuze beveiligingsincidenten. Er zijn ook scenario's denkbaar waarin niet alleen sprake is van een (tijdelijke) terugslag, maar zelfs van het uitsterven van Clouddiensten. Zoals in de inleiding van dit hoofdstuk aangegeven kunnen in het hedendaagse Internet tijdperk nieuwe diensten, technologieën en business modellen snel opkomen, maar ook weer snel verdwijnen. Wat is de volgende trend na Cloud Computing?

Naast de eerder genoemde beveiligingsincidenten zijn andere risico's voor het voortbestaan van Clouddiensten:

- Bedrijven en overheden hebben uiteindelijk toch te weinig vertrouwen in de Cloud om bedrijfskritische toepassingen uit de Cloud af te nemen;
- Het business / verdienmodel blijkt (op termijn) niet rendabel;
- Nieuwe (toekomstige) ontwikkelingen verdringen de Clouddiensten (bijvoorbeeld bij een verschuiving terug van centraal (Cloud) naar decentraal).

3.8 Scenario 4: Community Clouds hebben de toekomst

Een vorm van Clouddiensten tussen Openbare en Private in is de Community Cloud (zie ook bijlage B3). Diensten aangeboden vanuit een Community Cloud richten zich op een specifieke doelgroep en zijn ook alleen voor afnemers binnen die doelgroep toegankelijk.
Gartner ziet de opkomst van Community Clouds als één van de "transformational technologies" op de langere termijn (> 5 jaar) [R-20]. Ook Forrester verwacht een groei in Community Clouds [R-21].

Aan de mogelijke opkomst van Community Clouds liggen twee belangrijke drijfveren ten grondslag. Om te beginnen voldoen Openbare Clouds vaak niet aan de specifieke eisen die een sector stelt aan haar IT. Een Community Cloud kan worden ingericht conform de eisen en wensen van de sector. Denk bijvoorbeeld aan een Community Cloud voor ziekenhuistoepassingen of specifiek voor overheidstoepassingen. Een tweede argument voor de opkomst van Community Clouds zijn de bezuinigingen die de komende jaren moeten worden doorgevoerd en de zoektocht van organisaties naar samenwerking om hieraan invulling te geven. Voorbeelden van sectoren waarvoor dit geldt zijn Onderwijs, Zorg en Gemeenten. Community Clouds kunnen bijdragen aan meer samenwerking bij de ontwikkeling van IT en daarmee de kosten voor de deelnemende partijen verlagen.

3.9 Conclusie

Cloud Computing is geen op zichzelf staande ontwikkeling, maar een die samenhangt met een aantal andere trends, zoals Het Nieuwe Werken en consumerization. De meeste partijen zijn het er over eens dat het gebruik van (Openbare) Clouddiensten door organisaties de komende jaren groeit. Ook in 2015 zal de wereldwijde uitgave aan publieke Clouddiensten naar verwachting echter beperkt zijn tot een "single digit" percentage van de totale besteding aan IT (paragraaf 3.2).

De voorspellingen rondom Cloud Computing zijn echter nog met veel onzekerheden omgeven. Technologische ontwikkelingen gaan snel en (onverwachte) gebeurtenissen kunnen van grote invloed zijn. Twee uiterste scenario's in dit kader: I) gebruik van Cloud Computing stagneert (of daalt) bijvoorbeeld als gevolg van grote (veiligheids)incidenten met persoonsgegevens, of II) door het succes van Cloud Computing krijgen één of meer aanbieders een belangrijk marktaandeel waardoor deze Clouddiensten wellicht aangemerkt moeten worden als "vitale infrastructuur" omdat uitval van de betreffende dienst leidt tot discontinuïteit bij een grote verscheidenheid aan organisaties met in het ultieme geval economisch en/of maatschappelijke schade voor Nederland.

De volgende hoofdstukken zijn niet beschreven vanuit één gekozen voorkeursscenario. Er wordt met verschillende scenario's (behalve het afsterf-scenario) rekening gehouden.

DEEL II:
WET- EN REGELGEVING

4 JURIDISCHE CONTEXT: STAND VAN ZAKEN IN NEDERLAND

Dit hoofdstuk is opgesteld door het team van Kees Stuurman verbonden aan Van Doorne advocaten, notarissen en fiscalisten. In dit hoofdstuk wordt nader ingegaan op het juridische kader met betrekking tot Cloud Computing. Het onderzoek is gericht op het identificeren van die factoren die het gebruik van Cloud Computing diensten blokkeren dan wel belemmeren. Ook zal aandacht worden geschonken aan juridische aspecten die ten behoeve van het bevorderen van Cloud Computing nadere aandacht behoeven.

DE ESSENTIE VAN DE CLOUD PROBLEMATIEK

Cloud Computing is in essentie het via het Internet op afstand ter beschikking stellen van IT-voorzieningen, in de vorm van opslagcapaciteit, verwerkingscapaciteit of functionaliteit. Vanuit juridisch perspectief vertoont Cloud Computing derhalve (sterke) verwantschap met de uitbesteding van IT-voorzieningen maar ook met elektronische handel ('Internet based delivery').

Cloud Computing is ons inziens in het bestaande juridische kader relatief goed in te passen; wel is op een aantal punten aanpassing gewenst. Om barrières weg te nemen en het gebruik van Cloud Computing te stimuleren behoeft een aantal onderwerpen extra aandacht. In de kern samengevat, zijn dit juridische thema's rondom privacy, beveiliging, integriteit/betrouwbaarheid, toegang/continuïteit (incl. aspecten als invulling bewaarplichten en portabiliteit/‘lock-in’), contractuele voorwaarden en aansprakelijkheid. Hierna zullen wij op deze onderwerpen nader ingaan vanuit het perspectief van het Nederlands recht.

De beperking tot bovengenoemde onderwerpen betekent niet dat er geen andere juridische kwesties (kunnen) spelen in relatie tot Cloud Computing. Wij wijzen hier bijvoorbeeld op sectorale regels (zie onder) maar ook op meer generieke thema’s zoals intellectuele eigendom, mededingingsrecht (zie ook hoofdstuk 5), E-discovery, toepasselijk recht (zie onder) maar ook thema’s als toegang tot juridische expertise en toegang tot de rechter kunnen relevant zijn voor het bevorderen van het gebruik van Cloud Computing. In dit hoofdstuk blijven deze andere onderwerpen grotendeels buiten beschouwing gelet op de scope van het onderzoek (generieke toepassingen; zie hierna) en de beperking tot Nederlands recht dan wel omdat bepaalde kwesties niet specifiek zijn voor de Cloud maar ook bij andere vergelijkbare (internationale) transacties/dienstverlening aan de orde zijn.

TOEPASSELIJK RECHT

Hoewel Cloud Computing een typisch grensoverschrijdend fenomeen is, concentreren wij ons in dit hoofdstuk tot het Nederlands recht, omdat dit het meest relevant is voor Nederlandse afnemers en aanbieders. In het volgende hoofdstuk, wordt ingegaan op de Europese context. Het grensoverschrijdende karakter brengt automatisch de vraag met zich welk recht nu eigenlijk van toepassing is. Bij Cloud Computing speelt dat des te meer gelet op het vaak dynamische karakter van de gegevensopslag en het veelal aan de kant van de afnemer bestaande gebrek aan kennis over de precieze plaats of plaatsen waar zijn gegevens zijn opgeslagen. In een Cloud context kunnen zelfs meerdere rechtsstelsels naast elkaar van toepassing zijn. Via een in contracten te

maken rechtskeuze kan een deel van de onzekerheden worden weggenomen. Dat geldt echter niet voor de gevolgen van (meer) dwingende wettelijke bepalingen zoals bijvoorbeeld op het terrein van consumentenbescherming, privacy (zie onder), faillissementsrecht, strafrecht en (andere) regels voor toegang tot dataopslag door autoriteiten (zoals de veel besproken Amerikaanse USA PATRIOT Act; zie onder). Een belangrijk deel van de hier uit voortkomende onzekerheid is inherent aan internationaal zakendoen; mondiale harmonisatie is nu eenmaal geen gegeven. In de Internet context bestaat al veel aandacht voor het (verder) harmoniseren van regelgeving. Voor Cloud Computing is die ontwikkeling relevant en verdient deze ook verdere ondersteuning. Binnen de EU is in dit verband met name de ontwikkeling naar een 'digital single market' relevant. Aanbieders zouden ook meer transparantie moeten bieden ten aanzien van de locatie(s) waar gegevens worden opgeslagen (inclusief locaties voor uitwijk, back-up etc.) zodat (potentiële) afnemers een risicoafweging kunnen maken. In de markt is ook wel beweging op dit punt te zien; steeds meer maken providers de locatie van hun datacentrums tot 'selling point'.

GLOBALE SCHETS JURIDISCH KADER VOOR CLOUD COMPUTING

Voor wat de hoofdlijnen van het juridisch kader betreft zijn naar Nederlands recht voor Cloud Computing zowel het privaatrecht (Burgerlijk Wetboek), het publiekrecht (waaronder bestuursrecht, telecomrecht, fiscaal recht en mededingingsrecht) als het strafrecht relevant. De vorm van Cloud Computing (IaaS, PaaS, SaaS) als ook de sector waarin deze wordt toegepast, bepalen in een concreet geval mede waar het zwaartepunt van de juridische problematiek ligt. Zo gelden voor bijvoorbeeld de financiële sector maar ook voor de gezondheidszorg specifieke regels die direct relevant zijn voor de toepassing van Cloud Computing in deze sectoren.[8] Ook zijn er op bepaalde terreinen nog 'open vragen' die bij een verdere uitrol van Cloud Computing mogelijk een knelpunt kunnen gaan vormen. Een voorbeeld is de vraag in hoeverre er bij het afnemen van Cloud Computing diensten ter vervanging van bestaande infrastructuur/faciliteiten er sprake zou kunnen zijn van 'overgang van onderneming' met als gevolg een van rechtswege overgang van werknemers naar de Cloudaanbieder.

In het kader van dit onderzoek is het uiteraard niet mogelijk om de juridische aspecten van alle toepassingsmogelijkheden van Cloud Computing volledig in kaart te brengen. Wij beperken ons derhalve tot de hoofdlijnen voor generieke, niet-sector specifieke toepassingen van Cloud Computing. Met name zal nader worden ingegaan op de ons inziens meest relevante juridische 'issues' in het licht van de doelstelling van het bevorderen van de toepassing van Cloud Computing door in Nederland gevestigde bedrijven en instellingen, inclusief aanbiederzijde.

In dit hoofdstuk wordt binnen het hierboven geschetste kader nader ingegaan op de volgende aantal bijzondere juridische aandachtspunten voor het aanbieden en toepassen van Cloud Computing:

1. Privacy

[8] Voorbeelden zijn onder meer de uitbestedingsrichtlijnen van DNB, de dossierplicht op grond van de Wet geneeskundige behandelovereenkomst en de beveiligingsnorm voor de zorg (NEN 7510).

2. Beveiliging
3. Contractuele voorwaarden
4. Continuïteit
5. Aansprakelijkheid
6. Toegangsrechten overheidsinstanties

4.1 Privacy

Privacy in de sfeer van Cloud Computing beperkt zich voornamelijk tot de bescherming van persoonsgegevens. De regels inzake de bescherming van persoonsgegevens zijn voor Nederland vooral vastgelegd in de Wet bescherming persoonsgegevens (''WBP''). Voor een overzicht van de in de WBP gehanteerde begrippen, wordt verwezen naar bijlage C.
De WBP is gebaseerd op de EU Privacyrichtlijn 95/46. Momenteel is het privacyrecht volop in beweging. Eind vorig jaar verscheen (een uitgelekte) conceptversie van een voorstel voor een EU Privacyverordening die de EU Privacyrichtlijn op termijn dient te vervangen.
Hierna richten wij ons op het huidige Nederlandse recht, met de opmerking dat het landschap er over twee of drie jaar anders zou kunnen uitzien.

BEWERKER EN VERANTWOORDELIJKE

Naast de betrokkene zijn de twee hoofdrolspelers in de WBP de verantwoordelijke en de bewerker, waarbij de meeste verplichtingen rusten op de verantwoordelijke. Vanuit WBP perspectief is bij Cloud Computing denkbaar dat de klant de verantwoordelijke is, en de Cloudaanbieder de bewerker. Ook is mogelijk dat de Cloudaanbieder als (mede) verantwoordelijke gekwalificeerd moet worden, wanneer de Cloudaanbieder de gegevens ook voor eigen doeleinden verwerkt. In dat geval zal hij zelfstandig moeten voldoen aan de verplichtingen uit de WBP. De kwalificatie van Cloudaanbieders als bewerker en/of verantwoordelijke is niet eenduidig, echter de gevolgen van deze kwalificatie kunnen aanzienlijk zijn. De onduidelijkheid over deze kwalificatie brengt onzekerheid mee voor Cloudaanbieders en hun afnemers met zich; dit kan een belemmering zijn voor de ontwikkeling van Cloud Computing.

TOEPASSELIJKHEID WBP

De WBP is van toepassing als er persoonsgegevens worden verwerkt in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland. Ervan uitgaande dat de afnemer van de Clouddiensten de verantwoordelijke is en deze afnemer is in Nederland gevestigd, dient deze onderneming dus rekening te houden met de WBP. Ook is de WBP van toepassing als de afnemer van de Clouddiensten buiten de EU is gevestigd en er gebruik wordt gemaakt van middelen voor gegevensverwerking in Nederland, die niet uitsluitend bestemd zijn voor de doorvoer van persoonsgegevens. In lijn met een in 2010 afgegeven opinie van de Artikel 29 Werkgroep, het adviesorgaan van de Europese Commissie voor privacy-aangelegenheden, moet worden aangenomen dat deze laatste situatie zich voordoet indien bij het verwerken van persoonsgegevens bijvoorbeeld gebruik wordt gemaakt van servers, cookies, banners, search engines, sociale netwerken, Cloud Computing en/of outsourcing activiteiten in Nederland. Met inachtneming van onze eerdere overweging dat ook een Cloudaanbieder verantwoordelijke kan zijn, ontstaat nog een extra dimensie van de reeds gecompliceerde vraag over toepasselijkheid van de WBP. Ook hier kan de onduidelijkheid en daarmee onzekerheid over de toepasselijkheid van de

WBP een belemmering vormen voor Cloud Computing. Overigens kan de vraag naar de toepasselijkheid van de WBP op Europees niveau aan belang gaan inboeten indien inderdaad een EU verordening op het gebied van gegevensbescherming in werking treedt.

BEWERKERSOVEREENKOMST EN BEVEILIGING

Indien de Cloudaanbieder ''slechts'' een bewerker is, zal de klant met deze aanbieder een bewerkersovereenkomst moeten afsluiten. Daarin dienen de afspraken te staan over de beveiliging van de persoonsgegevens. In 2001 heeft (de voorganger van) het College Bescherming Persoonsgegevens (CBP) in een rapport een aantal risicoklassen geformuleerd ter invulling van de te nemen beveiligingsmaatregelen.

In dit rapport wordt een viertal risicoklassen onderscheiden:
• risicoklasse 0 publiek niveau;
• risicoklasse I basis niveau;
• risicoklasse II verhoogd risico;
• risicoklasse III hoog risico.

In onderstaand schema is de onderlinge relatie tussen de verschillende risicoklassen weergegeven. Het schema geeft een eerste indruk van de risicoklassen behorend bij een bepaald type persoonsgegeven én de hoeveelheid daarvan [R-22].

Aard van de persoonsgegevens:		Persoonsgegevens	Bijzondere persoonsgegevens	Financieel en / of economische persoonsgegevens
Hoeveelheid persoonsgegevens (aard en omvang)	*Aard van de verwerking*		Conform artikel 16 WBP	
Weinig persoonsgegevens	Lage complexiteit van verwerking	**Risicoklasse 0**	**Risicoklasse II**	**Risicoklasse II**
Veel persoonsgegevens	Hoge complexiteit van verwerking	**Risicoklasse I**	**Risicoklasse III**	

Tabel 1 Risicoklassen

Voor hogere risicoklassen gelden steeds strengere normen rondom het beveiligingsniveau van de gegevens. Deze risicoklassen en bijbehorende beveiligingsmaatregelen zijn onverminderd voor Cloud Computing relevant. Momenteel wordt overigens gewerkt aan een update van voornoemd rapport. Aannemelijk is overigens dat het maken van passende afspraken over het te hanteren beveiligingsniveau met name een obstakel zal kunnen zijn bij een Openbare Cloud. Bij een Private Cloud kan de afnemer ook op dit punt meer sturen.

DOORGIFTE

Een complicatie bij Cloud Computing is dat het voor klanten veelal ondoorzichtig zal zijn aan welke landen precies de gegevens worden doorgegeven. Als hoofdregel mogen persoonsgegevens alleen worden doorgegeven aan landen met een passend beschermingsniveau. Voor Cloud Computing is hierbij van belang om de onderkennen dat ten aanzien van de Verenigde Staten, waar met name

de grotere Cloud Computing aanbieders (Google, Microsoft, Amazon, e.d.) hun oorsprong vinden, de Europese Commissie heeft besloten dat enkel voor die organisaties die zich verplicht hebben tot naleving van de zogenaamde Veilige Haven Beginselen ("Safe Harbor Principles"), er sprake is van een passend beschermingsniveau. De genoemde grotere Cloud Computing aanbieders vallen hieronder.

Wanneer een land geen passend beschermingsniveau biedt, is de doorgifte toch toegestaan als er een beroep kan worden gedaan op een wettelijke uitzondering of als de minister van Justitie een vergunning heeft afgegeven voor de doorgifte. Bij Cloud Computing zijn de wettelijke uitzonderingen slechts beperkt toepasbaar. Daarom is de klant - naar huidig recht - veelal aangewezen op het aanvragen van een vergunning, die - zoals hierna nog wordt aangegeven - in combinatie met het sluiten van een EU modelcontract dient te worden aangevraagd. Daarbij moet de klant wel weten naar welke landen de doorgifte van de persoonsgegevens zal plaatsvinden, hetgeen problematisch kan zijn bij bepaalde vormen van Cloud Computing. De vergunning moet immers worden aangevraagd voor het doorgeven van persoonsgegevens naar een verantwoordelijke of bewerker, die gevestigd is een of meer bepaalde landen buiten de Europese Economische Ruimte[9] (EER). Om welke landen het gaat, moet in de vergunningaanvraag worden vermeld.

De vergunning wordt door de minister van Justitie verleend en dient via het CBP te worden aangevraagd. Aan de vergunningaanvraag worden nadere voorwaarden verbonden die als waarborg dienen voor de bescherming van de persoonsgegevens in kwestie. De eenvoudigste manier om aan te tonen dat deze waarborgen worden geboden, is door gebruik te maken van modelcontracten die goedgekeurd zijn door de Europese Commissie. Het in 2010 geïntroduceerde modelcontract tussen de verantwoordelijke/data-exporteur en de bewerker/data-importeur moet dan worden gesloten tussen de klant en de Cloudaanbieder. Overigens is dit modelcontract alleen van toepassing als de Cloudaanbieder buiten de EER gevestigd is. Onduidelijk is daardoor of het ook kan worden gebruikt als de Cloudaanbieder binnen de EER gevestigd is, maar gebruikmaakt van onderaannemers die gevestigd zijn in een land buiten de EER zonder passend beschermingsniveau. De kwestie van de vergunning zal overigens in de toekomst een minder heet hangijzer worden. Er is een wetswijziging ingediend waarin wordt voorgesteld de vergunningsplicht te laten vervallen indien gebruik wordt gemaakt van de ongewijzigde modelcontracten. Ook dan blijft echter gelden dat vooraf bekend moet zijn, naar welke niet-EER landen de gegevens zullen worden doorgegeven. Een andere mogelijkheid om de doorgifte te legitimeren is door gebruik te maken van Binding Corporate Rules (BCR's). Behalve dat het aanvragen van BCR's een nogal tijdrovende aangelegenheid is, geldt echter dat BCR's vooralsnog alleen beschikbaar zijn voor doorgifte binnen het concernverband van de verantwoordelijke. Indien de gegevens bij Cloud Computing aan de Cloudaanbieder als bewerker worden verstrekt, vormen BCR's vooralsnog geen oplossing.

[9] De EER bestaat uit de 27 landen van de Europese Unie en Liechtenstein, Noorwegen en IJsland.

INFORMATIEVERSTREKKING

Ook dient een afnemer van Clouddiensten (als verantwoordelijke) zijn gebruikers (de betrokkenen) nadere informatie te verstrekken over de verwerking van hun gegevens. Die informatie dient onder omstandigheden ook de ontvangers van de gegevens te omvatten. Daarbij geldt dat als de gegevensverwerking ook buiten de EER plaatsvindt, een afnemer zijn gebruikers veelal moet informeren over de doorgifte van hun gegevens. Aangezien veel Cloudaanbieders datacenters hebben buiten de EER, terwijl de afnemer van Clouddiensten veelal niet weet waar de gegevens worden verwerkt/opgeslagen, bestaat er veel onduidelijkheid bij afnemers of en hoe zij in het kader van Cloud Computing aan hun informatieplicht kunnen voldoen.

MELDPLICHT DATALEKKEN

Net als bij een IT-omgeving in eigen huis bestaat bij gegevensverwerkingen bij een Cloudaanbieder een kans op datalekken en daarmee op privacyinbreuken. Het past daarom rekening te houden met de te verwachten invoering van meldplicht rondom datalekken en continuïteit. Kern van de meldplicht zoals thans voorgesteld, is het door aanbieders van openbare telecommunicatiediensten onverwijld melden aan het slachtoffer en OPTA van een inbreuk op de beveiliging van persoonsgegevens. (het beoogde art. 11.3a Telecommunicatiewet, TW).
De meldplicht voor datalekken maakt onderdeel uit van wetsvoorstel 32.549, dat de Telecommunicatiewet wijzigt. Deze meldplicht komt voort uit de Richtlijn Burgerrechten 2009/136. Uiterlijk in mei 2011 had deze Richtlijn omgezet moeten zijn in de Nederlandse wetgeving. Deze deadline is niet gehaald. Het wetsvoorstel ligt nu bij de Eerste Kamer[10].

Volgens het wetsvoorstel zal de meldplicht vooralsnog alleen gaan gelden voor aanbieders van openbare telecommunicatiediensten. Omdat het risico van datalekken zich echter bij veel meer organisaties kan voordoen, is het de vraag of zo een beperkte meldplicht wel zinvol is. Daarom wordt er momenteel in Nederland en Europa gewerkt aan plannen om te komen tot een brede meldplicht. Als deze plannen doorgaan zal de meldplicht ook van toepassing zijn op andere organisaties die persoonsgegevens verwerken, zoals financiële instellingen, sociale netwerken, webwinkels, ziekenhuizen en OV-instellingen.

Op Europees niveau is deze uitbreiding pas te verwachten bij de herziening van de Privacyrichtlijn 95/46, die vermoedelijk zoals eerder aangegeven door een verordening zal worden vervangen. De Nederlandse overheid wilde daarop niet wachten. In december 2011 verscheen het voorontwerp van een wetsvoorstel voor de invoering van een algemene meldplicht (op te nemen in een nieuw artikel 34a WBP).

Wordt het voorgaande toegepast op Cloud Computing, dan geldt het volgende. Ervan uitgaande dat er inderdaad een algemene meldplicht zal worden ingevoerd, dan zullen de klanten van Cloudaanbieders, als verantwoordelijken, zowel de betrokkenen als de relevante toezichthouder moeten informeren over een lek in de beveiliging die gepaard gaat met de onrechtmatige verkrijging van persoonsgegevens uit de Cloud. Specifiek bij Cloud Computing is van belang dat de klanten voor deze informatie afhankelijk zullen zijn van hun Cloudaanbieder. Opdat ook de

[10] Stand van zaken januari 2012.

Cloudaanbieder weet waar hij aan toe is, is het voor beide partijen daarom raadzaam in de dienstverlenings- c.q. bewerkersovereenkomst nu reeds afspraken te maken over de invulling van de meldplicht.

4.2 Beveiliging

In de Nederlandse wet- en regelgeving is slechts op een beperkt aantal plaatsen een expliciete verplichting opgenomen tot het beveiligen van gegevens. Een voorbeeld voor persoonsgegevens is artikel 13 WBP.[11] Een ander voorbeeld vormt de verplichting uit hoofde van de Wet geneeskundige behandelingsovereenkomst tot het adequaat beveiligen van gegevens in de zorg[12]. Echter ook indien geen expliciete wettelijke verplichting tot het adequaat beveiligen van gegevens is opgenomen kan uit algemene normen (zorgvuldigheidsnormen, redelijkheid en billijkheid) voor tal van situaties de verplichting worden afgeleid om gegevens te beveiligen. Dit is niet anders bij het toepassen van Cloud Computing. Voor zover het persoonsgegevens betreft biedt de WBP een expliciet raamwerk. In de meeste andere gevallen zullen partijen afspraken moeten maken over het beveiligingsniveau dat zal worden toegepast.

Met betrekking tot beveiliging bestaan veel vraagtekens en onzekerheden, in de kern zijn deze echter niet van strikt juridische aard. Veelal betreft het zorgen over het realiseren van de mogelijkheden (en zeker ook kosten) van een adequaat beveiligingsniveau en de gevolgen van het eventueel doorbreken van die beveiliging. Ook voor dat laatste geldt dat het toepasselijke juridisch kader in principe duidelijk is (en ook in ontwikkeling; vergelijk de in de toekomst breder toe te passen verplichting tot het melden van datalekken), en als zodanig ons inziens niet een belemmering of beperking van de mogelijkheden voor de toepassing van Cloud Computing vormt. Wel geldt uiteraard dat het verder verduidelijken van de, veelal open, juridische normen (zoals de hiervoor genoemde norm uit artikel 13 WBP, maar ook die uit artikel 11.2 Tw) op dit punt kunnen bijdragen tot een groter vertrouwen in Cloud Computing.

4.3 Contractuele voorwaarden

In zijn algemeenheid kan worden gesteld dat voor de afnemers een aantal bezwaren kleeft aan de voorwaarden waaronder met name grote Amerikaanse aanbieders (Google, Microsoft, Amazon, e.d.) Cloud Computing in Nederland aanbieden. De betreffende voorwaarden worden doorgaans als sterk eenzijdig, niet onderhandelbaar en weinig transparant beschouwd. De voorwaarden zijn in de regel gemodelleerd naar de contractmodellen welke door de betreffende aanbieders in de Verenigde Staten worden gebruikt en kenmerken zich door weinig toegankelijk taalgebruik, mede gekleurd door veel (vertaalde) Angelsaksische begrippen en een voor de lezer complexe structuur in termen van gelaagdheid en doorverwijzing naar andere relevante (contract) documenten, zoals *privacy policies*.

Voor de kleinzakelijke of particuliere eindgebruiker zijn de voorwaarden in de praktijk niet onderhandelbaar. Vanuit het perspectief van de aanbieders is dit niet helemaal onbegrijpelijk,

[11] Op de invulling van deze verplichting kan ook de bewerker zelfstandig worden aangesproken.

[12] In relatie tot het BurgerServiceNummer(BSN): art. 10 Wet gebruik burgerservicenummer in de zorg en art 2. Regeling gebruik burgerservicenummer in de zorg. Maar zie verder onder meer ook art. 7:457.

aangezien een sterke mate van standaardisatie een belangrijk kenmerk is van Cloud Computing. Voor (grote) bedrijfsmatige gebruikers bestaat er in de praktijk wel enige ruimte om te onderhandelen over de inhoud van de voorwaarden. Naarmate er meer sprake is van een Openbare Cloud zal per definitie de ruimte om de voorwaarden daadwerkelijk aan te passen, beperkt zijn. Aanbieders van Clouddiensten zouden hun marktpositie mogelijk kunnen verbeteren (en derhalve het gebruik van Cloud Computing kunnen stimuleren) door meer toegankelijk en transparant te communiceren over de voorwaarden waaronder zij hun diensten aanbieden.

INHOUD VOORWAARDEN

Voor wat de inhoud van de betreffende voorwaarden betreft, kunnen kritische kanttekeningen worden geplaatst bij de wijze waarop daarin wordt omgegaan met onderwerpen zoals de bescherming van persoonsgegevens, vertrouwelijkheid van gegevens en verdeling van risico's. Dit betreft met de name de verdeling van verantwoordelijkheden ten aanzien van de bescherming van persoonsgegevens (verantwoordelijke of bewerker) en het veelal ontbreken van harde waarborgen, en sterker nog het vergaand beperken van verantwoordelijkheden, inzake onder meer toegankelijkheid en vertrouwelijkheid van gegevens.

Ten aanzien van consumenten /eindgebruikers ligt hier ook een spanning met het onderliggende businessmodel van deze aanbieders; de betreffende diensten worden veelal om niet aangeboden, waarbij als tegenprestatie de gebruiker geconfronteerd wordt met reclame-uitingen. Verder kunnen gegevens over (het gebruik van) de dienst door de aanbieders doorverkocht worden aan derden. Het Burgerlijk Wetboek (Boek 6, Titel 5, Afdeling 3) bevat wel enige bescherming voor gebruikers tegen onredelijk bezwarende algemene voorwaarden. Indien een bepaling als onredelijk bezwarend moet worden beschouwd, staat in beginsel een beroep op vernietigbaarheid van die bepaling open. De Cloudaanbieder kan dan geen beroep doen op bedoelde onredelijke bepaling. Welke bepalingen als onredelijk bezwarend moeten worden beschouwd, zal van geval tot geval verschillen. Voor Nederlandse consumenten is wel enige duidelijkheid geboden door de zogeheten 'zwarte lijst' en 'grijze lijst' van onredelijk bezwarende bepalingen. Ook de in een bijlage bij Richtlijn 93/13/EEG opgenomen oneerlijke bedingen in consumentenovereenkomsten (ook wel 'blauwe lijst' genoemd) zijn in dit verband relevant.

Voor ondernemers ligt de beschermingsomvang anders. Voor Nederlandse ondernemers (zowel grootzakelijk als kleinzakelijk/MKB) staat geen beroep op bescherming tegen onredelijk bezwarende voorwaarden open indien de Cloudaanbieder niet in Nederland is gevestigd. Bepalend hierbij is de vestiging van waaruit de Clouddienst wordt verricht. Voor de Clouddiensten van met name de grote buitenlandse aanbieders (Google, Microsoft, Amazon, e.d.), waar het probleem van eenzijdige en weinig transparante voorwaarden het meest wordt gevoeld, biedt Boek 6, Titel 5, Afdeling 3 van het Burgerlijk Wetboek dus geen bescherming. In zuiver Nederlandse verhoudingen geldt bovendien dat grootzakelijke gebruikers (ondernemers die een jaarrekening openbaar hebben gemaakt of ondernemers met 50 of meer werknemers) van de bescherming uit Boek 6, Titel 5, Afdeling 3 van het Burgerlijk Wetboek zijn uitgesloten. Nu grootzakelijke gebruikers in de praktijk wel enige ruimte zullen hebben om te onderhandelen over de inhoud van de voorwaarden, kan dit gebrek aan bescherming ons inziens niet snel als een blokkerende factor worden beschouwd voor gebruik van Cloud Computing.

Voor kleinzakelijke gebruikers (MKB) ligt de situatie meer gecompliceerd. Wel kunnen zij terugvallen op de open norm van vernietigbaarheid van onredelijk bezwarende algemene voorwaarden. Het meer concrete houvast van de drie lijsten ('zwart', 'grijs' en 'blauw') geldt echter in principe alleen voor consumenten. Toch kunnen de lijsten wel enige invloed uitoefenen op de toetsing aan de open norm (de zogeheten 'reflexwerking'). Dit zal met name het geval zijn indien de kleinzakelijke gebruiker in het concrete geval een met een consument vergelijkbare positie inneemt in verhouding tot de Cloudaanbieder. Nu kleinzakelijke gebruikers in de praktijk weinig onderhandelingsruimte hebben, zou meer duidelijkheid over de mogelijkheden om een beroep te doen op de bescherming tegen onredelijk bezwarende voorwaarden ons inziens drempels kunnen wegnemen richting gebruik van Cloud Computing door de kleinzakelijke/MKB-markt. Desondanks kan de vraag worden gesteld of de inhoud van door Cloudaanbieders gehanteerde voorwaarden door kleinzakelijke gebruikers daadwerkelijk als een drempel wordt gezien om Cloud Computing diensten af te nemen. Dit mede nu de grotere en meer bekende Cloudaanbieders vanwege hun gunstige prijsstelling ook in deze afzetmarkt al een positie van betekenis hebben verworven. In dit verband kan er voorts nog op worden gewezen dat ook de eenzijdige voorwaarden van de aanbieders van bijvoorbeeld software voor kantoorautomatisering geen drempel zijn gebleken voor het opbouwen van een - zelfs zeer sterke - marktpositie.

4.4 Continuïteit

Door organisaties, zowel in de overheid- als in de marktsector, wordt een continue beschikbaarheid van IT-voorzieningen terecht beschouwd als een kritische factor. De Nederlandse wet- en regelgeving kent geen specifieke normstelling voor (het waarborgen van) de continuïteit van het gebruik van IT-voorzieningen. Dit zowel aan aanbiederszijde als aan afnemerszijde.
Wel bestaan er specifieke voorzieningen voor het waarborgen van de continuïteit van IT-voorzieningen in bijzondere omstandigheden. Hierbij is het echter aan de betrokken aanbieders zelf om in onderling overleg invulling te geven aan de noodzakelijk geachte waarborgen.

NCO-T EN ANDERE TELECOM-CONTINUÏTEITSVOORZIENINGEN

Een voorbeeld is het Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T) van aanbieders van openbare telecommunicatienetwerken, openbare telecommunicatiediensten en huurlijnen, ingesteld uit hoofde van artikel 14.6 van de Telecommunicatiewet, om de continuïteit van elektronisch transport van gegevens over openbare telecommunicatienetwerken en huurlijnen te waarborgen indien zich een buitengewone omstandigheid voor doet (in de spreektaal veelal aangeduid als noodtoestand). Lidmaatschap van het NCO-T is verplicht, deelname niet. Echter, in het NCO-T gemaakte afspraken gelden voor iedere aangewezen aanbieder. In bijlage D is een korte samenvatting van de achtergrond en het doel van het NCO-T opgenomen.

Ook het uit het NCO-T voortgekomen Telecom-ISAC (Telecom Information Sharing and Analysis Center) kan in dit verband worden genoemd. Hierin werken deelnemers samen met enkele overheidsorganisaties voor het uitwisselen van informatie over incidenten, dreigingen, kwetsbaarheden en good practices in de telecommunicatiebranche.

Naast deze meer op branchesamenwerking gerichte continuïteitsvoorzieningen in de telecomsector, wordt op korte termijn ook nadere regelgeving verwacht met betrekking tot de op individuele aanbieders van openbare elektronische communicatienetwerken en -diensten gerichte technische en organisatorische maatregelen en eisen, meld- en informatieplichten en aanwijzingen. Dit alles ter waarborging van de continuïteit van bedoelde openbare elektronische communicatienetwerken en -diensten. Deze in een "Besluit continuïteit openbare elektronische communicatienetwerken en -diensten" vast te leggen maatregelen, eisen, plichten en aanwijzingen vinden hun grondslag in twee nieuwe artikelen in de Telecommunicatiewet (artikelen 11a.1 en 11a.2).

Volgens de Nota van Inlichtingen bij de consultatieversie van het voorgesteld Besluit van oktober 2011 is de verwachting dat de meeste aanbieders op eenvoudige wijze aan deze nieuwe verplichtingen zullen kunnen voldoen. Dit omdat zij in het kader van hun dagelijkse bedrijfsvoering en om een serieuze rol op de markt voor elektronische communicatie te kunnen spelen, er uiteraard zelf alle belang bij hebben om te zorgen voor continuïteit van hun netwerken en diensten en daartoe al de nodige maatregelen hebben getroffen. Voorts zouden de administratieve lasten en de bedrijfseffecten van de nieuwe verplichtingen beperkt blijven. De praktijk zal uitwijzen of de verplichtingen van deze nieuwe regelgeving al of niet een negatief effect zullen hebben op de aanbodzijde op de Cloud Computing markt (zowel ten aanzien van bestaande aanbieders als ten aanzien van potentiële markttoetreders).

WAARBORGING DOOR CONTRACT

Specifieke voorzieningen zoals het NCO-T en de Telecom-ISAC (en de voorzieningen uit hoofde van het Besluit continuïteit openbare elektronische communicatienetwerken en -diensten) zien echter op specifieke situaties en bieden daardoor lang niet altijd uitkomst. Continuïteitswaarborgen dienen naar huidig recht in eerste instantie dan ook te worden gerealiseerd in de contractuele voorwaarden welke tussen de gebruiker en aanbieder van Clouddiensten worden overeengekomen. Zoals gebruikelijk bij vergelijkbare contracten voor IT-dienstverlening vormen zogenaamde *Service Level Agreements* (SLA) een belangrijk instrument voor het vastleggen van de operationele afspraken over de kwaliteit van de dienstverlening tussen partijen. Gegeven het karakter van Cloud Computing (sterk gestandaardiseerde dienstverlening) zal de inhoud van een dergelijke SLA voor het overgrote deel van de gebruikersgroep gelijk (moeten) zijn. Hoewel de aanbieders van Clouddiensten, voor zover wij dat kunnen overzien, in toenemende mate bereid zijn om (hardere) waarborgen voor de continuïteit en kwaliteit van de dienstverlening af te geven, lijken de thans voorliggende service levels in veel gevallen nog tot aarzelingen aan de zijde van de beoogde afnemers te leiden. Een belangrijke de vraag is in hoeverre een dergelijke opstelling van de eindgebruikers zich door de feiten laat onderbouwen. Bij het analyseren van de mogelijkheden en risico's van Cloud Computing lijken veel eindgebruikers te willen streven naar een 100% betrouwbaarheid. Het is inherent aan de toegepaste technologie en daarbij bestaande afhankelijkheden dat dit in de praktijk niet te realiseren is. Voorts voldoet ook de huidige "*klassieke*" IT-dienstverlening niet aan dit criterium. Hier ligt met name een

communicatieprobleem, en geen typische juridische blokkade voor het verder ontwikkelen van Cloud Computing.[13]

BEDRIJFSPROCESSEN EN OVERSTAPMOGELIJKHEDEN

Naast continuïteit van de Clouddienstverlening als zodanig is een andere belangrijke dimensie het waarborgen van continuïteit van bedrijfsprocessen bij beëindiging van een Clouddienst. Dit ziet met name op het risico van een 'lock-in' of anderszins 'keuzebeperking' bij het overstappen op een alternatieve Clouddienst, of het overstappen naar 'eigen beheer' van de IT-voorziening, als gevolg van de toegepaste technologie of een gebrekkige toegang tot eigen data. In de rechtspraak zijn inmiddels enkele uitspraken voorhanden waaruit geconcludeerd kan worden dat scheidende aanbieders zich in beginsel coöperatief moeten opstellen om medewerking te verlenen aan de overgang, en dat de wensen van de gebruiker daarbij maatgevend zijn[14]. Dit ziet met name op activiteiten in het kader van dataverstrekking, al dan niet gecombineerd met dataconversie. Kern daarbij is steeds "eerst medewerking verlenen en daarna pas discussiëren over kosten". Een kanttekening is wel dat in bedoelde geschillen veelal sprake was van een overeengekomen exit-clausule op basis waarvan de aanbieder zich in beginsel had verplicht medewerking te verlenen om de continuïteit van de gebruiker te waarborgen. Aanbieders lijken echter in toenemende mate bereid een dergelijke algemene verplichting aan te gaan - al dan niet beperkt tot datacontinuïteit en al dan niet tegen vergoeding - waardoor dit niet langer een typisch juridische drempel lijkt naar verder gebruik van Cloud Computing. Door het stimuleren van gebruik van open datastandaarden, of anderszins algemeen beschikbare en gehanteerde bestandtypes, zou een nadere slag gemaakt kunnen worden. Ook initiatieven ter bevordering van interoperabiliteit en portabiliteit van Cloud oplossingen[15] verdienen in dit kader bijzondere aandacht.

INSOLVENTIE

Bijzondere aandacht verdient nog de situatie van insolventie aan aanbieders- dan wel aan afnemerszijde. Voor de gebruikerszijde geldt dat op dit moment geen bijzondere wettelijke voorziening bestaat gericht op verplichte voortgezette levering van de Clouddienst bij (dreigende) insolventie van de afnemer, zoals die wel bestaat voor voortgezette levering van gas, water elektriciteit of verwarming (art. 37b en 237b Faillissementswet). In een rechtszaak uit 2009 bevestigde de rechter dat de leverancier van een Clouddienst moest blijven leveren hoewel de afnemer intussen in surseance verkeerde. [R-23] Daarom kan op dit moment het ontbreken van een dergelijke bijzondere voorziening ons inziens niet als een werkelijk blokkerende factor worden beschouwd voor (de perceptie van) continuïteit van het gebruik van Cloud Computing.

---

[13] Zie voor het belang van een adequate sourcingstrategie bijvoorbeeld JR Raphael, The 10 worst cloud outages (and what we can learn from them), Infoworld, 27 juni 2011 (http://www.infoworld.com/d/cloud-computing/the-10-worst-cloud-outages-and-what-we-can-learn-them-902).

[14] Zie bijvoorbeeld Vzr. Rechtbank Amsterdam 15 februari 2010, KG ZA 10-193 NB/RV, LJN: BL4068, CR 2010/106 (Insinger de Beaufort/Centric); Vzr. Rechtbank Amsterdam 9 januari 2009, KG ZA 09-25 SP/EB (Telfort/XB Managed Services)

[15] Zie bijvoorbeeld het Open Cloud Manifesto, www.opencloudmanifesto.org.

Wel is het gerechtvaardigd om de vraag op te werpen of niet zou moeten worden gestreefd naar het aanbrengen van een dergelijke specifieke voorziening voor internettoegang en Internet gebaseerde dienstverlening, waaronder Cloud Computing.

In geval van (dreigende) insolventie aan aanbiederszijde zijn weinig voorzieningen beschikbaar om de continuïteit van de Clouddienstverlening voor de gebruiker te waarborgen. Voor zover in de traditionele situatie de IT-omgeving in eigen huis aanwezig was, bleef in het geval van een faillissement van de leverancier die omgeving vaak nog wel tenminste enige tijd beschikbaar. Eventueel werd zelfs de broncode veiliggesteld worden door middel van een escrowregeling[16]. Dit ligt anders in het geval van Clouddiensten. Een faillissement van de aanbieder of het om een andere reden stopzetten van een Clouddienst betekent dat per direct de IT-omgeving en de daarin opgeslagen gegevens niet meer beschikbaar zijn, met alle gevolgen van dien voor de bedrijfsvoering van de afnemer.

In beginsel is het aan de curator/bewindvoerder om in het belang van de schuldeisers te beslissen of voortzetting van de Clouddienstverlening opportuun is. Dit risico is echter niet veel anders dan bij de huidige "*klassieke*" IT-outsourcing. Ons inziens ligt hier dan ook geen typische juridische blokkade voor het verder ontwikkelen van Cloud Computing. Geen enkele IT-voorziening of -dienst is 100% betrouwbaar. Evenmin is de continuïteit van elke IT-aanbieder voor 100% gegarandeerd. Het is in beginsel aan de afnemers om bij de ontwikkeling van een IT-strategie rekening te houden met dergelijke externe factoren en afhankelijkheden. Wel zou het ministerie kunnen overwegen om vergelijkbaar met het NCO-T of Telecom-ISAC marktpartijen te stimuleren om maatregelen te treffen ter voorbereiding van gecontinueerde internetgebaseerde dienstverlening, waaronder Cloud Computing, in buitengewone omstandigheden zoals (dreigende) insolventie van een majeure marktpartij. Bijvoorbeeld een Cloud- of XaaS-ISAC.

4.5 Aansprakelijkheid

Zoals opgemerkt zijn op dit moment organisaties zowel in de overheidssector als in de marktsector in vrijwel alle gevallen voor hun continue functioneren voor vrijwel 100% afhankelijk van de ongestoorde beschikbaarheid van kwalitatief goede IT-voorzieningen. De overstap naar Cloud Computing brengt daarin ons inziens op zich geen verandering. Naarmate er bij één aanbieder meer Clouddiensten worden afgenomen, wordt de afhankelijkheid van deze ene aanbieder uiteraard wel groter. Of daarmee ook de risico's groter worden, is afhankelijk van vele factoren, en anders dan in veel gevallen gepercipieerd, geen gegeven. Vergelijk ook onze eerdere opmerkingen over de risicobeleving van (potentiële) gebruikers van Clouddiensten.

BEPERKING VAN AANSPRAKELIJKHEID WEINIG ANDERS DAN BIJ ANDERE IT-DIENSTEN

Strikt juridisch gesproken vormt de aansprakelijkheid voor eventuele aan de inzet van Cloud Computing gerelateerde schade naar ons oordeel geen belemmering voor de uitrol van deze

[16] Wiki: Escrow is een overeenkomst waarbij een software leverancier of distributeur en gebruiker overeenkomen dat de leverancier de broncode van een software product ten behoeve van de gebruiker deponeert bij een gespecialiseerd escrow agent. De broncode wordt aan de gebruiker overgedragen op het moment dat aan bepaalde voorwaarden wordt voldaan.

diensten. In de meeste gevallen zal het juridische kader primair worden gevormd door de contractuele relatie tussen de afnemer en de aanbieder, met in specifieke gevallen (bijvoorbeeld datalekken) aanvullende toepasselijke wet- en regelgeving, zoals privacywetgeving, strafrechtelijke regels etc. Contracten op grond waarvan Clouddiensten worden aangeboden, kennen veelal een vergaande beperking van aansprakelijkheid. Mede door de sterke afhankelijkheid van telecommunicatie-infrastructuren, tekenen aanbieders van Clouddiensten zich in veel gevallen nog verder vrij dan geldt voor andere aanbieders van IT-diensten. De ervaring met meer klassieke vormen van het afnemen van IT-diensten heeft geleerd dat de risico's verbonden aan IT nimmer volledig op een aanbieder kunnen worden afgewenteld; IT kent naar de aard steeds een hoog 'eigen risico'. Bij het afnemen van Clouddiensten is dit niet anders.

Daarbij moet bovendien in ogenschouw worden genomen dat de lage kosten die in rekening worden gebracht voor Clouddiensten ook uiteraard zijn weerslag hebben op het risicoprofiel dat de aanbieder kan accepteren. Bovendien stelt de cumulatie van risico's (veel gebruikers op dezelfde infrastructuur) uiteraard een beperking aan de mogelijkheden van risicoacceptatie door de aanbieders.

Vooralsnog beschouwen wij de sterke beperkingen van aansprakelijkheid in de voorwaarden waaronder Clouddiensten worden aangeboden wel als een relevante factor maar niet primair blokkerend (dan wel sterk) belemmerend voor de ontwikkeling van Clouddiensten. Zie in dit verband ook de eerdere opmerkingen over de bescherming van met name consumenten en in minder mate kleinzakelijke gebruikers tegen onredelijk bezwarende voorwaarden van (in geval van kleinzakelijke gebruikers: Nederlandse) Cloudaanbieders. De discussie is overigens ook niet anders dan bij het afnemen van meer klassieke IT-voorzieningen zoals standaardprogrammatuur op het gebied van kantoorautomatisering (bijv. tekstverwerking en documentopslag). Ook daar is sprake van enkele grote buitenlandse aanbieders die hun aansprakelijkheid voor risico's verbonden aan gebruik van hun programmatuur vergaand hebben beperkt. En gezien de marktpositie van bedoelde aanbieders op bedoelde 'productmarkt', beschouwen vele afnemers deze voor hen nadelige verdeling van verantwoordelijkheden kennelijk niet als een belemmering om toch in zee te gaan met dergelijke aanbieders.

AANSPRAKELIJKHEID VAN INTERNETDIENSTVERLENERS

Naast eventuele aansprakelijkheid binnen de contractuele verhouding tussen de Cloudaanbieder en de afnemer, is ook relevant dat de Cloudaanbieder door middel van levering van de Clouddienst in opdracht van de afnemer informatie/content (niet zijnde persoonsgegevens) doorgeeft of opslaat, en op die informatie/content (eigendoms)rechten van derden rusten.
De aansprakelijkheidspositie van de afnemer in dergelijke situaties laten wij hier verder buiten beschouwing, aangezien deze niet specifiek is voor Clouddiensten. De positie van de Cloudaanbieder, die als intermediair een rol speelt in het ontstaan en voortbestaan van de betreffende onrechtmatige situatie (inbreuk op rechten van derden), verdient wel nadere aandacht.

Een Cloudaanbieder kwalificeert in beginsel als een aanbieder van een dienst van de informatiemaatschappij (zie artikel 15d lid 3 van Boek 3 BW). Bij bepaalde Clouddiensten

(bijvoorbeeld mail uit de cloud) zal deze kunnen bestaan uit het doorgeven van informatie van de afnemer. Deze gevallen zullen in de praktijk beperkt zijn. Meer gebruikelijk is dat de Clouddienst mede bestaat uit het op verzoek opslaan van informatie van de afnemer. Bij veel Clouddiensten zal dit het geval zijn. Het probleem ontstaat indien de afnemer de Cloudaanbieder verzoekt informatie door te geven of op te slaan, terwijl een derde-rechthebbende ten aanzien van die informatie daarvoor geen toestemming heeft gegeven. Aanbieders zullen het zeker als belemmerend beschouwen om Clouddiensten aan te bieden, indien dit aansprakelijkheid jegens derden kan meebrengen voor de doorgegeven c.q. opgeslagen informatie.

Artikel 196c van Boek 6 BW, een resultante van de implementatie van de E-commerce Richtlijn, bevat enkele specifieke gevallen waarin internetdienstverleners (zoals Cloudaanbieders) gevrijwaard zijn van bedoelde aansprakelijkheid jegens derden. De vrijwaring van aansprakelijkheid voor doorgegeven informatie (lid 1) laat zich vrij eenvoudig toepassen. De vrijwaring van aansprakelijkheid voor opgeslagen informatie (lid 4) ligt meer complex.

Om op de vrijwaring van aansprakelijkheid voor opgeslagen informatie een beroep te kunnen doen, is het van belang dat de Clouddienst beperkt is tot een activiteit met een "louter technisch, automatisch en passief karakter". Dit houdt in dat de Cloudaanbieder "noch kennis noch controle" mag hebben (gehad) over de opgeslagen informatie. Uit recente jurisprudentie van het Hof van Justitie van de Europese Unie[17] blijkt dat onder meer geen beroep op de vrijwaring kan worden gedaan, indien de aanbieder "kennis heeft gehad van feiten of omstandigheden op grond waarvan een behoedzame marktdeelnemer de onwettigheid van de betrokken [informatie] had moeten vaststellen" (kennis), of indien de aanbieder "bijstand verleent die onder meer bestaat in het optimaliseren van de wijze waarop de betrokken [informatie] wordt getoond of het bevorderen daarvan" (controle). Het zal van de Clouddienst afhangen of de Cloudaanbieder op dit punt een verhoogd risico loopt dat hij geen beroep kan doen op de wettelijke vrijwaringen van aansprakelijkheid, hetgeen overigens niet betekent dat de Cloudaanbieder dan zonder meer aansprakelijk is voor de betreffende informatie.

Indien de Cloudaanbieder, gezien de aard van de Clouddienst, in beginsel wel een beroep kan doen op de vrijwaring van aansprakelijkheid voor opgeslagen informatie, is van belang dat hij niet weet, noch redelijkerwijs behoort te weten, van de activiteit of informatie met een onrechtmatig karakter, en dat zodra hij dat wel weet of redelijkerwijs behoort te weten, hij prompt de informatie verwijdert of de toegang daartoe onmogelijk maakt. In dit kader kan de Cloudaanbieder ook worden geconfronteerd met aanvullende bevelen, zoals het opschorten van de Clouddienst jegens de betreffende afnemer en het bekendmaken van de identiteit van de afnemer. Met name de norm "redelijkerwijs behoort te weten" zou bij Cloudaanbieders vragen kunnen oproepen. Hierbij dient te worden onderkend, dat voor aanbieders geen algemene surveillance-, filtering- en/of monitoringverplichting geldt.

Voor wat betreft aansprakelijkheid kan als mogelijk belemmerende factor voorts nog worden gewezen op de 'angst' van partijen voor de verschillen in lokale wetgeving, zowel in de EU als

[17] HvJ EG 12 juli 2011, C-324/09 (L'Oréal/eBay).

daarbuiten. Voor wat de EU betreft geldt dat ook na pogingen tot harmonisatie op Europees niveau er nog vele verschillen blijken te bestaan in de lokale uitwerking door de lidstaten. Dit laat zich met name voelen op het vraagstuk van de verdeling van verantwoordelijkheden en risico's. Kan een aanbieder er op vertrouwen dat hij in een andere jurisdictie dezelfde wettelijke bescherming geniet als in zijn eigen jurisdictie? Wat is de invloed van buitenlands recht op het risicoprofiel en de doorvertaling daarvan naar kosten, voorwaarden etc. Diensten van de informatiemaatschappij, zoals Clouddiensten, blijken toch steeds meer en meer onverenigbaar met territoriale grenzen binnen het recht. In dit verband kan het streven van de EU naar een 'digital single market' [R-24] alleen maar worden toegejuicht. Dit zou een 'boost' kunnen geven aan de verdere economische ontwikkeling binnen de EU. Zaak is dan wel om te stimuleren dat de reikwijdte van de 'digital single market' zo breed mogelijk is en alle internet-gerelateerde dienstverlening omvat (waaronder Clouddiensten).

4.6 Toegangsrechten overheidsinstanties

In Nederland is veel (Europese) wet- en regelgeving van toepassing is waarin onder (bijzondere) omstandigheden overheidsdiensten toegang kunnen krijgen tot bij bedrijven opgeslagen gegevens. Een belangrijke hierna te bespreken regeling op dit punt is de Telecommunicatiewet. Ook dienen Nederlandse bedrijven die met Amerikaanse bedrijven zaken doen rekening te houden met de te bespreken Amerikaanse USA PATRIOT Act, die toegangsrechten verleent aan Amerikaanse overheidsinstanties. Daarnaast is er een meer algemene discussie over toegangsrechten van overheidsinstanties, ook op internationaal niveau.

TELECOMMUNICATIEWET

Vanuit aanbiederszijde bestaat veel onduidelijkheid over de toepasselijkheid van de Telecommunicatiewet op Clouddiensten, met name vanwege de ruime begripsomschrijvingen van kernbegrippen als ‘openbaar elektronisch communicatienetwerk of -dienst’ c.q. ‘openbaar telecommunicatienetwerk of -dienst’. Toepasselijkheid van deze wetgeving wordt wel als belemmering gezien voor totstandkoming van innovatieve diensten als Cloud Computing. Dit houdt hoofdzakelijk verband met de verplichtingen uit hoofdstuk 13 van de Telecommunicatiewet inzake aftapbaarheid van het netwerk of de dienst en andere opsporings- en nationale veiligheidsbevoegdheden in dit verband (waaronder de bewaarplicht ten aanzien van verkeersgegevens). Het voldoen aan bedoelde verplichtingen kan gemoeid gaan met substantiële investeringen die slechts deels door de bevoegde autoriteiten worden vergoed.
Kernpunt in deze discussie is dat er sprake moet zijn van:

a) ofwel een transmissiesysteem dat het mogelijk maakt om signalen over te brengen, en voor de toepasselijkheid van hoofdstuk 13 Tw dan uitsluitend signalen ten behoeve van communicatie tussen netwerkaansluitpunten;
b) ofwel een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen, en voor de toepasselijkheid van hoofdstuk 13 Tw dan uitsluitend communicatiesignalen.

De onder a) bedoelde transmissiesystemen zullen Cloudaanbieders over het algemeen niet zelf aanbieden (deze worden beheerd door wat ook wel de Cloudinfrastructuur aanbieders worden

genoemd), waardoor deze verder buiten beschouwing kunnen blijven. De onder b) bedoelde diensten komen op de Cloud menukaart ook slechts in beperkte mate voor, namelijk slechts daar waar de Clouddienst ziet op het overbrengen van signalen (in andere woorden: daar waar de Clouddienst aanbieder tevens kwalificeert als communicatiedienst aanbieder). Clouddiensten die primair betrekking hebben op opslag of bewerking van gegevens vallen hier niet onder. Zodoende lijken thans alleen communicatiediensten uit de Cloud zoals webmail onder de reikwijdte van de Telecommunicatiewet te vallen. Het Agentschap Telecom pleegt hiervoor ook wel het gebruik van een domein als 'vuistregel' te hanteren. Daar waar de webmail onder het domein van de aanbieder wordt aangeboden, is er sprake van een communicatiedienst, en daar waar de webmail onder het domein van de klant wordt aangeboden, is er geen sprake van een communicatiedienst (en dus enkel 'kale' mailhosting).
Voor de toepasselijkheid van hoofdstuk 13 Tw is voorts nog relevant of er sprake is van een openbare dienst, oftewel: een voor het publiek beschikbare dienst. Alleen openbare diensten vallen onder de reikwijdte. Dit is het geval indien de dienst in principe voor iedereen beschikbaar is (waaronder groepen waarvan nagenoeg iedereen lid kan worden). Besloten diensten, zoals diensten die niet toegankelijk zijn voor anderen dan werknemers van een bepaald bedrijf, vallen er in beginsel buiten.

CONCLUSIE TELECOMMUNICATIEWET

Recapitulerend betekent dit dat Cloudaanbieders slechts te maken hebben met toepasselijkheid van de Telecommunicatiewet, in het bijzonder hoofdstuk 13 daarvan, indien zij een Clouddienst aanbieden die geheel of hoofdzakelijk bestaat uit een communicatiedienst (zoals e-mailfunctionaliteit) die voor een ieder beschikbaar is. Het aanbieden van hostingdiensten voor communicatieberichten (zoals mailhosting) valt daarentegen buiten de reikwijdte van de Telecommunicatiewet, tenzij dit gecombineerd wordt met het aanbieden van de openbare communicatiedienst zelf.
In het kader van de bewaarplicht gegevens telecommunicatie bevat de website van de Rijksoverheid [R-25] een leidraad voor ondernemers om te bepalen of zij onder de reikwijdte van de Telecommunicatiewet, meer in het bijzonder hoofdstuk 13 daarvan, vallen. Onze ervaring leert dat deze leidraad voor Cloudaanbieders echter weinig houvast biedt. Het verder verduidelijken van de leidraad op dit punt zou kunnen bijdragen tot het wegnemen van eventuele belemmeringen voor potentiële Cloudaanbieders om de markt te betreden.

USA PATRIOT ACT

In (juridische) discussies over Cloud Computing wordt vaak ook gewezen op de risico's die verbonden zijn aan de Amerikaanse USA PATRIOT Act. In essentie gaat het daarbij om de mogelijke toegang tot (vertrouwelijke) gegevens door Amerikaanse opsporingsdiensten en andere overheidsorganisaties. Naar onze ervaring geldt ook voor dit aspect dat de perceptie over de aan Cloud Computing verbonden risico's nogal eens relatief eenzijdig wordt ingekleurd. Zonder hier op de details van de (overigens zeer complexe) USA PATRIOT Act in te gaan, is het bij het beschouwen van de daaraan verbonden risico's tenminste van belang vast te stellen dat deze Amerikaanse wetgeving niet alleen ziet op de activiteiten van Amerikaanse bedrijven maar ook van toepassing kan zijn als Europese bedrijven door middel van een Amerikaanse dochteronderneming activiteiten in de VS ontplooien. Deze wetgeving is derhalve niet alleen relevant bij uitbesteding

van IT-activiteiten naar (in Europa gevestigde dochters van) Amerikaanse aanbieders, maar kan mogelijk ook aan de orde komen bij uitbesteding naar Europese aanbieders met een in de Verenigde Staten gevestigde dochteronderneming. Dit vraagstuk inzake de jurisdictie van Amerikaanse opsporingsdiensten en andere overheidsorganisaties is niet nieuw voor Cloud Computing; deze kwestie speelt bijvoorbeeld ook al jaren een rol bij het afnemen van datacenter diensten in Europa van (dochters van) Amerikaanse bedrijven. De Minister van Veiligheid en Justitie heeft de Tweede Kamer nog recent op deze problematiek gewezen [R-26].

In de discussie over de risico's verbonden aan de Amerikaanse regelgeving dient niet uit het oog te worden verloren dat ook op basis van de Nederlandse/Europese wet- en regelgeving er ruime bevoegdheden bestaan voor overheidsdiensten om toegang te krijgen tot door bedrijven opgeslagen gegevens. Die regels zijn in principe ook van toepassing als gegevens in de Cloud zijn ondergebracht.

Tot slot wordt in (juridische) discussies over toepasselijkheid van de USA PATRIOT Act nog wel eens het vraagstuk van de doorgifte van persoonsgegevens buiten de Europese Economische Ruimte (zie hiervoor) opgeworpen. Bij het afnemen van Clouddiensten van met name de grote buitenlandse aanbieders (Google, Microsoft, Amazon, e.d.) lijkt de doorgifte-problematiek echter thans geen groot obstakel te vormen. Genoemde aanbieders hebben zich veelal verplicht tot naleving van de "Safe Harbor Principles", waardoor in het kader van de doorgifte naar de Verenigde Staten een passend beschermingsniveau aanwezig wordt geacht. De aan de "Safe Harbor Principles" ten grondslag liggende "Safe Harbor Agreement" tussen de Europese Commissie en de U.S. Department of Commerce staat expliciet toe dat aan verzoeken van Amerikaanse opsporingsdiensten en andere overheidsorganisaties tot verstrekking van gegevens wordt voldaan.

Transparantie over de daadwerkelijke reikwijdte en werking van de USA PATRIOT Act voor de Cloud Computing markt, afgezet tegen de reikwijdte en werking van vergelijkbare Nederlandse/Europese wet- en regelgeving, kan ons inziens een positieve bijdrage leveren aan de verdere ontwikkeling van Cloud Computing.

TOEGANG IN NEDERLANDS EN INTERNATIONAAL PERSPECTIEF

Dit betreft zowel strafvorderlijke wet- en regelgeving in het bijzonder, als de regelgeving die ziet op de bestrijding van terrorisme. Ook bevat bijvoorbeeld de Nederlandse fiscale wetgeving vergaande mogelijkheden om toegang te krijgen tot gegevensverzamelingen van bedrijven. Zonder de risico's op dit punt te willen bagatelliseren, stellen wij vast dat de voor het voeren van een gebalanceerde discussie hierover, het verbeteren van de informatievoorziening op dit punt een belangrijk element is. Alleen daardoor kan hierover meer duidelijkheid worden gecreëerd. In dat verband zou tevens aandacht besteed kunnen worden aan de risico's verbonden aan het door overheidsinstanties steeds meer vertrouwen op informele samenwerking tussen overheidsdiensten uit de verschillende landen, zoals dit naar verluidt gebeurt onder de noemer van 'verbetering van de effectiviteit van internationale opsporings- en strafvorderingsactiviteiten'. Dit vertrouwen over en weer kan leiden tot een aflatende aandacht aan de grenzen van de te onderscheiden bevoegdheden van bedoelde overheidsdiensten in andere jurisdicties. In de

praktijk zou dit zelfs tot gevolg kunnen hebben dat overheidsdiensten gegevens kunnen opvragen bij en kunnen verkrijgen van Cloudaanbieders gevestigd in een andere jurisdictie, zelfs zonder een medewerkingsverzoek te doen aan de collega-overheidsdienst in de betreffende jurisdictie. [R-27]

5 CLOUD COMPUTING IN EEN EUROPESE CONTEXT

Dit hoofdstuk is opgesteld onder redactie van N. Robinson en J. Cave van het internationale onderzoeksbureau RAND. In dit hoofdstuk wordt met name ingegaan op de Europese context van Cloud Computing.

5.1 De EU Digital Agenda 2009

Het EU Digital Agenda initiatief uit 2009 [R-28] richt zich op de bevordering van economische en sociale voordelen van één enkele digitale markt. Het is de eerste van zeven vlaggenschipinitiatieven van de overkoepelende Europa 2020 strategie. Europa 2020 draait om drie dingen: slimme, duurzame en "inclusieve" groei. De Digital Agenda geeft door kernactiviteiten in zeven gebieden aan hoe Europa de mogelijkheden van IT het best kan benutten. De gebieden zijn: de versnippering van de digitale markten, het gebrek aan interoperabiliteit, de toenemende cybercriminaliteit en het gevaar van een tekort aan vertrouwen in netwerken, het gebrek aan investeringen in netwerken, de ontoereikendheid van de geleverde inspanningen op het vlak van onderzoek en innovatie, het gebrek aan digitale geletterdheid en digitale vaardigheden en de gemiste kansen op het gebied van de aanpak van maatschappelijke problemen.
In de Europese Digitale Agenda is als actie opgenomen dat lidstaten voorzien in voldoende financiële steun voor een EU-strategie voor “wolkwebben” (Cloud Computing), met name ten bate van de overheid en wetenschap [R-6]. Eurocommissaris Kroes heeft diverse keren aangegeven dat zij Europa niet zozeer Cloud-vriendelijk wil maken, maar juist Cloud-actief. Kroes geeft daarbij aan dat Cloud Computing een belangrijke ontwikkeling is voor innovatie en economische groei in Europa [R-7].

5.2 Wettelijke regelingen inzake privacy en gegevensbescherming m.b.t. Cloud Computing

Ook in Europees verband (vanuit de overweging van maatregelen om het gebruik van Cloud Computing te stimuleren) wordt nagedacht over het juridische raamwerk rond privacy en gegevensbescherming. Ervoor zorgen dat Cloudaanbieders en afnemers zich aan de wettelijke verplichtingen met betrekking tot vertrouwelijke gegevens houden is een van de belangrijkste beleidsuitdagingen.

Beleidsmakers op Europees en nationaal niveau worstelen met de vraag hoe houdbaar de bestaande Europese regelgeving is met betrekking tot privacy en gegevensbescherming. Ook op Europees niveau wordt dit aspect beschouwd als een van de belangrijkste oorzaken voor gebrek aan vertrouwen door afnemers. Ten aanzien van de huidige regelgeving wordt op verschillende plaatsen gewezen op belemmeringen in de volgende domeinen: verantwoordelijkheid, locatie, transparantie, omschrijving van verantwoordelijke en bewerker; controle, instemming, privacy by default en privacy by design. Hieronder wordt dit laatste thema nog verder uitgewerkt.

PRIVACY BY DESIGN

Privacy by Design (PbD) kan een uitkomst bieden bij een aantal van de moeilijkheden die Cloud Computing en de regelgeving omtrent privacy en gegevensbescherming met zich meebrengt. Dit werd in 2010 door de Artikel 29 werkgroep naar voren gebracht in hun antwoord op de consultatie

rondom de toekomst van privacy (zie volgende paragraaf). Ook enkele regelgevers, zoals de Canadese Privacy Commissioner, hebben dit geopperd. Probleem is echter dat PbD niet voor iedereen hetzelfde betekent, en het mogelijk bijvoorbeeld innovatie in de weg zou kunnen staan. Vanuit overheidsperspectief betekent dit dat bij het ontwikkelen van regelgeving rondom Cloud Computing en privacy en gegevensbescherming, de beleidsmakers zich moeten afvragen of het noodzakelijk is PbD exact te omschrijven – is het een formele reeks processen die bedrijven eerst moeten doorlopen voordat ze nieuwe producten en diensten kunnen aanbieden (zoals een privacy impact assessment), of een meer technische betekenis die inhoudt dat nieuwe technologieën altijd voorzien moeten zijn van privacy-vriendelijke functionaliteiten. TNO verricht op dit moment onderzoek naar de succes- en faalfactoren van de toepassing van dit beginsel in het ontwerp van systemen. Dit onderzoek is nog niet afgerond.

5.3 De herziening van de Europese regelgeving omtrent privacy en gegevensbescherming

In juli 2009 hield de EC een consultatie over de regelgeving omtrent het fundamentele recht op bescherming van persoonlijke gegevens. Hierin werd speciale aandacht geschonken aan de werking van de bestaande regelgeving in het licht van nieuwe technologische ontwikkelingen, de globalisering en de structurele veranderingen in de EU sinds het van kracht zijn van het verdrag van Lissabon in 2009. In de hierbij behorende stukken werd ook verwezen naar Cloud Computing. De werkgroep Article 29 en de werkgroep Policy & Justice stelden een antwoord op naar aanleiding van de consultatie: "The Future of Privacy – Joint contribution to the Consultation of the European Commission on the Legal framework for the fundamental right to protection of personal data" [R-29]. Het antwoord op de consultatie geeft de volgende vier aspecten in overweging:

- Verduidelijk de toepassing van een aantal hoofdregels en –beginselen van gegevensbescherming (zoals toestemming en transparantie).
- Verbeter de regelgeving door de invoering van additionele beginselen (bijvoorbeeld ‘privacy by design’ en 'accountability').
- Verbeter de effectiviteit van het systeem door modernisering van afspraken in Directive 95/46/EC (bijvoorbeeld door de bureaucratische last te verlichten).
- Breng de fundamentele beginselen van gegevensbescherming onder in één juridisch raamwerk, dat ook van toepassing is op politie en justitiële samenwerking in criminele zaken.

Op 25 januari 2012 heeft de Europese Commissie een voorstel voor een verordening (COM(2012)11) voorgesteld om de EU-gegevensbeschermingsregels van 1995 te hervormen. [RIn de nieuwe Privacyverordening wordt duidelijke hoe het huidige juridische raamwerk zich in grote lijnen ontwikkelt. De noodzaak tot een uniforme EU benadering van Cloud Computing om de voordelen zoals efficiëntie, innovatiesnelheid en kostenbesparing te bewerkstelligen, wordt erkend. Ook werd de complexiteit van Cloud Computing in relatie tot de huidige wet- en regelgeving omtrent de bescherming van persoonsgegevens onderkend. Cloud Computing leidt tot het distributie van persoonsgegevens naar een groot aantal bestemmingen.
Eén van de mogelijkheden is volgens Reding de ontwikkeling op EU niveau van Cloud Computing centra die voldoen aan de EU regels met betrekking tot privacy en gegevensbescherming. Hierbij zou gebruik gemaakt kunnen worden van al bestaande aanbieders van EU-gebaseerde Clouddiensten.

Voorgesteld wordt om de Europese Privacyrichtlijn uit 1995 te vervangen door een verordening. Dit heeft als voordeel dat de regeling rechtstreeks werking krijgt in de EU en er geen implementatievoorstellen meer nodig zijn. Dit betekent vanzelfsprekend harmonisatie. Verder beoogt de verordening de export van gegevens naar landen buiten de EU te vereenvoudigen. Wel moeten eerst alle EU-lidstaten en het Europarlement akkoord gaan, zodat het nog wel 2 of 3 jaar kan duren voordat de verordening van kracht is.
Belangrijkste kenmerken van deze verordening zijn:

- De verordening zal van toepassing zijn voor alle verantwoordelijken van de verwerking en verwerkers die een vestiging hebben in de EU, ongeacht of het verwerken van de gegevens op zich in de EU plaats vindt of niet.
- Als bedrijven van buiten de EU activiteiten rechtstreeks richten op burgers binnen de EU, dan moeten zij zich houden aan de nieuwe EU regelgeving omtrent gegevensbescherming (EU data protection rules);
- Stroomlijnen en versterken van de regels inzake toepasselijkheid en het vereenvoudigen en verbeteren van de procedures voor doorgifte van gegevens buiten de EEA. Het is niet langer nodig om in elke lidstaat melding te doen van elke verwerking van persoonsgegevens.
- Verduidelijking van het begrip 'toestemming'.
- Organisaties zullen slechts onderworpen zijn aan één privacy autoriteit, namelijk diegene van het land waar hun hoofdzetel gevestigd is.
- Een meldplicht voor datalekken waarbij binnen 24 de autoriteiten en de betrokkene moeten worden geïnformeerd op straffe van hoge boetes.
- Het verplicht aanstellen van een "Data Protection Officer" in entiteiten met meer dan 250 medewerkers.
- 'Privacy by default' – de inspanning die consumenten moeten verrichten om hun privacy voorkeuren in te stellen dient verminderd te worden, met name daar waar een individu geconfronteerd wordt met oneerlijke, onverwachte of onredelijke verwerking van gegevens. Om persoonsgegevens te verzamelen, zal dus expliciet toestemming van betrokkene nodig zijn.
- Transparantie en minimalisatie– een fundamentele voorwaarde waarbij individuen geïnformeerd dienen te worden welke gegevens worden verzameld en voor welke doeleinden. Gegevens mogen niet langer opgeslagen worden dan nodig is, waarbij gebruikers moeten worden geïnformeerd over de duur van de opslag. Daarnaast mogen bedrijven en overheden niet meer gevegens verwerken dan strikt noodzakelijk voor de dienstverlening.
- Het recht vergeten te worden ("Right to be forgotten") – een recht op grond waarvan individuen onder omstandigheden kunnen afdwingen dat hun gegevens worden verwijderd, bijvoorbeeld indien deze gegevens niet meer nodig zijn voor de verzameldoeleinden, of bij intrekking van een eventueel verleende toestemming.
- Controle over eigen data - De betrokkene heeft recht op toegang tot de gegevens, kopie, verbetering en het recht om zijn gegevens over te dragen van de ene naar een andere dienstverlener (bijvoorbeeld van het ene sociale netwerk naar het andere).

Op diverse plaatsen is naar aanleiding van de voorgestelde verordening een discussie ontstaan of de maatregelen niet te ver gaan en innovatie in de weg staan. Bovendien wordt de problematiek rondom de toegang tot data door opsporingsdiensten en andere overheidsorganisaties van buiten volgens sommigen onvoldoende opgelost. Het CBP heeft bij monde van haar voorzitter, Kohnstamm, aangegeven dat de verordening een goede basis vormt voor de komende besprekingen in de Raad van Ministers en het Europees Parlement.
Rondom de publicatie van het ontwerp werd ook aangekondigd dat de Europese Commissie de komende maanden nog zal terugkomen op de werking van de Safe Harbor Agreement. (R-XX http://www.theregister.co.uk/2012/01/27/microsoft_cpdp_data_protection_planned_eu_reform/

5.4 De positie van Nederland in Europa

Nederland is een van de koplopers op het gebied van infrastructuur als gebruik van IT in Europa. En ook de Nederlandse economie is een van de meest IT-intensieve van Europa. Eén van de belangrijkste sterktes van Nederland op het gebied van IT is zonder meer de aanwezige infrastructuur. Ons land is, dankzij uitstekende binnenlandse netwerken en internationale verbindingen (AMS-IX), nu al de Digital Gateway to Europe op niveau van het fysieke netwerk. Maar ook de fiscale mogelijkheden die Nederland biedt (belastingverdragen) kan aanleiding voor organisaties om zicht hier te vestigen. Google en Facebook zouden om belastingtechnische redenen kantoren in Nederland hebben opgezet. Daarnaast is Nederland aantrekkelijk vanwege de hier aanwezige hoogopgeleide arbeidskrachten.
Vanuit die positie ligger er duidelijk kansen voor Nederland om bijvoorbeeld met sectorspecifieke systeemplatformen, gericht op afnemers binnen Europa, de positie uit te bouwen.
De zorgen rondom toegang tot data opgeslagen in de Cloud, door opsporingsdiensten en andere overheidsorganisaties van buiten Europa (zie de discussie rondom de USA PATRIOT ACT in Hoofdstuk 4) bieden ook een kans. Aanbieders van Clouddiensten die gevestigd zijn in Nederland en de opslag ook binnen Nederland houden, kunnen dat feit gebruiken in hun positionering naar afnemers in Europa.
Alhoewel de juridische "speelruimte" binnen de Europese context beperkt is, zou het Nederlandse beleid erop gericht kunnen zijn dat het Nederlandse (regelgevings)klimaat toonaangevend wordt in Europa en in de wereld, bijvoorbeeld op het vlak van privacybescherming .

5.5 Conclusies

Om een aantrekkelijk klimaat voor Cloud Computing in Nederland te creëren dient rekening gehouden te worden met een aantal complexe uitdagingen met betrekking tot privacy en gegevensbeveiliging in de Cloud. Hiervoor is de betrokkenheid van meerdere belanghebbenden noodzakelijk, evenals nauwe afstemming met beleidsontwikkelingen op Europees niveau.

In het licht van de op export gebaseerde Nederlandse economie zou het verstandig zijn nadruk te leggen op hoe bepaalde EU regels impact zouden hebben op economische initiatieven om Nederland te promoten als een voorkeurslocatie voor Clouddiensten. Hierbij dient ongetwijfeld een balans gevonden te worden gelet op de gegevensbescherming en privacy debatten op EU niveau. Een voorbeeld van deze balans is de promotie van Nederland als vestigingslocatie voor

Cloudaanbieders vanwege de aanwezig goede infrastructuur enerzijds en de op EU-normen gebaseerde wet- en regelgeving (met name gegevensbescherming) anderzijds. Hierop kan worden ingehaakt door Nederland als voorkeursland te promoten vanwege de aantrekkelijke wetgeving voor export, passende infrastructuur en hoogopgeleide arbeidskrachten. Dit kan ook andere voordelen hebben, bijvoorbeeld het ontwikkelen van certificeringprogramma's (zoals het EuroCloud initiatief [R-31]), die van invloed zijn op de strijd om welk land de beste regelgeving en ondersteunende technologische infrastructuur biedt.

DEEL III:
BELEMMERINGEN EN AANBEVELINGEN

6 BELEMMERINGEN

Dit hoofdstuk beschrijft een aantal van de grootste dan wel meest gehoorde belemmeringen bij het aanbieden en/of afnemen van Clouddiensten. In bijlage E is een totaaloverzicht opgenomen van "alle" mogelijke belemmeringen die uit de literatuurstudie en interviews naar voren zijn gekomen. Dit totaaloverzicht is in dit hoofdstuk samengevat tot een verkorte lijst met de belangrijkste belemmeringen. Hierbij is onder meer gekeken of een belemmering werkelijk nieuw is, met andere woorden is dit probleem werkelijk door Cloud Computing geïntroduceerd of bestond het wellicht al in de één of andere vorm. Voor sommige belemmeringen geldt dat deze ook al in meer of mindere mate bestaan bij een meer traditionele inzet van IT-middelen, echter dat door de aard van Cloud Computing deze belemmering een veel groter probleem wordt. Hiermee is rekening gehouden bij het samenvatten van de belemmeringen.

Voorbeelden van belemmeringen die in het totaaloverzicht in bijlage E staan, maar niet (expliciet) zijn opgenomen in de samenvatting in dit hoofdstuk zijn:

- Gebrek aan standaarden voor interoperabiliteit tussen Clouddiensten onderling;
- Belemmeringen met betrekking tot de migratie van legacy IT-omgeving naar Clouddiensten (deze verschillen in het algemeen per organisatie);
- Onvoldoende tooling en kennis bij organisaties voor gebruik van PaaS-diensten;
- Bestaande licentie(structuur) staat migratie naar de Cloud in de weg;
- Snelheid van uitrol van FTTH belemmert de ontwikkeling van Clouddiensten.

Voor een beschrijving van deze belemmeringen wordt verwezen naar bijlage E.

Dit hoofdstuk beschrijft de samenvatting van de belemmeringen, verdeeld in vijf clusters:

1. Compliance / Privacy
2. Informatiebeveiliging en controle
3. Business Continuïteit
4. Markt, aanbod & business case
5. Overig (waaronder Integratie, standaarden en netwerkinfrastructuur)

Niet alle belemmeringen gelden voor alle (type) Clouddiensten. SaaS-, PaaS- en IaaS-diensten hebben elk hun eigen kenmerken en belemmeringen. Een belemmering kan dan ook niet zonder meer veralgemeniseerd worden, bijvoorbeeld "bij Clouddiensten weet je niet in welk land je gegevens staan"; er zijn (met name IaaS-) Clouddiensten die wel degelijk inzicht gegeven in de locatie waar de gegevens worden opgeslagen en verwerkt.
Daarnaast is het onderscheid tussen kleine en middelgrote afnemers van grote invloed op de mate van belemmering. Een grote afnemer van Clouddiensten beschikt over de technische, bedrijfseconomische en juridische expertise middelen om een goed afgewogen oordeel over het aanbod aan Clouddiensten te kunnen vormen. Een kleine afnemer ziet mogelijk veel onduidelijkheden, of krijgt juist een te positief beeld voorgesteld door de aanbieder. Voor kleine en middelgrote afnemers ligger er anderzijds ook veel kansen. Kleine afnemers kunnen middels Cloud Computing de beschikking krijgen over moderne IT-middelen zonder daar op voorhand de

investeringen voor te doen. Juist de flexibiliteit en het wegnemen van de beheersmatige inspanning kan voor kleine en middelgrote afnemers aantrekkelijk zijn.

6.1 Compliance / Privacy

Zonder meer één van de meest besproken onderwerp in relatie tot Cloud Computing is privacy. Hieronder worden de belangrijkste aspecten van het cluster privacy in relatie tot Cloud Computing beschreven.

VOLDOEN AAN DE WBP & DE (NIEUWE) MELDPLICHT

Veel organisaties leggen informatie vast over personen (klanten, relaties, medewerkers, etc.) en zijn hierdoor gehouden aan de Wet Bescherming Persoonsgegevens, de WBP. Deze wet schrijft onder meer voor dat organisaties bij uitbesteding van de verwerking van persoonsgegevens zorgen voor een 'bewerkersovereenkomst', en toezien op naleving van de afgesproken beveiligingsmaatregelen. Daarin dienen de afspraken te staan over de beveiliging van de persoonsgegevens. De wet is onverminderd van toepassing op Cloud Computing.

Omdat veel aanbieders van Clouddiensten datacenters hebben buiten de EU, of omdat de afnemer bij gebruik van Clouddiensten niet weet waar de gegevens worden verwerkt/opgeslagen, bestaat er veel onduidelijkheid bij afnemers of, en hoe, bij toepassing van Cloud Computing, kan worden voldaan aan de eisen die voortvloeien uit de WBP.

Voorbeeld:
In Denemarken heeft de privacytoezichthouder geoordeeld dat een Deense gemeente haar leraren geen gebruik kan laten maken van Google Apps voor onder meer het registreren van lesroosters, het toetsen van leerontwikkeling van leerlingen en het communiceren met andere leraren, leerlingen en hun ouders. De privacybescherming bij gebruik van de diensten zouden onvoldoende gewaarborgd zijn.

Het oordeel van de Deense toezichthouder is interessant, omdat de Deense privacywet, net als de Nederlandse privacywetgeving, voorkomt uit dezelfde EU privacyrichtlijn. Voor veel afnemers is dit de reden geen gebruik te maken van Clouddiensten.

Naast de bestaande verplichtingen die voortkomen uit de WBP komt er naar verwachting in de Telecomwet (TW) een wettelijke meldplicht van inbreuken op privacy en veiligheid. Naast een meldplicht voor datalekken is in het wetsvoorstel ook een voorstel opgenomen rondom het melden van discontinuïteit (zie verder paragraaf 4.1). Volgens het wetsvoorstel zal de meldplicht vooralsnog alleen gaan gelden voor telecomproviders, maar er is al aangekondigd dat er ook een algemene meldplicht zal komen voor alle bedrijven en overheidsdiensten.
Het is bovendien niet altijd duidelijk wanneer een aanbieder van Clouddiensten onder de TW valt. Het moeten voldoen aan de meldplicht kan door afnemers en aanbieders worden ervaren als een belemmering voor het gebruik van Clouddiensten (zie verder 4.6). Daartegenover staat dat een dergelijke meldplicht bijdraagt aan meer transparantie van Clouddiensten waardoor het vertrouwen bij afnemers toeneemt. Dit is ook in het belang van aanbieders van Clouddiensten.

VOLDOEN AAN DE WETGEVING MET BETREKKING TOT DE FISCALE EN COMMERCIËLE JAARREKENING (/IFRS)

Naast de verplichtingen die voortkomen uit de WBP zijn organisaties gehouden aan wetgeving met betrekking tot de fiscale en commerciële jaarrekening. Denk hierbij aan regels als IFRS, SOx en wetgeving op de jaarrekening. Deze wettelijke verplichtingen leiden tot vergelijkbare belemmeringen als die gelden voor de WBP.
Afnemers vragen zich af of, en hoe, bij gebruik van Clouddiensten aan deze wetgeving kan worden voldaan. Een complicerende factor bij het beantwoorden van deze vraag is dat aanbieders van Clouddiensten in het algemeen niet, of slechts beperkt, voorzien in mogelijkheden voor afnemers om audits uit te (laten) voeren. Er is geen automatische "right-to-audit".

PER LAND WISSELENDE WET- EN REGELGEVING

Tussen landen, ook binnen de EU, verschilt wet- en regelgeving (bijvoorbeeld op het gebied van privacy, dataretentie, etc.). Omdat Cloud Computing locatieonafhankelijk en grensoverschrijdend is, vormen deze verschillen tussen landen een belemmering voor de ontwikkeling en het gebruik van Clouddiensten. Zowel aanbieders van Clouddiensten als internationaal opererende afnemers zien de verschillen in wet- en regelgeving als één van de grootste belemmeringen voor de ontwikkeling en het gebruik van Clouddiensten.

AANBIEDERS: VOLDOEN AAN DE TW (REIKWIJDTE TW; IMPACT OP INNOVATIE)

Sommige Clouddiensten bevatten functies waardoor de dienst het karakter krijgt van een openbare telecommunicatiedienst (zie verder 4.6). De vraag is of dergelijke aanbieders daarmee gekwalificeerd kunnen worden als aanbieders van elektronische communicatienetwerken of –diensten, of zelfs als aanbieder van openbare telecommunicatienetwerken of –diensten, en daarmee onder de scope van de Telecommunicatiewet vallen. Het voldoen aan de telecommunicatiewet kan van invloed zijn op aanbieders van Clouddiensten. Dit houdt hoofdzakelijk verband met de verplichtingen uit Hoofdstuk 13 van de Telecommunicatiewet inzake aftapbaarheid van het netwerk of de dienst, en andere opsporings- en nationale veiligheidsbevoegdheden in dit verband (waaronder de bewaarplicht ten aanzien van verkeersgegevens). Ook de eerder genoemde meldplicht wordt waarschijnlijk onderdeel van de Telecomwet.

6.2 Informatiebeveiliging en controle

Het tweede cluster van belemmeringen, heeft betrekking op het cluster informatiebeveiliging en controle. Bij het opslaan van gegevens in de Cloud, hebben afnemers vragen en/of zorgen rondom de veiligheid van die gegevens.

CONTROLE OVER DE EIGEN GEGEVENS

Omdat bij gebruik van Clouddiensten de data wordt opgeslagen bij de aanbieder van de Clouddienst kan onduidelijkheid ontstaan over het eigendom (afnemer, aanbieder of beide?) van de opgeslagen gegevens. Hoe weet je als afnemer of de aanbieder van Clouddiensten de data ook niet voor andere doeleinden gebruikt? Is het intellectueel eigendom (IPR) gewaarborgd? En heb je het recht te allen tijde over je eigen gegevens te beschikken (ook als er sprake is van een geschil

tussen aanbieder en afnemer)? De WBP schrijft voor dat persoonsgegevens niet langer bewaard mogen worden in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. Toch vragen veel afnemers zich ad of er geen "sporen" achter blijven nadat gegevens zijn verwijderd uit de Cloud, of nadat het gebruik van een Clouddienst is stopgezet. Met andere woorden, hoe weet de afnemer dat er niet alsnog misbruik van informatie kan plaatsvinden?
Mede door de vaak ondoorzichtige standaardvoorwaarden die verbonden zijn aan Clouddiensten ontstaan vragen en twijfels over het eigendom van data. Hoe weet een afnemer of de standaardvoorwaarden voldoende bescherming bieden? Voor wat de inhoud van de betreffende voorwaarden betreft, zien we in de praktijk vaak een eenzijdige invulling door Cloudaanbieders als het gaat om onderwerpen zoals de bescherming van persoonsgegevens, vertrouwelijkheid van gegevens en hoe met de verdeling van risico's wordt omgegaan (zie verder 4.3).

Grootzakelijke afnemers en overheidsorganisaties beschikken in het algemeen over voldoende juridische kennis, of hebben de middelen deze in te huren, om op deze vragen een goed antwoord te kunnen formuleren. Dit in tegenstelling tot het MKB en startende ondernemers waar (juridische) kennis en middelen vaak ontbreken om vragen rondom data en intellectueel eigendom te kunnen beantwoorden.

Controle over de eigen gegevens betekent ook te allen tijde de eigen gegevens uit de Clouddienst kunnen onttrekken. Met andere woorden biedt de aanbieder een mogelijkheid om snel, en in een standaard (/bruikbaar) formaat, alle eigen gegevens uit de Clouddienst weg te halen (te "downloaden" of te migreren naar een andere Clouddienst). Deze mogelijkheid zit niet standaard in iedere Clouddienst. Het ontbreken van de mogelijkheid om gegevens eenvoudig weg te kunnen halen creëert een "vendor lock-in" situatie die voor afnemers een belemmering vormt om van een Clouddiensten gebruik te maken. Hieronder, in paragraaf 6.5, gaan we ook in op het punt portabiliteit.

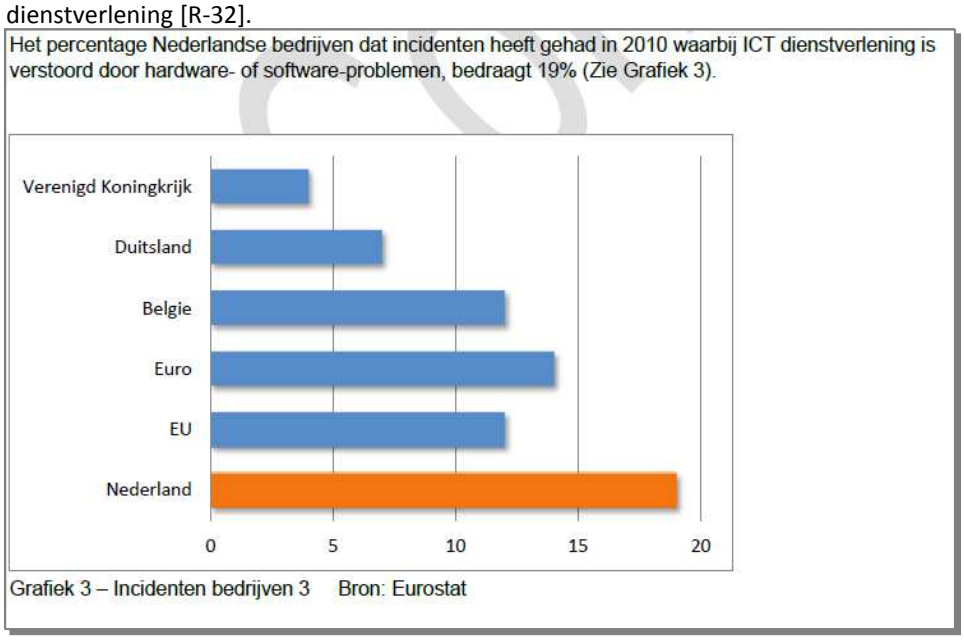
TRANSPARANTIE VAN, EN CONTROLE OP, HET NIVEAU VAN INFORMATIEBEVEILIGING

Bij gebruik van Cloud Computing wordt de data van de afnemer opgeslagen in de Cloud. De zorg voor een adequate beveiliging van deze data ligt nu bij de aanbieder van de Clouddienst. Afnemers maken zich zorgen of de aanbieder voldoende maatregelen heeft getroffen om de data te beschermen tegen ongeautoriseerde toegang, manipulatie en besmetting door virussen, malware etc.. Ook vraagt men zich af hoe het zit met aansprakelijkheid in het geval er sprake is van een inbreuk op en misbruik van de opgeslagen gegevens.
Aanbieders geven vaak geen, of slechts in beperkte mate, inzicht in de beveiligingsmaatregelen die zijn genomen en de manier waarop de aanbieder deze maatregelen test en controleert. Ook geven maar weinig aanbieders van Clouddiensten inzicht in de mate waarin deze beveiligingsmaatregelen effectief zijn, met andere woorden, hoe vaak, en welke, veiligheidsincidenten hebben zich voorgedaan.

Door veel (potentiële) afnemers wordt het gebrek aan transparantie en controle als één van de grootste obstakels gezien. Het belemmert afnemers in de afweging of de geboden

beveiligingsmaatregelen aansluiten bij het gewenste niveau. Een vergelijking met eventuele eigen bestaande maatregelen wordt daarmee ook lastig.

Overigens wordt in dit kader opgemerkt dat uit eerder onderzoek door Eurostat is gebleken dat het Nederlandse bedrijfsleven in vergelijking met een aantal andere EU landen een relatief hoog percentage kent aan hard- en/of software problemen die leiden tot incidenten in de IT dienstverlening [R-32].



Figuur 4 Europese benchmark beveiligingsincidenten bedrijfsleven

Uit hetzelfde onderzoek blijkt tevens dat Nederland hoog scoort als het gaat om het lekken van gevoelige informatie als gevolg van IT aanvallen. Met een percentage van 4% van de Nederlandse bedrijven dat dergelijke incidenten heeft gehad, scoort Nederland significant slechter dan de rest van de EU.
Behalve dat Cloud Computing nieuwe risico's met betrekking tot informatiebeveiliging met zich meebrengt, biedt het wellicht ook kansen voor Nederland het aantal incidenten terug te dringen en beter op dit thema te scoren. Hiervoor is een nadere analyse van het door Eurostat uitgevoerde onderzoek nodig. De gegevens uit het onderzoek stammen uit 2009 en gelden voor het gebruik van IT in het algemeen (ongeacht het gebruik van Cloud Computing dat toen nog in de kinderschoenen stond).
Het onderzoek geeft wel aan dat beveiligingsincidenten altijd een punt van aandacht vormen, los van Cloud Computing. De beveiligingsrisico's die het gebruik van Cloud Computing met zich meebrengt, zullen dan ook tegen de risico's van andere vormen van IT moeten worden afgezet. Deze afweging vergt transparantie in de manier waarop de beveiliging van Clouddiensten is vormgegeven.
De vraag hoe transparantie te verkrijgen is een ingewikkelde zaak bij Cloud Computing. Degene voor wie de informatie om transparantie te vergroten is bedoeld, moet deze ook kunnen begrijpen (om transparantie ook effectief te maken). Dit geldt met name voor bekendmaking van incidenten en informatieverstrekking aan particulieren (bijv. gebruikers van SaaS-diensten) maar ook aan

zakelijke gebruikers. De ontwikkeling van een model met de belangrijkste KPI's zou gebruikers kunnen helpen bij de vraag 'hoe goed beschermt deze Cloudaanbieder mijn vertrouwelijke gegevens (of die van mijn klanten)?' Beleidsmakers zullen bij het creëren van een aantrekkelijk Cloud Computing klimaat moeten nagaan hoe ze voor Cloudaanbieders en gebruikers bruikbare transparantietesten kunnen ontwikkelen. Bijvoorbeeld hoe gedetailleerd dient een melding van inbreuk op gegevens[18] te zijn en hoe kunnen wettelijke verplichtingen omtrent privacy- en beveiligingsbeleid begrijpelijk voor de eindgebruiker worden gemaakt vanuit de technologische complexiteit van Cloud Computing.

IDENTITEIT- EN TOEGANGSBEHEER

Een specifiek onderwerp binnen het cluster informatiebeveiliging en controle is identiteits- en toegangsbeheer. In een traditionele IT-omgeving is een organisatie hiervoor volledig zelf verantwoordelijk. Bij Cloud Computing ligt ook een belangrijke verantwoordelijkheid bij de aanbieder van de dienst. Het is uiteindelijk de aanbieder die het technisch beheer voert over het identiteits- en toegangsbeheer met betrekking tot de Clouddienst. Maar hoe weet een organisatie die gebruik maakt van Clouddiensten of het identiteits- en toegangsbeheer voldoende veilig is ingericht? En heeft de organisatie direct invloed op wie toegang heeft tot de dienst, zodat bijvoorbeeld in geval van ontslag een medewerker per direct de toegang tot dienst ontnomen kan worden?

TOEGANG TOT INFORMATIE DOOR ANDERE (NIET-EU) OVERHEDEN (O.A. USA PATRIOT ACT)

Eén van de veel besproken onderwerpen rondom Cloud Computing is toegang tot opgeslagen informatie door andere overheden. Cloud Computing heeft als eigenschap locatieonafhankelijkheid; het maakt voor de afnemer (functioneel) niet uit waarvandaan de Clouddiensten worden geleverd. Aanbieders van Clouddiensten, en de rekencentra waar de data is opgeslagen, kunnen in principe overal ter wereld zijn gevestigd. Dit roept bij afnemers vragen op over de mogelijkheden die overheden hebben zich toegang te verschaffen tot de aanbieders van Clouddiensten en/of de aldaar opgeslagen informatie.
In het bijzonder wordt vaak gewezen op de USA PATRIOT Act, ofwel de mogelijkheden die de Amerikaanse overheid zou hebben om zich toegang te verschaffen tot informatie opgeslagen in de Cloud (zie verder 4.6).
Het vraagstuk van toegang tot informatie door overheden van andere landen speelt voornamelijk bij afnemers binnen het publieke domein (zorg, overheid). Het MKB en grootzakelijke afnemers zien dit in mindere mate als belemmering. Bedrijven met veel intellectueel eigendom zullen zich eerder zorgen maken over toegang door derden, o.a. door gebrekkige informatiebeveiliging (zie begin van deze paragraaf).

[18] Een voorstel tot het introduceren van dit meldingsregime in de Telecom Wet is nu onderdeel van een wetgevingsproces (Eerste Kamer). Bovendien werkt het European Network and Information Security Agency (ENISA) samen met landelijke telecom wetgevers om operationele procedures en regels inzake de melding van inbreuk op gegevens vast te leggen omdat de landelijke wetgevers sommige gegevens aan ENISA moeten doorgeven.

6.3 Business continuïteit

Het derde cluster van belemmeringen voor Cloud Computing, is het cluster business continuïteit.

BESCHIKBAARHEID VAN DE DIENST

Veel Clouddiensten worden aangeboden zonder een garantie voor de minimale beschikbaarheid van de dienst. Met beschikbaarheid wordt hier bedoeld de "uptime" van de dienst, ofwel de tijd dat alle functionaliteit met de gebruikelijke performance door de afnemer gebruikt kan worden. Voor slechts een aantal Clouddiensten wordt wel een minimale beschikbaarheid gegarandeerd. Dit zijn voornamelijk IaaS-diensten. Tot op heden worden Clouddiensten om die reden het meest ingezet voor niet-bedrijfskritische toepassingen, zoals bijvoorbeeld e-mail of toepassingen rondom kantoorautomatisering. Om afnemers over de streep te trekken ook meer bedrijfskritische toepassingen in de Cloud te plaatsen zal de aanbieder meer werk moeten maken van het bieden van zekerheden met betrekking tot de beschikbaarheid van de dienst.

De recente inval bij de aanbieder MegaUpload.com zorgde wereldwijd bij veel afnemers problemen om de opgeslagen informatie terug te halen. Het is op het moment van het schrijven van het rapport niet duidelijk of/wanneer gebruikers weer toegang tot de opgeslagen informatie krijgen.

Figuur 5 Afbeelding op de site www.megaupload.com op 24 januari 2012

Daarbij komt dat aanbieders in het algemeen niet transparant zijn over de in het verleden geleverde prestaties. Zeer weinig aanbieders publiceren de behaalde beschikbaarheid van de dienst in de afgelopen periode.

Zoals in paragraaf 4.1 is beschreven ligt er een voorstel tot wijziging van de Telecomwet in de Eerste Kamer. Onderdeel van dat wetsvoorstel is het opnemen van een verplichting voor aanbieders om inbreuken op de veiligheid, en/of een verlies van integriteit, waardoor de continuïteit in belangrijke mate werd onderbroken onverwijld te melden (Art 11a.2).

CONTINUÏTEIT BIJ INSOLVENTIE (OP TERMIJN: CLOUDDIENSTEN ALS VITALE INFRASTRUCTUUR)

Cloud Computing is een relatief nieuw fenomeen dat nog volop in beweging is. Innovaties volgen elkaar snel op. Ook blijkt dat diensten snel kunnen groeien, maar ook in korte tijd weer snel kunnen verdwijnen of sterk krimpen. Hetzelfde geldt voor de aanbieders zelf. Deze snel veranderende omgeving, gecombineerd met de afhankelijkheid van een Clouddienst, vormt voor potentiële afnemers een belemmering voor het gebruik van deze diensten. Dit geldt met name voor SaaS-diensten. Een afnemer heeft geen garantie voor het voortbestaan van een Clouddienst, terwijl het wegvallen van deze dienst grote gevolgen kan hebben voor de continuïteit van de bedrijfsvoering. Het risico op een faillissement en de onzekerheid wat er in zo'n geval gebeurt met de continuïteit van de dienst vormt voor alle afnemers, groot en klein, een belemmering.

GARANTIES M.B.T. (MINIMALE) LEVENSDUUR DIENST/FUNCTIONALITEIT ("OPZEGTERMIJN")

De vorige belemmering richt zich op het volledig wegvallen van een dienst als gevolg van een faillissement van de aanbieder. Echter, ook zonder faillissement van de aanbieder kan de continuïteit van de (functionaliteit van de) Clouddienst in gevaar komen. Zeker de standaard voorwaarden die op veel Openbare Clouddiensten van toepassing zijn bieden geen zekerheid dat de aanbieder de Clouddienst niet op enig moment afbouwt of in functionaliteit wijzigt (bijvoorbeeld omdat de aanbieder denkt daarmee een beter economisch resultaat te behalen). Alvorens de bedrijfsprocessen aan te passen om van een Clouddienst gebruik te kunnen maken, wil een afnemer een zekere mate van zekerheid dat functies waarvan de processen afhankelijk zijn, niet zomaar door de aanbieder worden gewijzigd.

6.4 Markt, aanbod en business case

Het vierde cluster van belemmeringen concentreert zich rondom het aanbod en de markt voor Clouddiensten.

FUNCTIONALITEIT NIET TE BEÏNVLOEDEN / ONGEVRAAGD GEWIJZIGD

Een van de kernelementen van (met name Openbare) Clouddiensten is dat de aanbieder tracht schaalgrootte te ontwikkelen. Door zijn IT-middelen te delen met meerdere gebruikers kan hij efficiënter werken dan een enkele afnemer. Dit concept betekent echter ook dat er weinig ruimte is voor een individuele afnemer om specifieke maatwerk-oplossingen in de afgenomen diensten aan te (laten) brengen. Voor organisaties betekent dit in veel gevallen dat zij processen en/of systemen moeten aanpassen aan datgene dat door de aanbieder geboden wordt. Wanneer een organisatie zelf een bepaalde toepassing ontwikkelt kan echt maatwerk worden gerealiseerd. Bij het kiezen voor een Clouddienst moet dan ook worden afgewogen of de kosten van het aanpassen van bestaande bedrijfsprocessen opweegt tegen de voordelen van de Cloud. Juist de voordelen van Clouddiensten, zoals bijvoorbeeld flexibiliteit, kan bij de gebruiker leider tot het besef dat "goed, goed genoeg is".
Wanneer eenmaal een bepaalde Clouddienst is afgenomen, rijst de vraag op welke wijze de Clouddienst zich ontwikkelt. Enerzijds verwacht de afnemer dat hij/zij ontzorgd wordt op het vlak van het beheer van de dienst en dat doorontwikkeling gegarandeerd is. Anderzijds heeft een individuele afnemer hier niet of nauwelijks invloed op. Zo kan de aanbieder besluiten de dienst aan te passen, terwijl personeel net was getraind op een bepaalde manier, of dat koppelingen met

andere systemen waren gemaakt. Door de wijzigingen moeten de gebruikers weer "wennen" of moeten koppelingen weer worden aangepast.

Voor sommige organisaties geldt dat zij zich door een maatwerk oplossing van haar concurrenten kan onderscheiden. Wanneer veel organisaties van dezelfde Clouddienst gebruik maken, wordt het maken van een onderscheid op dat terrein lastig.

CONTRACTEN & STANDAARDVOORWAARDEN

In zijn algemeenheid kan worden gesteld dat voor de afnemers een aantal belangrijke bezwaren kleeft aan de voorwaarden waaronder met name grote Amerikaanse aanbieders Clouddiensten in Nederland aanbieden. De betreffende voorwaarden worden doorgaans als sterk eenzijdig, niet onderhandelbaar en weinig transparant beschouwd. De voorwaarden zijn in de regel gemodelleerd naar de contractmodellen welke door de betreffende aanbieders in de Verenigde Staten worden gebruikt en kenmerken zich door weinig toegankelijk taalgebruik, mede gekleurd door veel (vertaalde) Angelsaksische begrippen, en een voor de lezer complexe structuur in termen van gelaagdheid en doorverwijzing naar andere relevante (contract) documenten, zoals privacy policies.
In de voorwaarden treft men vaak een eenzijdige verdeling van verantwoordelijkheden, met name ten aanzien van de bescherming van persoonsgegevens (verantwoordelijke of bewerker). Veelal ontbreken harde waarborgen inzake toegankelijkheid en vertrouwelijkheid van gegevens. Voor de individuele eindgebruiker zijn de voorwaarden in de praktijk niet onderhandelbaar (zie verder 4.3).

VOLWASSENHEID: TRANSPARANTIE / RAPPORTAGE OVER GELEVERDE PRESTATIES

De markt voor Clouddiensten is nog volop in ontwikkeling. Voor de bepaling van het stadium van ontwikkeling van een industrie wordt vaak gebruik gemaakt van de volgende begrippen: embryonaal, groei, shake-out, volwassenheid en terugval [R-33]. De markt voor Clouddiensten is duidelijk in de groeifase. Zowel op het vlak van aanbod, als op het vlak van standaarden is er nog veel ruimte voor ontwikkeling.
Er is wel een onderscheid tussen de verschillende soorten Clouddiensten, SaaS, PaaS en IaaS. Met name met betrekking tot IaaS zijn er voorbeelden van diensten die al een hoge mate van volwassenheid hebben bereikt (bijvoorbeeld door garanties met betrekking tot de fysieke locatie van gegevens, beschikbaarheid en performance van de dienst).

Aanbieders van Clouddiensten zijn weinig transparant over de geleverde prestaties. Niet veel aanbieders hebben op hun website bijvoorbeeld een overzicht staan van de gerealiseerde beschikbaarheid, aantal incidenten of responsetijden. Slechts enkele aanbieders vormen de uitzondering op de regel. Bijvoorbeeld Google die met haar Apps Dashboard een relatief goed inzicht biedt in de beschikbaarheid. De bereikbaarheid en deskundigheid van een servicedesk kan een belangrijk criterium voor een afnemer zijn, om voor een bepaalde leverancier te kiezen. In een volwassen markt is het waarschijnlijk dat leveranciers zelf, of onafhankelijke derden, hier meer transparantie creëren.

Het ontbreken van heldere prestatie-indicatoren en garanties op die indicatoren, kan worden gezien als een symptoom van de onvolwassenheid van de markt voor Clouddiensten. Grote aanbieders van Clouddiensten zijn op dit moment wel hard aan de slag om de transparantie rondom hun prestaties te vergroten.
Anderzijds is het een kenmerk van Openbare Clouddiensten dat zij worden aangeboden via het Internet. Het verkrijgen van garanties rondom de beschikbaarheid van *het* Internet bestaan niet. Specifiek voor de Cloud geldt dat het bij het delen van voorzieningen, acties van één klant van invloed kunnen zijn op de geleverde prestaties aan andere klanten. Het "overboeken" van een bepaalde voorziening is een veelgeziene strategie om schaalvoordelen te realiseren.

6.5 Overig (waaronder Integratie, standaarden en netwerkinfrastructuur)

Hieronder wordt de vijfde en laatste cluster van belemmeringen beschreven. Het betreffen een aantal belemmeringen die lastig onder één noemer zijn te vangen.

GEGEVENS PORTABILITEIT EN INTEROPERABILITEIT

Afnemers van Clouddiensten kunnen te maken krijgen met beperkingen rondom het terugdraaien (reversibility) of het porteren van de door hen afgenomen diensten. Doordat een leverancier van Clouddiensten keuzes maakt rondom de wijze van opslaan van gegevens van haar klant, kan een situatie ontstaan dat die gegevens niet zonder meer door een andere leverancier kunnen worden ingelezen en de dienstverlening kan overnemen. Bij een overstap naar Clouddiensten kan deze belemmering overigens ook zichtbaar worden. Wanneer een organisatie eigen dienstverlening wil gaan vervangen voor Clouddiensten kan zij te maken krijgen met dataconversie en migratie.

Het vraagstuk rondom portabiliteit en interoperabiliteit is groter naarmate de Clouddiensten meer richting eindgebruiker worden afgenomen. Bij IaaS-diensten speelt het minder dan bij PaaS en zeker SaaS. Dit wordt met name veroorzaakt door het gebrek aan (open) standaarden voor de integratie van Clouddiensten. Om dit probleem op te lossen werken op dit moment verschillende partijen aan het creëren van voorzieningen die de integratie van verschillende diensten (Cloud en niet-Cloud) beter mogelijk maken. Een mooi voorbeeld is de dienstverlening die door SURFnet wordt ontwikkeld: SURFconext. SURFconext is een op open standaarden gebaseerde samenwerkingsinfrastructuur waarmee instellingen interne en externe online diensten kunnen integreren.

INFRASTRUCTURELE BELEMMERINGEN

Clouddiensten komen in de meeste gevallen tot stand door een samenspel van diensten van verschillende partijen. De meest in het oog springende is het onderscheid tussen het afnemen van het transportkanaal (het Internet) en de aanbieder van de dienst. In de meeste gevallen levert een aanbieder van telecommunicatiediensten de toegang tot het Internet. Ook de aanbieder van de Clouddienst maakt gebruik van een andere aanbieder om hem de toegang tot het Internet te leveren. Zoals al eerder gesteld, is het niet mogelijk om garanties af te geven over de beschikbaarheid van het Internet.
Als afnemer van een Clouddienst kan een organisatie bij problemen met de prestaties van een Clouddienst dus te maken krijgen met een aantal partijen die allen een rol spelen bij de

totstandkoming van de dienst. Wanneer de dienst zelf "in huis" tot stand wordt gebracht speelt dit probleem niet of veel minder.

In dit kader moet worden opgemerkt dat het Nederlandse aanbieders van openbare telecommunicatiediensten in het kader van netneutraliteit niet is toegestaan om onderscheid te maken naar verschillende Internet- (en dus Cloud)diensten. Clouddiensten hebben daarmee eenzelfde status, en dus beschikbaarheid en performance, als andere internetdiensten. De vraag is of de huidige regelgeving met betrekking tot netneutraliteit voldoende ruimte biedt aan aanbieders van telecommunicatiediensten om netwerkverbindingen aan te bieden met kwaliteitsgaranties gericht op Clouddiensten, mocht hier (in de toekomst) behoefte aan bestaan.

Het ontbreken van een zeer breedbandige (glas)netwerk naar een groot deel van de huishoudens in Nederland betekent dat Clouddiensten die behoefte hebben aan de capaciteit van zo´n netwerk nu (nog) niet tot stand kunnen komen. In die zin geldt de belemmering mogelijk aan de aanbiederszijde. Afnemers ervaren de belemmering nog niet of nauwelijks. Zakelijke afnemers van Clouddiensten, zullen indien nodig, op heel veel plaatsen in Nederland wel een glasvezelverbinding kunnen afnemen.

6.6 Samenvatting

In dit hoofdstuk zijn de uit het onderzoek gebleken belemmeringen samengevat in vijf clusters:

1. Compliance / Privacy
2. Informatiebeveiliging en controle
3. Business Continuïteit
4. Markt, aanbod & business case
5. Overig (waaronder Integratie, standaarden en netwerkinfrastructuur)

Voor een volledig overzicht van alle gevonden belemmeringen wordt verwezen naar C. Daarnaast is voor diepgang ten aanzien van de juridische context Deel II in dit rapport opgenomen.

Wanneer in publicaties of gesprekken wordt gewezen op de mogelijke belemmeringen voor het gebruik, of verdere groei van het gebruik van Cloud Computing, gaat het meestal over de belemmeringen in het cluster Compliance / Privacy en het cluster Informatiebeveliging en controle. Veel minder is er geschreven over de mate waarin organisaties nu daadwerkelijk om de genoemde belemmeringen afzien van het gebruik van Cloud Computing. Daarnaast bestaat het gevoel dat er een aanzienlijk gat zit tussen de perceptie en de werkelijkheid van een bepaalde belemmering. Belemmeringen voor het gebruik van Cloud Computing worden wellicht zwaarder gewogen dan strikt noodzakelijk is en belemmeringen gelden wellicht in dezelfde mate voor de huidige inzet van IT-middelen en of IT-leveranciers.

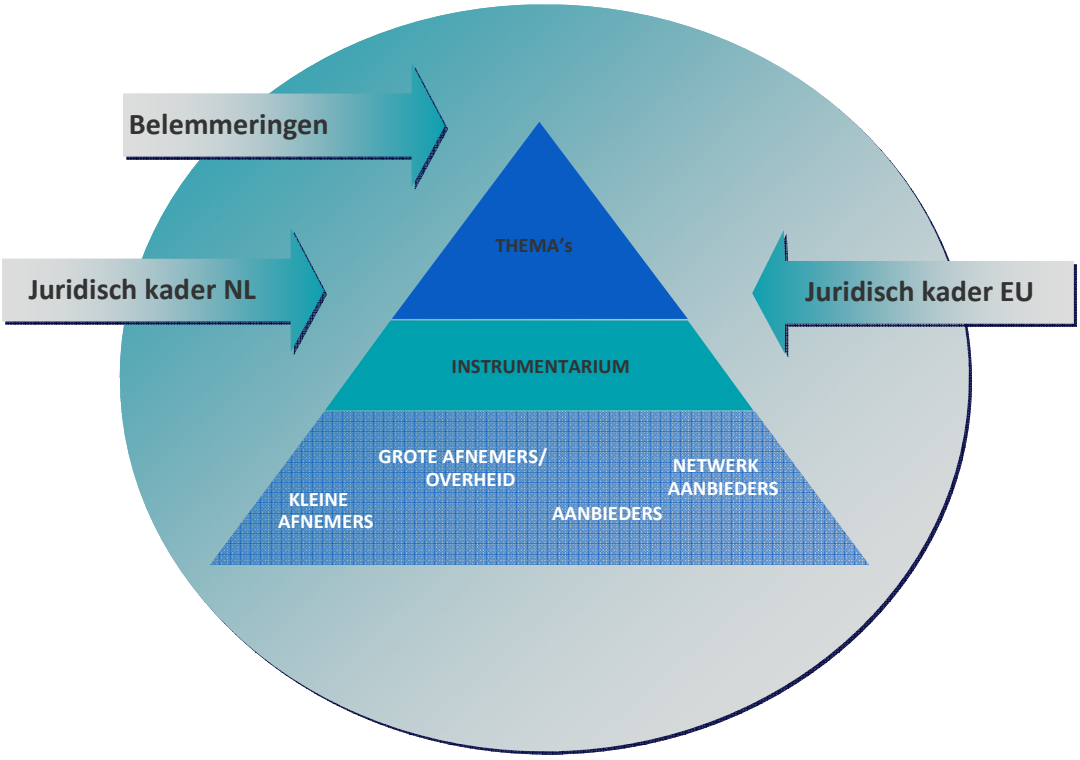
In het volgende hoofdstuk worden een aantal voorstellen gedaan voor maatregelen die de genoemde belemmeringen (of de perceptie daarvan) adresseren.

7 AANBEVELINGEN: HET FUNDAMENT OP ORDE

In de vorige hoofdstukken zijn de belangrijkste ontwikkelingen, (clusters van) belemmeringen en de juridische context geïdentificeerd. Dit hoofdstuk geeft richting aan het door EL&I te voeren beleid ter bevordering van de productiviteit en innovatie bij organisaties in Nederland door toepassing van Cloud Computing: het fundament op orde.

De aanbeveling voor het EL&I beleid gaat uit van de volgende structuur:

- Thema's. Er is gekozen voor een viertal thema's die EL&I als uitgangspunt voor het beleid met betrekking tot Cloud Computing kan hanteren. Deze thema's staan boven de meer specifieke maatregelen die EL&I kan overwegen, en dienen als algemene uitgangspunten voor beleid. Ze geven houvast in een markt die nog volop in beweging is en ongetwijfeld nieuwe (beleids)vragen zal opwerpen.
- Beleidsinstrumentarium. Het ministerie van EL&I heeft een aantal mogelijkheden waarmee het Cloud Computing beleid vorm gegeven kan worden, het beleidsinstrumentarium.
- Aanbeveling per doelgroep. De thema's worden uitgewerkt in meer specifieke aanbevelingen per doelgroep: Afnemers klein, afnemers groot/overheid, aanbieders Clouddiensten en aanbieders netwerkdiensten (de aanbieders van telecommunicatiediensten).



7.1 De vier thema's

Op basis van de analyse van de ontwikkelingen rondom Cloud Computing (H3), de juridische en Europese context (H4 en 5) en de inventarisatie van belemmeringen die afnemers en aanbieders van Clouddiensten ervaren (H6), is gekomen tot vier thema's voor beleid rondom Cloud Computing van EL&I.

Om Cloud Computing te kunnen laten bijdragen aan de productiviteitsverbetering en innovatie van de BV Nederland en overheid, wordt het ministerie van EL&I aanbevolen haar beleid te richten op:

1. het bevorderen van transparantie en volwassenheid;
2. duidelijke en geharmoniseerde wet- en regelgeving;
3. zorgen voor continuïteit;
4. stimuleren van het gebruik van Cloud Computing.

De eerste drie thema's richten zich op het wegnemen of verminderen van belemmeringen, terwijl thema 4 een stap verder gaat door actief het gebruik van Cloud Computing te bevorderen. Elk thema wordt in dit hoofdstuk nader toegelicht en uitgewerkt. In de volgende paragrafen worden de thema's vertaald naar meer specifieke aanbevelingen per doelgroep, uitgaande van de voor EL&I beschikbare beleidsinstrumenten (paragraaf 7.7).

7.2 Thema 1: Het bevorderen van transparantie en volwassenheid

Uit het onderzoek blijkt dat de markt voor Clouddiensten nog volop in beweging is en nog niet het stadium van volwassenheid heeft bereikt, zeker daar waar het gaat om toepassingen ter ondersteuning van kritische bedrijfsprocessen. Het aanbod is veelal nog onvoldoende afgestemd op de vraag. Dit geldt voor de markt voor (Openbare) Clouddiensten in het algemeen, maar bijvoorbeeld ook voor de specifieke markt voor overheiddiensten.

Behalve volwassenheid vormt het gebrek aan transparantie van de markt in het algemeen, en van individuele Clouddiensten in het bijzonder, een belemmerende factor voor snelle groei. Voor afnemers is het lastig vast te stellen welke Clouddiensten passen bij het gewenste service niveau, en hoe deze diensten in werkelijkheid presteren. Relatief eenzijdig opgestelde en ondoorzichtige voorwaarden dragen verder bij aan de ondoorzichtigheid. En dat terwijl het een complexe markt betreft met veel dienstverleningsaspecten die voor organisaties van groot belang zijn (beveiliging, responsetijd, beschikbaarheid, support etc.). Het gebrek aan transparantie leidt tot verschillen in perceptie en werkelijkheid, onzekerheid over de kwaliteit van de aangeboden dienst en een gebrek aan vertrouwen in de Cloud.

Meer transparantie, en de verdere ontwikkeling van Clouddiensten richting volwassenheid, zijn belangrijke voorwaarde voor het succes van Clouddiensten.

Aanbevolen wordt om het bevorderen van transparantie en volwassenheid als algemeen uitgangspunt te hanteren en nader uit te werken hoe EL&I hier, in samenwerking met de markt, concreet invulling aan kan geven.

Hoewel primair een verantwoordelijkheid van aanbieders en afnemers van Clouddiensten, kan het ministerie van EL&I bijdragen aan het proces van totstandkoming van meer transparantie. Hierbij kan worden gekeken naar initiatieven als certificering, voorlichting, vraagarticulatie en ontwikkeling en gebruik van (open) standaarden. Gelet op de snelle ontwikkelingen en het innovatieve karakter van Clouddiensten, wordt geadviseerd terughoudend te zijn met het fors inzetten van meer juridische beleidsinstrumenten. Door in te zetten op het stimuleren van de eigen verantwoordelijkheid van de aanbieders kan de markt, zo is onze verwachting, zelf doorgroeien naar een volgend volwassenheidsniveau.

Noot: Bij de onderstaande aanbevelingen wordt steeds aangegeven op welke doelgroepen de aanbevelingen het meest betrekking hebben. Met andere woorden, welke (groep van) actor(en) kan het meest bijdragen aan het wegnemen van belemmeringen binnen dit thema.

Aanbeveling 1.1 (afnemers klein). Steun en stimuleer brancheorganisaties en koepels bij a) sectorgerichte voorlichting gericht op het MKB, en b) sector- of branchegerichte vraagarticulatie en contractering.

Toelichting: door voorlichting leren (potentiële) afnemers de voor- en nadelen en risico's van Cloud Computing kennen. Zij zullen daardoor beter in staat zijn de goede keuzes te maken bij het overwegen van een Clouddienst. Door een verbeterde informatiepositie zal de contractering met Cloudaanbieders mogelijk transparanter en evenwichtiger tot stand komen.
Door vraagarticulatie te stimuleren ontstaat mogelijk een betere onderhandelingspositie voor het MKB. Gezamenlijk kunnen zij opereren als grote afnemers. Dit betekent onder meer een betere onderhandelingspositie, meer juridische kennis, etc. Samenwerkende afnemers kunnen, samen met aanbieders, komen tot evenwichtiger en transparantere voorwaarden.

Aanbeveling 1.2 (afnemers groot / overheid). Onderzoek in samenwerking met BZK de mogelijkheden om standaard voorwaarden voor (overheids) aanbestedingen op te stellen ter bevordering van de transparantie van Clouddiensten, en b) hoe ervaringen met Clouddiensten binnen de overheid structureel verzameld, vastgelegd en inzichtelijk gemaakt kunnen worden.

Toelichting: Grote afnemers kunnen zelf meer transparantie afdwingen door eisen te stellen bij aanbestedingen, bijvoorbeeld een "Right-to-audit".In aanvulling hierop kunnen overheden onderling afspraken maken over een set aan eisen die overheden standaard opnemen in een aanbesteding. Dit geeft tevens duidelijkheid aan de aanbieders van Clouddiensten. Ook kunnen overheden ervaringen met Clouddiensten structureel vastleggen en delen zodat er stapsgewijs meer transparantie ontstaat. Onderdeel van de set aan voorwaarden is het eisen van het gebruik van (open) standaarden. Ondanks dat grote afnemers meer mogelijkheden hebben druk uit te oefenen op aanbieders om invulling te geven aan specifieke eisen of wensen, blijft dit, zeker bij Openbare Clouddiensten, lastig. Openbare Clouddiensten bedienen per definitie meerdere afnemers, en aanbieders zullen om die reden individuele aanpassingen tot een minimum proberen te beperken.

Aanbeveling 1.3 (aanbieders van Clouddiensten). Steun en stimuleer de totstandkoming van een breed gedragen certificering, keurmerk of erkenningsregeling in Nederland, of in EU verband.

Toelichting: Meer transparantie zal voor een groot deel door de aanbieders van Clouddiensten moeten worden ingevuld. Een deel van de aanbieders is zich terdege bewust van de noodzaak te zorgen voor meer transparantie. Vanuit de aanbieders van Clouddiensten zijn recent initiatieven ontstaan. Voorbeelden zijn Eurocloud en de Dutch Hosting Provider Association (DHPA). Wij zien dit als een positieve ontwikkeling: een certificering, keurmerk of erkenningsregeling draagt bij aan meer transparantie. EL&I zou kunnen overwegen dit soort initiatieven te ondersteunen.

7.3 Thema 2. Duidelijke en geharmoniseerde wet- en regelgeving

Cloud Computing is in het huidige juridische kader goed in te passen; wel is op een aantal punten aanpassing gewenst. Aanbieders (en grote afnemers) van Clouddiensten hebben baat bij geharmoniseerde wet- en regelgeving tussen landen. In ieder geval tussen de landen binnen de EU, maar ook met de Verenigde Staten. Dit geldt zeker ook voor Nederland als land met een sterke internationale oriëntatie. Verder blijkt uit de inventarisatie voor dit rapport dat naast harmonisering ook behoefte bestaat aan verduidelijking van bestaande wetgeving, bijvoorbeeld de toepassing van de Telecomwet. Een helder onderscheid tussen de verschillende rollen bij de totstandkoming van een Clouddienst kan hierbij helpen.

Aanbevolen wordt om (in EU verband) de harmonisatie van regelgeving te bevorderen en zorg te dragen voor eenduidige wetgeving, rekening houdend met de opkomst van Cloudaanbieders in aanvulling op de al jaren bekende aanbieders van netwerkdiensten.

Opgemerkt wordt dat bij de aanbeveling om in EU verband de harmonisatie van regelgeving te bevorderen, ook hoort het voorkomen, of in ieder geval minimaliseren, van afwijkende of aanvullende regelgeving in Nederland zelf.

Aanbeveling 2.1 (EU / Internationaal) Zet in op aanpassing, harmonisatie van wet- en regelgeving met betrekking tot privacy en andere relevante aspecten en monitor de ontwikkelingen in dit domein.

Toelichting: Met geharmoniseerde wet- en regelgeving wordt het voor aanbieders en afnemers duidelijker op welke manier met privacy-gevoelige informatie wordt omgegaan. Huidige onduidelijkheid voor aanbieders hoe om te gaan met de eisen van het land waaruit de gegevens afkomstig zijn wordt weggenomen doordat dit in alle landen dezelfde eisen zijn. In het onlangs uitgelekte ontwerp voor de nieuwe privacyverordening wordt duidelijke dat de Europese Commissie werkt aan een verordening en niet aan een nieuwe Richtlijn. Dit heeft als voordeel dat de regeling rechtstreeks werking krijgt in de EU en er geen implementatievoorstellen meer nodig zijn. Dit betekent vanzelfsprekend harmonisatie. In dit verband wordt ook gewezen op het streven van de EU naar een 'digital single market'. Dit zou een 'boost' kunnen geven aan de verdere economische ontwikkeling binnen de EU. Zaak is dan wel om te stimuleren dat de reikwijdte van

de 'digital single market' zo breed mogelijk is en alle internet-gerelateerde dienstverlening omvat (waaronder Clouddiensten).

Aanbeveling 2.2 (ministerie EL&I) Verduidelijk en of licht de relevante wetgeving en begrippenkader toe.

Toelichting: Onderzoek of het begrippenkader in de TW kan worden aangepast aan nieuwe ontwikkelingen zoals Cloud Computing, en streef naar duidelijkheid in wetgeving: op wie is de wet van toepassing en wat wordt verwacht?
Een harmonisatie van basisbegrippen met betrekking tot netwerken, datatransport, Internet, Cloud Computing etc, helpt bij het vaststellen en toelichten van wettelijke kaders voor bijvoorbeeld de WBP, TelecomWet (inclusief de nieuwe meldplicht) en opsporingsmogelijkheden.

Tot slot is geïdentificeerd dat ook ten aanzien van het aspect aansprakelijkheid er 'angst' van partijen is voor de verschillen in lokale wetgeving, zowel in de EU als daarbuiten. Er blijken nog vele verschillen te bestaan in de lokale uitwerking door de lidstaten als het gaat over het vraagstuk van de verdeling van verantwoordelijkheden en risico's bij de aankoop van diensten tegen onredelijk bezwarende voorwaarden.

Aanbeveling 2.3 (ministerie EL&I) Zet in Brussel de belangen van bedrijfsleven en met name die van het MKB op de agenda.

Toelichting: Vanuit de verschillende initiatieven van de Europese Commissie ontstaat het beeld dat veel aandacht uitgaat naar bescherming van (de privacy van) burgers. Veel minder aandacht lijkt uit te gaan naar het bedrijfsleven. Initiatieven die de positie van het bedrijfsleven, met name MKB'ers, verbeteren zouden kunnen bijdragen aan een verdere groei van het gebruik.

7.4 Thema 3. De zorg voor continuïteit

Een belangrijk zorg met betrekking tot Clouddiensten is continuïteit. Het niet, of slecht, bereikbaar zijn van Clouddiensten kan direct gevolgen hebben voor de bedrijfsvoering bij afnemers, en misschien zelfs voor een hele sector of een deel van de Nederlandse economie. Het maken van een risicoafweging ten aanzien van uitval van een Clouddienst of –aanbieder is primair een verantwoordelijkheid van iedere individuele afnemer. Echter,de verzameling netwerken en systemen waaruit de Cloud is opgebouwd vraagt om een bredere kijk op continuïteit.

Daarnaast raakt continuïteit aan aspecten als dataportabiliteit. Continuïteit, gezien vanuit de afnemer van Clouddiensten, is gebaat bij de mogelijkheid voor afnemers om te allen tijde, snel en in een bruikbaar (standaard) formaat, over de eigen gegevens te kunnen beschikken.

Aanbevolen wordt de zorg voor continuïteit als algemeen uitgangspunt bij beleidsvorming te hanteren en nader uit te werken hoe EL&I hier concreet invulling aan kan geven.

Aanbeveling 3.1 (aanbieders van Clouddiensten). Stimuleer aanbieders tot het nemen van continuïteitsmaatregelen.

Toelichting: Sommige aanbieders werken zelf aan continuïteitsvoorzieningen die afnemers zekerheid geven over de voortzetting van dienstverlening bij bijvoorbeeld faillissement van een aanbieder; een soort van Escrow-regeling gericht op Clouddiensten

Aanbeveling 3.2 (aanbieders van Clouddiensten) Monitor de mate waarin Clouddiensten vitaal zijn, of in de toekomst kunnen worden, en besluit op basis van de uitkomst van dit onderzoek over eventuele vervolgstappen, in nationaal en internationaal verband.

Toelichting: Zoals in dit rapport beschreven bestaat de Cloud uit een stelsel van netwerken, datacenters en toepassingen. Alleen als alle elementen in het stelsel werken krijgt de afnemer zijn dienst goed geleverd. In principe kan uitval van een element leiden tot een sneeuwbaleffect met als gevolg grootschalige uitval van diensten met negatieve gevolgen voor de maatschappij en economie. Net als telecommunicatie-infrastructuren, kunnen Cloud-infrastructuren zich ontwikkelen tot vitale infrastructuur. Het verschil zit in het nationale karakter van de telecommunicatiediensten en het internationale karakter van Clouddiensten. In Nederland zijn een beperkt aantal telecommunicatie-infrastructuren aan te wijzen die vitaal zijn. Deze hebben bovendien één duidelijke eigenaar die verantwoordelijk is voor die infrastructuur. Dit ligt gecompliceerder bij Clouddiensten. In principe is het mogelijk dat bijvoorbeeld een Indiaase aanbieder van Clouddiensten als vitaal gezien wordt. Net als bij de eerder besproken wet- en regelgeving, geldt voor de behandeling van vitale Clouddiensten dat dit voor een groot deel in internationaal verband plaats zal moeten vinden.

Aanbeveling 3.3 (aanbieders van Clouddiensten). Onderzoek op welke wijze in internationaal verband dataportabiliteit verder kan worden gestimuleerd.

Toelichting: Aanbieders van Clouddiensten zullen, teneinde afnemers te verleiden om hun bestaande dienstverlening in te ruilen tegen die van de Cloudaanbieder, inzetten op het bieden van datamigratie. Toch is, het migreren van data naar een ander formaat is steeds een omslachtig en mogelijk kostbaar proces. Mogelijk stuit men bij de migratie zelfs op technische beperkingen aan de zijde van de "oude" aanbieder (bijv. maximaal hoeveelheid Mb's export). Ten einde transparantie van de markt te vergroten en lock-in bij aanbieders te verkleinen verdiend het aanbeveling dataportabiliteit verder te stimuleren. Veel standaarden zijn reeds (ook in open varianten) beschikbaar.

Aanbeveling 3.4 (ministerie EL&I). Monitor (op termijn) of de huidige regelgeving met betrekking tot netneutraliteit (in de toekomst) geen belemmering vormt voor de groei van Clouddiensten.

Toelichting. Al jaren is de continuïteit van netwerken van groot belang. Dit belang neemt verder toe naarmate het gebruik van Clouddiensten groeit. Uitval van een netwerk betekent dan niet alleen uitval van telefonie en internettoegang, maar ook van toegang tot bedrijfsapplicaties in de Cloud. Daarnaast zorgt onder andere de toename in het gebruik van Clouddiensten voor een

verdere groei in dataverkeer. Aanbieders van netwerkdiensten zullen daarom moeten blijven investeren in uitbreiding van netwerkcapaciteit om continuïteit van Clouddiensten te waarborgen. De vraag is wel of en hoe een netwerkaanbieder in de toekomst kan blijven investeren. De regelgeving met betrekking tot netneutraliteit legt de aanbieder van netwerkdiensten immers grote beperkingen op ten aanzien de mogelijkheid differentiatie aan te brengen in verkeersstromen op basis van het type dienst (netneutraliteit). Internationale ontwikkelingen op dit vlak zullen goed moeten worden gevolgd om te beoordelen of Nederland in dit dossier de juiste positie heeft ingenomen.

7.5 Thema 4. Stimuleren van het gebruik van Cloud Computing

Door een aantal andere landen [R-34] wordt actief beleid gevoerd ter bevordering van het gebruik van Cloud Computing. Ook het ministerie van EL&I kan actief beleid voeren om het gebruik van Cloud Computing te stimuleren ter bevordering van de productiviteit en innovatiekracht van het Nederlandse bedrijfsleven. Hiermee wordt tevens de vooraanstaande positie van Nederland op het gebied van de (elektronische) infrastructuur versterkt. Nederland heeft één van 's werelds grootste internetknooppunten en is al jaren koploper in breedbandaansluitingen. Ook zijn Nederlanders in vergelijking met andere landen zeer actief op het Internet.
In een recent onderzoek van Roland Berger wordt de relatie gelegd met de topsectoren: Voor verschillende van de zogenaamde topsectoren is IT een belangrijke sleutel tot succes. In de topsectoren logistiek, tuinbouw, media en in de gezondheidszorg is het nu noodzaak sectorspecifieke systeemplatformen te creëren.

Eén van de belangrijkste sterktes van Nederland op het gebied van IT is zonder meer de aanwezige infrastructuur. Ons land is, dankzij uitstekende binnenlandse netwerken en internationale verbindingen, nu al de Digital Gateway to Europe op niveau van het fysieke netwerk. Met de vorming van sectorspecifieke systeemplatformen zet Nederland de volgende stap en breidt het haar positie uit van fysieke 'platte' digital gateway tot een virtuele 'intelligente' digital gateway. Het systeemplatform vormt de schakel tussen de sterke infrastructuur en de betreffende sector. [R-35]

Aanbevolen wordt actief beleid te voeren dat is gericht op het stimuleren van het aanbieden en gebruiken van Clouddiensten.

Aanbeveling 4.1 (aanbieders Clouddiensten). Stimuleer de ontwikkeling van aanbod en afname van Clouddiensten, zodat Nederland optimaal gebruik maakt van de positie die Nederland heeft (vestigingsklimaat, internetknooppunt).

Toelichting: Alhoewel de juridische "speelruimte" binnen de Europese context beperkt is, zou de Nederlandse regelgeving op het vlak van bijvoorbeeld privacybescherming toonaangevend kunnen worden in Europa en in de wereld. Dit lijkt enigszins op gespannen voet te staan met verdere harmonisering, met bovendien kans op een "race to the bottom".

Aanbeveling 4.2 (afnemers en aanbieders Clouddiensten). Community Clouds bieden mogelijkheden voor sectoren om de belemmeringen van Openbare Clouddiensten weg te nemen of te verminderen Start met belanghebbenden een discussie over de (verdere) inzet van Community Clouds, bijvoorbeeld in sectoren Zorg, Onderwijs en Overheid.

- Topsectoren logistiek, tuinbouw, media en gezondheidszorg worden in onderzoeken als kansrijk genoemd

Toelichting. Community Clouds kunnen bijdragen aan kostendeductie en innovatie in specifieke sectoren. Organisaties binnen deze sectoren krijgen de beschikking over de voordelen van openbare Cloud Computing, terwijl aan de specifieke eisen behorende bij de sector wordt voldaan. Ook biedt dit mogelijkheden voor meer lokale aanbieders om dergelijke Clouddiensten aan te bieden.

Aanbeveling 4.3 (aanbieders Clouddiensten). Stimuleer Nederlandse organisaties gebruik te maken van het door de EU beschikbaar gestelde budget voor onderzoek naar Cloud Computing.

Toelichting: Uit onderzoek blijkt dat overheden nog relatief weinig gebruik maken van het door de EU beschikbaar gestelde budget voor onderzoek naar Cloud Computing [R-14].

Aanbeveling 4.4 (afnemers groot/overheid). Geef als overheid het voorbeeld door meer van Clouddiensten gebruik te maken, en maak hierbij eventueel gebruik van ervaring opgedaan door overheden in andere landen.

Toelichting: Vanuit de concurrentiepositie vanuit Nederland is het sowieso verstandig goed in de gaten te houden wat met name de Europese landen op dit vlak doen. Toch zijn ook verder weg (bijv. in Japan) interessante voorbeelden te vinden rondom het stimuleren van Cloud Computing.

7.6 Korte versus lange termijn aanbevelingen

De aanbevelingen kennen verschillende "implementatiesnelheden". Harmoniseren van regelgeving zal nu eenmaal meer tijd vragen dan het starten van voorlichting. In onderstaand overzicht is een onderscheid gemaakt naar aanbevelingen die op relatief korte termijn (1-2 jaar) zijn effect kunnen sorteren en aanbevelingen die op een wat langere termijn (3-4 jaar) effect kunnen sorteren. Bovendien is aangegeven op welke (groep van) actor(en) de aanbeveling het meest betrekking heeft. Het gaat steeds om aanbevelingen voor EL&I, echter welke (groep van) actor(en) naar aanleiding van een aanbeveling het meeste werk moet verzetten verschilt.

	KT: Korte termijn (2013/2014)	LT: Langere Termijn
EU / Internationaal		Aanbeveling 2.1
Ministerie EL&I	Aanbeveling 2.2, 2.3	Aanbeveling 3.4
Programma Cloud Computing (DA.nl / PPS)		
Markt – Afnemers klein	Aanbeveling 1.1,	
Markt – Afnemers groot / overheid	Aanbeveling 1.2, 4.4	
Markt - Aanbieders	Aanbeveling 1.3, 3.1, 4.3	Aanbeveling 3.2, 3.3, 4.1, 4.2
Markt - Netwerkaanbieders		

Tabel 2 Samenvatting aanbevelingen

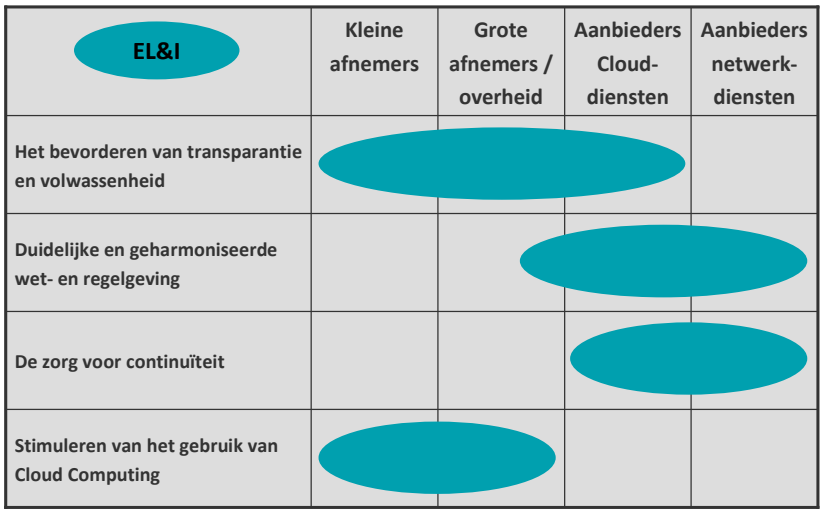
Uit het overzicht blijkt dat er voor EL&I op de korte termijn, er relatief veel aanknopingspunten liggen. Vanuit de ambitie die EL&I heeft op het gebruik van Cloud Computing te stimuleren, en mede gelet op de hoge snelheid waarmee Clouddiensten zich ontwikkelen, ligt het ook voor de hand om niet te lang te wachten.

Bij de totstandkoming van dit rapport is gebleken dat er rondom Cloud Computing, zowel nationaal als internationaal, al heel veel initiatieven lopen. Hierbij is veel aandacht voor de diversiteit aan belemmeringen zoals deze in dit rapport zijn geschetst. Geadviseerd wordt voor aanvang van de uitwerking van een aanbeveling een inventarisatie te maken van de al lopende initiatieven, en hier zoveel als mogelijk bij aan te sluiten.

7.7 Beleidsinstrumentarium

Het ministerie van EL&I heeft een aantal instrumenten beschikbaar om de ontwikkeling van Cloud Computing vorm te geven. Dit zijn algemene beleidsinstrumenten (niet specifiek voor Cloud Computing). Een overzicht is te vinden in bijlage F.

In onderstaand schema is aangegeven op welke doelgroepen de thema's het meest betrekking hebben. Met andere woorden, welke (groep van) actor(en) kan het meest bijdragen aan het wegnemen van belemmeringen binnen dit thema.



Figuur 6 Thema's en doelgroepen

DEEL IV:
BIJLAGEN

A Bronnen

A1. Documentatie

Ref.	Bron
R-1	Special Publication 800-145, The NIST Definition of Cloud Computing (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)
R-2	J. van Hoof, 'Cloud Computing: Het concept ontrafeld'
R-3	http://news.cnet.com/8301-13772_3-20114975-52/microsoft-aiming-to-clean-up-hotmail-users-inboxes/ op 28 november 2011 geraadpleegd
R-4	Etro, F. The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe Review of Business and Economics 2009
R-5	Cloud Computing voor de Nederlandse overheid, oktober 2010, KPMG
R-6	Digitale agenda voor Europa
R-7	Eurocommissaris Kroes, Towards a European Cloud Computing Strategy, World Economic Forum, 2011
R-8	Digitale Agenda.NL
R-9	Prospectief marktonderzoek zakelijke markt, april 2011, Roland Berger Strategy Consultants in opdracht van OPTA
R-10	Bronnen: (1) Digitale Agenda.nl, hoofdstuk 5; (2) ICT~Kwartaalmonitor, Augustus 2011, door ICT~Office
R-11	Gartner nieuwsbericht 30 juni 2011, http://www.gartner.com/it/page.jsp?id=1735214
R-12	ICT~Office, http://www.ictoffice.nl/index.shtml?id=10377&ch=ICT
R13	Artikel over onderzoek door Forrester research: http://www.informationweek.in/Cloud_Computing/11-04-26/Forrester_forecasts_USD_241_billion_cloud_computing_market_by_2020.aspx
R-14	Roland Berger, Survival of the Fittest, How Europe can assume a leading role in the cloud
R-15	Persbericht in de Computable, 29-08-2011, http://www.computable.nl/artikel/ict_topics/cloud_computing/ 4114875/2333364/verizon-versterkt-terremark-met-cloudswitch.html
R-16	Bloomberg, http://gigaom.com/cloud/microsoft-plans-8-6b-in-cloud-rd-but-where-should-it-go/
R-17	http://www.successfactors.com, geraadpleegd op 5 december 2011
R-18	Artikel "Facebook kent geen uitgang" van Danny Mekic, NRC Weekend 26/27 november
R-19	ANP persbericht van 29 november 2011, http://www.nu.nl/tech/2680768/zweden-getroffen-enorme-datastoring.html
R-20	Gartner, Hype Cycle for Cloud Computing, 2011 David Mitchell Smith Publication Date: 27 July 2011
R-21	http://blogs.forrester.com/james_staten/10-11-15-cloud_predictions_for_2011_gains_from_early_experiences_come_alive

Ref.	Bron
R-22	Beveiliging van persoonsgegevens, G.W. van Blarkom en drs. J.J. Borking, nr 23, Registratiekamer april 2001
R-23	http://zoeken.rechtspraak.nl/detailpage.aspx?ljn=BJ5559
R-24	http://ec.europa.eu/information_society/newsroom/cf/pillar.cfm?pillar_id=43&pillar=Digital%20Single%20Market
R-25	http://www.rijksoverheid.nl/onderwerpen/telecomwet-en-regelgeving/bewaarplicht-gegevens-telecommunicatie
R-26	Antwoord van minister Opstelten (Veiligheid en Justitie) op vragen Elissen, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, Aanhangsel Handelingen, vergaderjaar 2010-2011, nr. 3516
R-27	Prof. Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement* Agent, http://ssrn.com/abstract=1781067
R-28	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe, COM(2010) 245
R-29	Robinson, N., Graux, H. Valeri L. et al: (2010) Review of the Strengths and Weaknesses of the European Data Protection Directive 95/46/EC RAND Santa Monica TR-710-ICO
R-30	COM(2012)11 , d.d. 25 januari 2012
R-31	http://www.eurocloud.org/about-eurocloud
R-32	Eurostat newsrelease STAT/10/187, 9 december 2010 http://europa.eu/rapid/pressReleasesAction.do?reference=STAT/10/187&format=HTML&aged=0&language=EN&guiLanguage=en
R-33	Naar Hill en Jones, Strategic Management, sixth edition 2004
R-34	Cloud computing in the public sector: rapid international stocktaking, 2010, RAND Europe
R-35	Roland Berger, Van een fysieke naar een intelligente Digital Gateway to Europe
R-36	http://www.cbpweb.nl/,geraadpleegd op 28 november 2011
R-37	http://www.volkskrant.nl/vk/nl/2664/Nieuws/article/detail/ 1068196/2010/12/04/Kenniseconomie-onder-druk-door-tekort-aan-ict-ers.dhtml
R-38	http://www.reuters.com/article/2011/10/04/us-computing-cloud-survey-idUSTRE7932G720111004

Overige bronnen
Lopend onderzoek van EU-commissie naar omvang en belemmeringen Cloud Computing
Privacy en Cloud Computing, augustus 2010, Elizabeth Thole, van Doorne
Uitgangspunten voor een nationale Cloud agenda, 2011, Stichting Eurocloud Nederland
Cloud Computing, Benefits, risks and recommendations for information security, 2009, Enisa
Security and resilience in Governmental clouds, 2011, Enisa

Overige bronnen
Information Assurance Framework Cloud Computing, 2009, Enisa
Aktionsprogramm Cloud Computing, 2010, BMWi
Presentatie juridische uitdagingen van Cloud Computing, 2010, Van Doorne
De wolk in het onderwijs, privacy aspecten bij Cloud Computing services, 2011, TILT
The Cloud, understanding the security, privacy and trust challenges, 2011, RAND Europe
Opportunities for European Cloud Computing beyond 2010, 2009, Expert Group Report
Motie van der Burg
Kamerbrief-over-cloud-computing
SURF positioning paper
Toespraak Paul Frencken (CBP), Het Outsourcing Congres, PON, 16 juni 2011, Haarlem
Wikipedia http://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size
http://dirkzwagerieit.nl/2011/06/01/deense-privacytoezichthouder-staat-gebruik-google-cloud-niet-toe/, geraadpleegd op 21 december 2011
http://bestconnected.enterprise-ireland.com/peter-fleischer-google-at-the-iiea-cloud-can-be-good-for-privacy/, geraadpleegd op 21 december 2011

A2. Gesprekken

Gesprek met:
Verizon, Michiel de van der Schueren (ook chairman SaaS~Cloud Network, ICT~Office)
Syntens, Monique Fledderman
KPN, Paul Knol & Iris van der Hart
CIO Platform Nederland, Ronald Verbeek
VNO-NCW/MKB, David de Nood
STN, John van der Meulen
BZK, Henri Rauch
Google, Rogier Klimbie
Vopak, Ton van Dijk
Heineken, Jeroen Aris
DHCP, Michiel Steltman

B Wat is Cloud Computing

B1. Definitie

De meest gehanteerde definitie van Cloud Computing is opgesteld door het US National Institute of Standards and Technology (NIST) [R-1] en luidt:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

VKA hanteert voor Cloud Computing de volgende definitie:

> "Cloud Computing is een model voor het snel beschikbaar stellen van on-demand netwerktoegang tot een gedeelde pool van configureerbare IT-middelen (zoals netwerken, servers, opslag, applicaties en diensten), met een minimum aan managementinspanning of interactie met de aanbieder." [R-2]

Kenmerkend voor Cloud Computing is dat IT als dienst wordt afgenomen, deze dienst via het netwerk overal toegankelijk is en gebruik maakt van internetstandaarden waardoor de dienst vanaf elk type randapparatuur met internettoegang te gebruiken is.

B2. Eigenschappen van Cloud Computing

Er worden veel eigenschappen aan Cloud Computing toegedicht. Door het NIST zijn vijf "essentiële" eigenschappen gedefinieerd. Vrij vertaald gaat het om de volgende eigenschappen:

ON-DEMAND SELF-SERVICE

Afnemers kunnen zich (online) aanmelden voor het gebruik van Clouddiensten zonder tussenkomst van medewerkers van de aanbieder. Nadat de afnemer zich door middel van zelfbediening heeft aangemeld kan (vrijwel) direct van de Clouddiensten gebruik gemaakt worden.

GENERIEKE TOEGANG

Voor toegang tot de Clouddienst wordt gebruik gemaakt van standaard internetprotocollen zodat vanaf elke locatie, en in principe los van het type randapparatuur (laptop, tablet, smartphone, etc.), toegang tot de dienst beschikbaar is.

DELEN VAN MIDDELEN

De middelen (servers, opslag, netwerk) van de aanbieder van Clouddiensten worden gedeeld door meerdere afnemers. Het, op aanvraag, fysiek en/of virtueel toewijzen van middelen aan een afnemer gebeurt dynamisch, veelal zonder dat de afnemer weet waar de middelen zich (fysiek)

bevinden. Dit delen van middelen tussen verschillende afnemers wordt ook wel "Multi-tenant" of "Multi-tenacy" genoemd.

HOGE MATE VAN ELASTICITEIT

De capaciteit van een Clouddienst kan op verzoek van de afnemer, meestal automatisch, direct worden uitgebreid of juist weer worden vrijgegeven. Dit naar boven en beneden schalen van de benodigde middelen stelt de afnemer in staat alleen die capaciteit af te nemen, en te betalen, die strikt noodzakelijk is. Voor de afnemer lijkt het alsof een ongelimiteerde hoeveelheid middelen ter beschikking staat.

GEBRUIK IN MEETBARE EENHEDEN

Clouddiensten worden aangeboden en afgenomen, en in het algemeen afgerekend, in eenheden die passen bij het type dienst. Deze eenheden zijn meetbaar, controleerbaar en rapporteerbaar. Voorbeelden van meetbare eenheden zijn Gbytes (opslagcapaciteit), het aantal actieve gebruikersaccounts, de verwerkingscapaciteit per uur of Mbps (bandbreedte).

De eigenschappen van Cloud Computing leiden tot verschillende (potentiële) voordelen voor afnemers van deze diensten:

- Een hoge mate van flexibiliteit met betrekking tot de afname, en betaling, van IT;
- Verschuiving van investering- (CAPEX) naar exploitatiekosten (OPEX);
- Snelle ontwikkeling van nieuwe dienstverlening (innovatie) en minder risico ten aanzien van nieuwe investeringen in IT;
- Lagere kosten;
- Verlaging van de beheersinspanning.

B3. Verschillende soorten Cloud Computing diensten

In het algemeen worden drie soorten Cloud Computing diensten onderscheiden:

SOFTWARE-AS-A-SERVICE, SAAS

Veel Cloud Computing diensten vormen voor een afnemer een kant-en-klare toepassing (applicatie). Voorbeelden zijn toepassingen voor CRM, kantoorautomatisering, boekhouding etc.. Afnemers gebruiken de standaard functionaliteit zoals die door de aanbieder van de SaaS-dienst wordt aangeboden. De volledige verantwoordelijkheid voor de toepassing, en alle onderliggende hard- en software, ligt bij de aanbieder van de dienst. In veel gevallen maakt een aanbieder van SaaS-diensten op haar beurt weer gebruik van één of meer onderliggende Clouddiensten zoals PaaS en/of IaaS. Voorbeelden van Saas-diensten zijn Salesforce.com, Google Apps en Exact Online.

PLATFORM-AS-A-SERVICE, PAAS.

Een aantal grote aanbieders van Clouddiensten, zoals Microsoft, Amazon en Google, bieden een ontwikkelplatform aan in de vorm van een Clouddienst. Het ontwikkelplatform bevat een verzameling standaard services op basis waarvan een ontwikkelaar snel (eigen) (web)toepassingen kunnen ontwikkelen. Met andere woorden, PaaS diensten stelt organisaties in staat snel nieuwe (web)toepassingen te ontwikkelen. De uiteindelijke applicatie blijft daarmee een eigen

verantwoordelijkheid van de afnemer, terwijl het onderliggende platform (services en verwerkings- en opslagcapaciteit) een verantwoordelijkheid is van de aanbieder van de Clouddienst. Voorbeelden van PaaS diensten zijn Microsoft Azure, Google App Engine, Force.com en Amazon Web Services (AWS).

INFRASTRUCTURE-AS-A-SERVICE, IAAS

De meest "kale" vorm van Cloud Computing is Infrastructure-as-a-Service (Iaas). Bij IaaS is het de verwerkingscapaciteit (een virtuele server) en/of opslagcapaciteit dat als dienst wordt aangeboden. Door verwerkings- en opslagcapaciteit als dienst af te nemen investeert de afnemer niet in eigen IT hardware. Het plaatsen van toepassingen of gegevens op de afgenomen verwerkings- en/of opslagcapaciteit is een volledige verantwoordelijkheid van de afnemer, terwijl de aanbieder verantwoordelijk is voor de onderliggende infrastructuur zoals servers en systemen voor opslag van gegevens. Voorbeelden van IaaS diensten zijn Amazon EC2, Terremark, Dropbox en Rackspace Cloud Servers.

B4. Openbare, Private en Community Clouds

De meest ultieme vorm van Cloud Computing staat bekend als "Public" of "Openbare" Cloud Computing[19] [20]. Openbare Clouddiensten zijn voor iedereen toegankelijk. De benodigde infrastructuur is onzichtbaar voor de afnemer, bevindt zich op locatie(s) van de aanbieder(s) van de dienst en wordt met andere afnemers gedeeld.

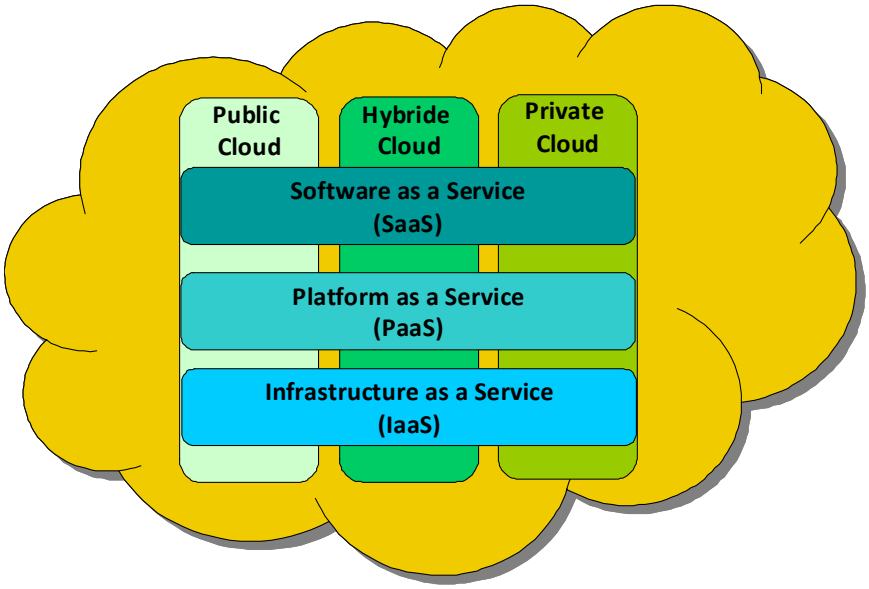
Tegenover Openbare Cloud Computing staat Private Cloud Computing. Bij Private Cloud Computing is sprake van een aparte, gesloten Cloudinfrastructuur ten behoeve van één afnemer. De gebruikte IT-middelen en toepassingen zijn alleen door de eigen organisatie te gebruiken. Deze aparte Cloudinfrastructuur kan in eigendom en beheer zijn van de organisatie zelf, een derde partij of een combinatie van beide, en kan fysiek "on-premise" of "off-premise" zijn geplaatst.

Tussen de twee uiterste implementatiemodellen Openbare en Private Cloud zit nog een derde vorm: Community Cloud. Een Community Cloud is een aparte Cloudinfrastructuur ten behoeve van een specifieke groep van organisaties die een gemeenschappelijk belang hebben. De betreffende Community Cloud voldoet aan de specifieke eisen die door de deelnemende organisaties aan de Cloud worden gesteld. Voorbeelden van groepen met een gemeenschappelijk belang zijn onderwijsorganisaties, overheid en zorginstellingen.
De Community Cloudinfrastructuur kan in eigendom en beheer zijn van één of meer van de deelnemende organisaties, een derde partij of een combinatie van beide. De fysieke middelen waarmee de Community Clouddienst wordt aangeboden bevinden zich op locatie bij één of meer van de deelnemende organisaties of bij een derde partij.

[19] Naar de Public Cloud zoals gedefinieerd door de NIST wordt in dit rapport verwezen als Openbare Cloud.

[20] Ter voorkoming van verwarring, de term Public Clouddiensten verwijst hier niet naar de Clouddiensten binnen de overheid. Naar de Cloud van de overheid wordt in dit rapport verwezen als Overheidscloud, overeenkomstig de brief van minister Donner aan de tweede kamer, gedateerd 20 april 2011.

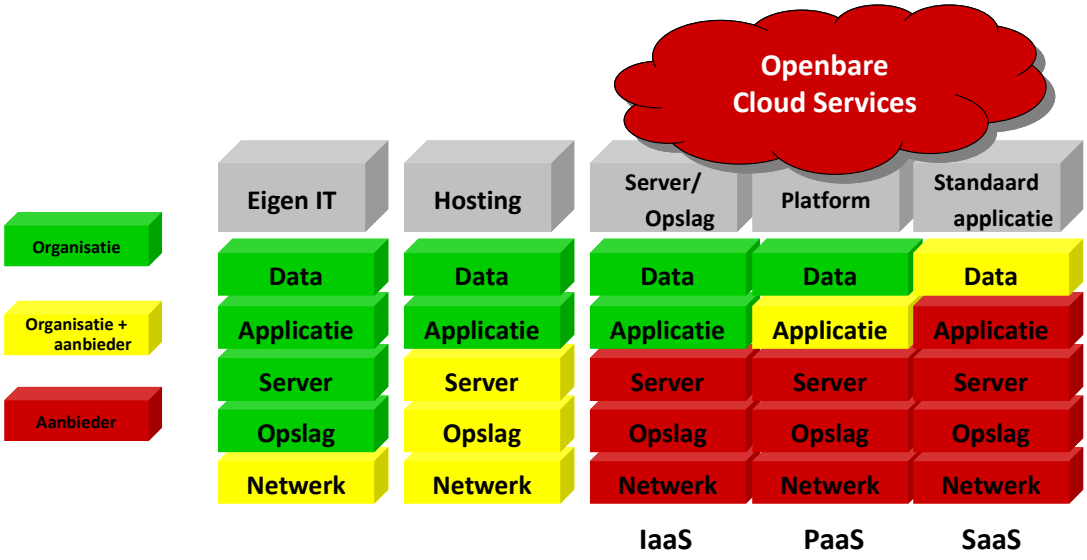
Er bestaan ook Cloudinfrastructuren die bestaan uit een combinatie van een verschillende Cloudinfrastructuren (Openbare, Private en/of een Community). Zo kunnen bijvoorbeeld toepassingen in een Private Cloud voor de opvang van piekbelastingen op het systeem tijdelijk middelen uit de Openbare Cloud bijschakelen.



Figuur 7 Verschillende vormen van Cloud Computing

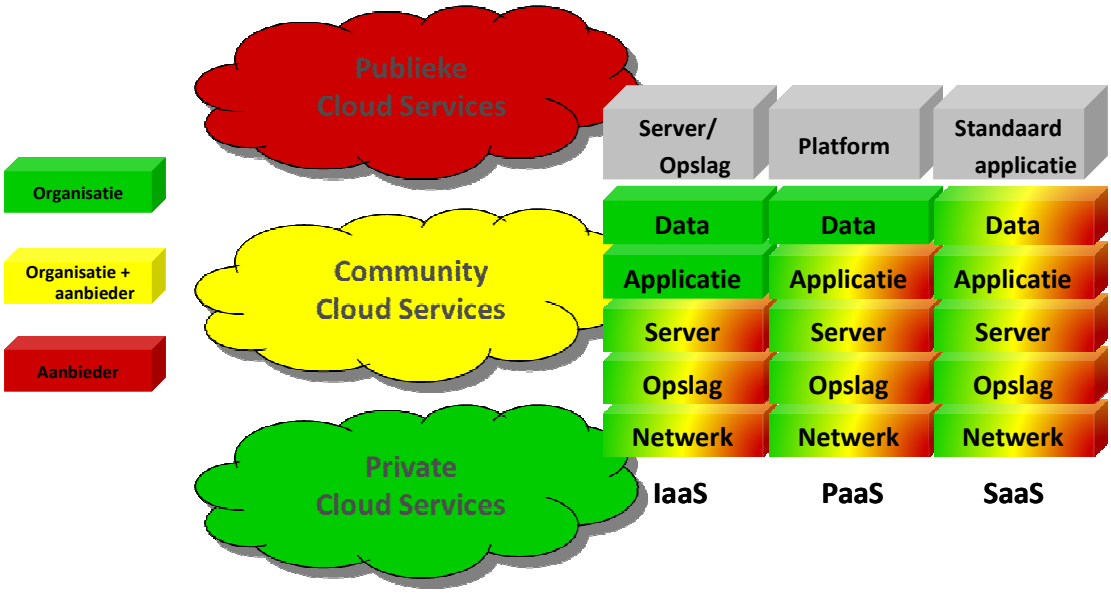
B5. De mate van invloed op verschillende soorten Clouddiensten

Zoals in de vorige paragrafen beschreven bestaan er meerdere soorten Clouddiensten (SaaS, PaaS en IaaS) die op verschillende manier kunnen worden aangeboden: in de vorm van een Openbare, Community of Private Cloud. Zowel het soort Clouddienst als de vorm waarin de dienst wordt aangeboden hebben invloed op de mate waarin de afnemer invloed heeft op de dienst. Figuur 2 en 3 geven een en ander schematisch weer, waarbij groen aangeeft dat de afnemer volledige invloed, geel een gedeelte verantwoordelijkheid (met andere woorden beperkte invloed) en rood betekent dat de afnemer niet of slechts in zeer beperkte mate invloed heeft (op aspecten als iniformatiebeveiliging, kwaliteit van dienstverlening, functionaliteit, etc.). Naarmate de afnemer meer invloed heeft (IaaS) neemt het risico af, dat wil zeggen het risico is volledig door de afnemer zelf te beheersen.



Figuur 8. Mate van invloed op IaaS, PaaS en SaaS diensten

Verschillende soorten Clouddiensten hebben een verschillende risicoprofiel. Dit is relevant bij de interpretatie van de in dit rapport geschetste belemmeringen en risico's. Deze zijn niet op alle soorten Clouddiensten in gelijke mate van toepassing. Sommige belemmeringen die zich bij SaaS diensten manifesteren, bijvoorbeeld geen of beperkte invloed op functionaliteit, doen zich bij andere soorten Clouddiensten, in dit voorbeeld bij IaaS, helemaal niet voor. Dit geldt ook voor het onderscheid tussen Openbare, Community en Private Clouddiensten, waarbij in het laatste geval een afnemer volledige controle heeft over alle lagen waaruit de dienst is opgebouwd (figuur 3).



Figuur 9. Verschil in invloed tussen een Openbare, Community en Private Cloud

C Begrippen (in WBP)

Voor een goed inzicht is het belangrijk de betekenis van een aantal begrippen uit de WBP nader toe te lichten [R-36]:

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens zijn alle gegevens die iets over u zeggen of die van invloed kunnen zijn op de manier waarop u wordt beoordeeld of behandeld. Dat kunnen dus zijn uw naam, uwgeboortedatum en uw adres, maar ook uw banksaldo, uw beroep en het kentekennummer van uw auto. Wel moet degene op wie de gegevens betrekking hebben te identificeren zijn.

Bijzondere gegevens
Dat zijn gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijk verleden. Financiële gegevens zijn voor de wet dus niet 'bijzonder'.

Verwerking van persoonsgegevens
Dat is elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Dit omvat alle handelingen met die gegevens vanaf het moment van het verzamelen tot en met het vernietigen ervan.

Verantwoordelijke
De verantwoordelijke is de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Kort gezegd: degene die voor eigen doeleinden persoonsgegevens verwerkt.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.

Bewerker
Een bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, maar niet rechtstreeks valt onder het gezag van de verantwoordelijke. Een voorbeeld van een bewerker is een verzendhuis dat namens een andere organisatie folders verstuurt. Om de folders te versturen krijgt het verzendhuis de adressen, maar wordt geen eigenaar van het adressenbestand. Het verzendhuis voert alleen maar een opdracht uit. De verantwoordelijkheid voor de verwerking kan niet overgedragen worden.

Doel
Om het verzamelen van persoonsgegevens een rechtmatige basis te geven dient de verantwoordelijke vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen te hebben bepaald. Alleen onder strikte voorwaarden mogen de verzamelde gegevens ook voor

andere doeleinden gebruikt worden dan waarvoor ze oorspronkelijk verzameld zijn. Dat kan alleen als dat gebruik niet op gespannen voet staat met het oorspronkelijke doel.

Grondslag

Om verzamelde persoonsgegevens verder te mogen verwerken dient een wettelijke grondslag aanwezig te zijn. Deze kan bestaan uit bijvoorbeeld de toestemming van de betrokkene, de noodzaak voor de uitvoering van een contract of voor het nakomen van een wettelijke verplichting.

D Nationaal Continuïteitsoverleg – Telecommunicatie (NCO-T)

Het Nationaal Continuïteitsoverleg – Telecommunicatie, kortweg NCO-T, vindt zijn oorsprong in artikel 14.6 van de Telecommunicatiewet. Dit artikel geeft de mogelijkheid aanbieders van openbare telecommunicatiediensten en/of -infrastructuur aan te wijzen die voorbereidingen moeten treffen om de telecommunicatie in stand te houden tijdens een Buitengewone Omstandigheid, wat in de spreektaal meestal aangeduid wordt als de noodtoestand.

Het in aanmerking komen voor aanwijzing geschied op basis van de volgende criteria:
- het beschikken dan wel in direct beheer hebben van eigen infrastructuur;
- het leveren van een als vitaal aangemerkte openbare telecommunicatiedienst en/of -infrastructuur;
- het hebben van een zeker marktaandeel voor de als vitaal aangemerkte openbare telecommunicatiedienst en/of -infrastructuur;

Op dit moment (december 2011) zijn 6 aanbieders aangewezen: KPN, Tele2, T-Mobile, UPC, Vodafone, Ziggo.

In de bij artikel 14.6 behorende Ministeriële Regeling Buitengewone Omstandigheden Telecom 2007 is aangegeven dat één van de voorbereidingen is het deelnemen aan door de overheid ingesteld overleg. Het NCO-T is een dergelijk overleg, ingesteld via Instellingsbesluit NCO-T 2007.

Lidmaatschap van het NCO-T is verplicht, deelname niet. Echter, in het NCO-T gemaakte afspraken gelden voor iedere aangewezen aanbieder. Het voorzitterschap en secretariaat worden door het ministerie van EL&I vervuld. De werkwijze van het NCO-T is werken via consensus en op basis van een verklaring van vertrouwelijkheid.

Het doel van het NCO-T is dat overheid samen met de aanbieders:
- preventieve maatregelen opstellen om ernstige verstoring of uitval van openbare communicatienetwerken en -diensten te voorkomen;
- maatregelen treffen om een eventuele verstoring of uitval zo snel mogelijk en met zo weinig mogelijk schade aan vitale belangen te verhelpen.

In het NCO-T worden afspraken gemaakt over de verplichtingen die voor deze aanbieders volgen uit de Telecommunicatiewet, met name uit artikel 14.6. Dit zijn verplichtingen op het gebied van continuïteitsplanning en crisismanagement. Daarbij wordt zo veel als mogelijk en wenselijk is aangesloten bij de maatregelen die de bedrijven zelf vanuit de strategie m.b.t. hun bedrijfscontinuïteit reeds getroffen hebben.

Daarnaast krijgen de deelnemers aan het NCO-T de gelegenheid mee te denken over beleidskwesties op het gebied van vitale elektronische communicatiediensten en -infrastructuur. Zo kan onnodige regelgeving worden voorkomen of zo nodig op adequate wijze worden vorm gegeven.

Van een Buitengewone Omstandigheid zal niet vaak sprake zijn, maar de gemaakte afspraken zijn ook bruikbaar bij kleinere incidenten of crises. Om deze reden worden de afspraken ook tijdens deze responssituaties gevolgd.

Op deze wijze werken in het NCO-T de aanbieders samen met het ministerie van EL&I om de kwetsbaarheid van vitale telecommunicatie infrastructuur/-diensten te verminderen. Door o.a. onderling afspraken te maken over basisvoorzieningen en door deelname vanuit het NCO-T aan activiteiten die uitgevoerd worden in het kader van de Strategie Nationale Veiligheid, Nationale Crisismanagement structuur, de Nationale Cyber Security Strategie, de Nationale Risicobeoordeling, etc etc.

E Totaaloverzicht van belemmeringen

Dit hoofdstuk bevat een volledig overzicht van de belemmeringen die uit de geraadpleegde documentatie (bijlage A1) en de gevoerde gesprekken (bijlage A2) naar voren zijn gekomen. Het betreft (gepercipieerde) belemmeringen die afnemers mogelijk weerhouden gebruik te maken van Cloud Computing. De belemmeringen zijn beschreven vanuit het perspectief van de afnemer, wat niet betekent dat deze belemmeringen ook niet op aanbieders van toepassing kunnen zijn. Sommige belemmeringen hebben betrekking op zowel afnemers als aanbieders.

In het totaaloverzicht staan ook een aantal meer specifieke belemmeringen afkomstig van de aanbieders van Cloud Computing (of netwerk)diensten. Naar de mening van de aanbieders remmen deze belemmeringen de ontwikkeling van de (Nederlandse) markt voor Cloud Computing.

De belemmeringen zijn in de volgende zeven paragrafen beschreven;
1. Informatiebeveiliging (waaronder betrouwbaarheid/integriteit data).
2. Compliance / Privacy.
3. Business continuïteit (waaronder beschikbaarheid dienst/dienstverlener).
4. Integratie en standaarden.
5. Markt (aanbod, perceptie, vertrouwen).
6. Business Case.
7. Overig.

Wellicht ten overvloede wordt opgemerkt dat de belemmeringen niet (in dezelfde mate) op elke Clouddienst van toepassing zijn. Tussen SaaS-, PaaS- en IaaS-diensten kunnen grote verschillen zitten. Voorzichtigheid is geboden niet alles over één kam te scheren.

Om de komen tot een goede samenvatting van de belangrijkste belemmeringen is gekeken naar;
- Welke belemmeringen zijn in de kern terug te voeren tot eenzelfde (achterliggende) probleem.
- Kan EL&I op de een of andere manier (via directe en/of indirecte maatregelen die zij zelf inzet of waarop zij op een of andere manier en met redelijkerwijs te verwachten resultaat) iets bijdragen aan het wegnemen of verminderen van de belemmering.
- Heeft de belemmering specifiek betrekking op Cloud Computing, of heeft het een meer generiek karakter dat ook bij al langer bestaande wijzen van IT-dienstverlening voorkomt.

In de samenvatting zijn de belemmeringen uiteindelijk ingedeeld in een vijftal clusters; zie hiervoor hoofdstuk 6.

E1. A. Informatiebeveiliging

BA-1. IS DE BESCHERMING VAN DATA GEWAARBORGD?

Bij gebruik van Cloud Computing wordt de data van de afnemer opgeslagen in "de Cloud". De zorg voor een adequate beveiliging van deze data ligt nu bij de aanbieder van de Clouddienst. Afnemers maken zich zorgen of de aanbieder voldoende maatregelen heeft getroffen om de data te

beschermen tegen ongeautoriseerde toegang en manipulatie en besmetting door virussen, malware etc..

BA-2. ONDUIDELIJKHEID OMTRENT HET EIGENAARSCHAP VAN GEGEVENS.

Omdat bij gebruik van Clouddiensten de data wordt opgeslagen bij de aanbieder van de Clouddienst kan onduidelijkheid ontstaan over het eigendom (afnemer, aanbieder of beide?) van de opgeslagen gegevens. Hoe weet je als afnemer of de aanbieder van Clouddiensten de data ook niet voor andere doeleinden gebruikt? En heb je het recht ten alle tijden over je eigen gegevens te beschikken? Andersom geldt ook voor de aanbieder dat hij niet altijd zicht heeft op de verplichtingen die op hem rusten vanuit de wetgeving in het land waar de dienst wordt afgenomen.

BA-3. WIE IS AANSPRAKELIJK BIJ EEN INBREUK OP DE DATA CONFIDENTIALITEIT.

Mocht er sprake zijn van inbreuk op de (in de Cloud) opgeslagen gegevens, wie is daarvoor dan verantwoordelijk, de afnemer of de aanbieder? Kan je als afnemer de aanbieder hiervoor aansprakelijk stellen?

BA-4. DE AFNEMER WEET NIET WAAR ZIJN GEGEVENS (FYSIEK) STAAN OPGESLAGEN.

Voor veel Clouddiensten geldt dat de afnemer niet weet waar (fysieke locatie) de data in de Cloud is opgeslagen. Dit "gebrek aan controle" vormt voor sommige afnemers een belemmering voor het gebruik van Clouddiensten.

BA-5. HOE WORDT ZEKERGESTELD DAT VERWIJDERDE DATA OOK ECHT HELEMAAL (UIT DE CLOUD) VERDWENEN IS?

Afnemers vragen zich af of er geen "sporen" achterblijven nadat gegevens zijn verwijderd uit de Cloud, of nadat het gebruik van een Clouddienst is stopgezet. Met andere woorden, hoe weet de afnemer dat er niet alsnog misbruik van informatie kan plaatsvinden?

BA-6. HOE KAN DE AFNEMER DE VEILIGHEIDSMAATREGELEN VAN EEN AANBIEDER CONTROLEREN EN TESTEN?

Het is voor afnemers vaak niet duidelijk hoe het veiligheidsniveau dat de aanbieder biedt kan worden gecontroleerd en/of getest. Met andere woorden, heeft de aanbieder de veiligheidsmaatregelen ook daadwerkelijk geïmplementeerd en worden deze regelmatig op kwaliteit getest? Het "Multi-tenancy" aspect van Cloud Computing speelt hierbij een rol. Backup/restore en overschakelen op een uitwijk voorziening kan in een eigen IT omgeving regelmatig worden getest, echter in een Multi-tenancy omgeving is dit minder eenvoudig omdat meerdere afnemers gebruik maken van dezelfde hard- en/of software.

BA-7. ZORGEN OVER DE VEILIGHEID VAN HET GEBRUIK VAN GEDEELDE INFRASTRUCTUUR

Sommige afnemers vragen zich af of het delen van hard- en software ("multi-tenancy") met andere afnemers niet leidt tot additionele veiligheidrisico's, ook als de aanbieder in algemene zin voldoende veiligheidsmaatregelen heeft getroffen. Multi-tenancy is juist één van de specifieke eigenschappen van Cloud Computing. Naar verwachting speelt deze overweging voornamelijk bij grootzakelijke afnemers en overheidsorganisaties. Kleinere afnemers, vaak MKB bedrijven, zijn zich

waarschijnlijk minder of zelfs niet bewust van deze eigenschap van Cloud Computing en de mogelijke additionele risico's die dit met zich meebrengt.

BA-8. IS IDENTITEITS- EN TOEGANGSBEHEER ADEQUAAT?

In een traditionele IT-omgeving is een organisatie volledig zelf verantwoordelijk voor het identiteits- en toegangsbeheer. Bij Cloud Computing ligt op dat terrein een belangrijke verantwoordelijkheid bij de aanbieder van de dienst. Het is uiteindelijk de aanbieder die het technisch beheer voert over het identiteits- en toegangsbeheer met betrekking tot de online dient. Maar hoe weet een organisatie die gebruik maakt van Clouddiensten of het identiteits- en toegangsbeheer voldoende veilig is ingericht? En heeft de organisatie direct invloed op wie toegang heeft tot de dienst zodat bijvoorbeeld in geval van ontslag een medewerker per direct de toegang tot dienst ontnomen kan worden?

BA-9. ONVOLDOENDE TRANSPARANTIE VAN DE AANBIEDER

Een deel van de aanbieders van Clouddiensten geeft geen, of slechts in beperkte mate, inzicht in de beveiligingsmaatregelen die zijn genomen. Ook geven maar weinig aanbieders van Clouddiensten inzicht in de mate waarin deze beveiligingsmaatregelen effectief zijn, met andere woorden, hoe vaak, en welke, veiligheidsincidenten hebben zich voorgedaan. Door veel (potentiële) afnemers wordt het gebrek aan transparantie als één van de grote obstakels gezien. Het belemmert afnemers in de afweging of de geboden beveiligingsmaatregelen aansluiten bij het gewenste niveau.

BA-10. HOE ZIT HET MET EIGENDOM VAN DATA / IPR?

Mede door de vaak ondoorzichtige standaardvoorwaarden die verbonden zijn aan Clouddiensten ontstaan vragen en twijfels over het eigendom van data. Behoudt een afnemer het volledig eigendom over zijn gegevens wanneer deze worden overgeheveld naar de Cloud? Is het intellectueel eigendom (IPR) voldoende gewaarborgd? Hoe weet je of de standaardvoorwaarden voldoende bescherming bieden? Grootzakelijke afnemers en overheidsorganisaties beschikken in het algemeen over voldoende juridische kennis, of hebben de middelen deze in te huren, om op deze vragen een goed antwoord te kunnen formuleren. Dit in tegenstelling tot het MKB en startende ondernemers waar (juridische) kennis en middelen vaak ontbreken om vragen rondom data en intellectueel eigendom te kunnen beantwoorden.
De vraag rondom intellectueel eigendom wordt nog gecompliceerder wanneer informatie "in, of door middel van de Cloud" tot stand is gekomen.

BA-11. KUNNEN OVERHEDEN VAN ANDERE (NIET-EU) LANDEN MIJN INFORMATIE INZIEN?

Eén van de meest besproken thema's rondom Cloud Computing is toegang tot opgeslagen informatie door andere overheden. Cloud Computing heeft als eigenschap locatieonafhankelijkheid; het maakt voor de afnemer (functioneel) niet uit waarvandaan de Clouddiensten worden geleverd. Aanbieders van Clouddiensten, en de rekencentra waar de data is opgeslagen, kunnen in principe overal ter wereld zijn gevestigd. Dit roept bij afnemers vragen op over de mogelijkheden die overheden hebben zich toegang te verschaffen tot de binnen de landsgrenzen gevestigde aanbieders van Clouddiensten en/of de hier opgeslagen informatie.

In het bijzonder wordt vaak gewezen op de USA PATRIOT Act[21], ofwel de mogelijkheden die de Amerikaanse overheid zou hebben om zich toegang te verschaffen tot informatie opgeslagen in de Cloud. Veel aanbieders van Clouddiensten zijn immers Amerikaanse bedrijven, vaak met rekencentra in de Verenigde Staten (of andere landen buiten Nederland).
Het vraagstuk van toegang tot informatie door overheden van andere landen speelt voornamelijk bij afnemers binnen het publieke domein (zorg, overheid). Het MKB en grootzakelijke afnemers zien dit in het algemeen in mindere mate als belemmering.

E2. B. Compliance / Privacy

BB-1. HOE TE VOLDOEN AAN DE PRIVACY WETGEVING?

Zonder meer, één van de meest besproken onderwerp in relatie tot Cloud Computing is privacy. Veel organisaties leggen informatie vast over personen (klanten, relaties, medewerkers, etc.) en zijn hierdoor gehouden aan de Wet Bescherming Persoonsgegevens, de WBP. Deze wet schrijft onder meer voor dat organisaties bij uitbesteding van de verwerking van persoonsgegevens zorgen voor een 'bewerkersovereenkomst', en toezien op naleving van de afgesproken beveiligingsmaatregelen. Er bestaat veel onduidelijkheid bij afnemers hoe, bij toepassing van Cloud Computing, kan worden voldaan aan deze eisen. Voor veel afnemers is dit dé reden om geen gebruik te maken van Clouddiensten.

BB-2. WET- EN REGELGEVING VARIEERT PER LAND (OOK BINNEN DE EU)

Tussen landen, ook binnen de EU, verschilt wet- en regelgeving (bijvoorbeeld op het gebied van privacy, dataretentie, etc.). Omdat Cloud Computing locatieonafhankelijk en grensoverschrijdend is, vormen deze verschillen tussen landen een belemmering voor de ontwikkeling en het gebruik van Clouddiensten. Zowel aanbieders van Clouddiensten als internationaal opererende afnemers zien de verschillen in wet- en regelgeving als één van de grootste belemmeringen voor de ontwikkeling van Clouddiensten.

BB-3. IS DE TELECOMMUNICATIEWET VAN TOEPASSING OP AANBIEDERS VAN CLOUDDIENSTEN?

Sommige Clouddiensten bevatten functies waarmee informatie niet alleen wordt bewerkt of opgeslagen, maar ook (actief) wordt doorgestuurd naar andere personen of organisaties. De aanbieder van deze Clouddiensten lijkt hiermee op een aanbieder van telecommunicatiediensten die zich ook met het doorgeven van informatie bezighoudt. De vraag is of dergelijke aanbieders daarmee gekwalificeerd kunnen worden als aanbieders van elektronische communicatienetwerken of –diensten, of zelfs als aanbieder van openbare telecommunicatienetwerken of –diensten, en daarmee onder het bereik van de Telecommunicatiewet vallen. Het voldoen aan de telecommunicatiewet kan van invloed zijn op aanbieders van Clouddiensten.

[21] Voluit de Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, Public Law 107-56) is in 2003 door het Amerikaans Congres aangenomen.

BB-4. WETGEVING SCHRIJFT VOOR DAT (OVERHEIDS)GEGEVENS BINNEN DE NL-GRENZEN BLIJFT

Er bestaat bij verschillende afnemers onduidelijkheid of informatie van organisaties verplicht op Nederlands grondgebied moet worden verwerkt en opgeslagen. Dit speelt met name in het publieke domein (zorg, overheid).
Omdat bij Clouddiensten informatie vaak buiten Nederland wordt verwerkt en/of opgeslagen, of omdat niet bekend is in welk(e) land(en) informatie zich bevindt, vormt deze onduidelijkheid een belemmering om van Clouddiensten gebruik te maken. De vraag of een dergelijke wettelijke verplichting bestaat voor organisaties staat nog los van de vraag of het wenselijk is dat dergelijke informatie in het buitenland wordt opgeslagen.

BB-5. KAN JE ALS ORGANISATIE VOLDOEN AAN AL JE WETTELIJKE VERPLICHTINGEN?

In belemmering BB-1 is al ingegaan op een specifieke wettelijke verplichting, de WBP. Er zijn echter meer verplichtingen waaraan organisaties moeten voldoen en die bij het gebruik van Clouddiensten vergelijkbare vragen oproepen als besproken bij het voldoen aan de WBP. Denk hierbij aan regels als IFRS, SOx, Tabaksblatt, wetgeving op de jaarrekening, bewaarplichten en in de toekomst de wettelijke Meldplicht van privacy-inbreuken. Afnemers, maar ook aanbieders van Clouddiensten staan voor de vraag hoe te voldoen aan de wettelijke verplichtingen.
Onduidelijkheid vormt een belemmering voor het aanbieden en gebruiken van Clouddiensten.

BB-6. TOEPASSELIJK RECHT

Clouddiensten kunnen aangeboden worden zonder dat de aanbieder in Nederland gevestigd is of een Nederlandse vestiging heeft. Het land waar de aanbieder van een Clouddienst de informatie verwerkt en opslaat kan vervolgens nog weer afwijken van het land waar de aanbieder gevestigd is. Daarboven komt nog dat veel Clouddiensten weer gebruik maken van andere Clouddiensten, bijvoorbeeld door gebruik te maken van verwerkings- en opslagcapaciteit van een andere aanbieder (IaaS). Het grenzenloze karakter van Clouddiensten leidt bij afnemers tot de vraag onder welke jurisdictie de aangeboden dienst valt.

BB-7. AANSPRAKELIJKHEID (IN GRENSOVERSCHRIJDENDE SITUATIES) IS ONDUIDELIJK

Bij het gebruik van Clouddiensten kan onduidelijkheid ontstaan over aansprakelijkheid. Eén van de aspecten heeft te maken met het toepasselijk recht, zie de vorige belemmering, BB-6. Een ander aspect betreft het vaak ontbreken van een rechtstreekse (fysieke) koppeling met de aanbieder van de Clouddienst. Voor toegang tot de Clouddienst wordt vaak gebruik gemaakt van het Internet als transport medium. Het Internet bestaat vervolgens weer uit een aaneenschakeling van netwerken van verschillende telecommunicatieaanbieders.
Er is niet één partij die door de afnemer van een Clouddienst aangesproken kan worden op de "end-to-end" beschikbaarheid en performance van de dienst. Dit kan leiden tot onduidelijkheid over wie aansprakelijk is, bijvoorbeeld wanneer beschikbaarheid en performance achterblijven bij de verwachtingen van de afnemer.

BB-8. OVERHEIDSDATA OPGESLAGEN/VERWERKT BUITEN DE LANDSGRENZEN DOOR PRIVATE PARTIJEN VALT ONDER BUITENLANDSE WETGEVING. DIT IS NIET ACCEPTABEL.

Organisaties binnen het publieke domein zien als belemmering voor het gebruik van Clouddiensten de verwerking en opslag van gegevens in landen buiten Nederland, waarop

buitenlandse jurisdictie van toepassing is. Organisaties binnen de publieke sector vinden de bescherming van "overheidsdata" in de Cloud onvoldoende.

BB-9. HOE TE VOLDOEN AAN DE AANKOMENDE WETGEVING MET BETREKKING TOT DE MELDPLICHT?

Naar verwachting komt er een wettelijke meldplicht van inbreuken op privacy en veiligheid. Aanbieders van Clouddiensten waarop deze verplichting van toepassing is zullen maatregelen moeten treffen om aan de meldplicht te kunnen voldoen. Mocht de wet het karakter krijgen van een algemene meldplicht, dan zou deze op alle bedrijven en overheidsdiensten van toepassing zijn. Bij het gebruik van Clouddiensten heeft de afnemer niet direct zicht op mogelijke privacy-inbreuken. Verwerking en opslag van gegevens vindt plaats bij de dienstenaanbieder. Het moeten voldoen aan de meldplicht kan door afnemers worden ervaren als een belemmering voor het gebruik van Clouddiensten.

BB-10. HOE TE VOLDOEN AAN ARTIKEL 33 WBP / ART. 10 EUROPESE DATAPROTECTIERICHTLIJN?

Op grond van artikel 33 van de Wet bescherming persoonsgegevens / artikel 10 van de Europese dataprotectierichtlijn dient een afnemer van Clouddiensten (als verantwoordelijke volgens de WBP) nadere informatie te verstrekken over de ontvangers van de gegevens en de aard van de gegevensverwerking. Dit is vooral van toepassing als een belangrijk deel van de gegevensverwerking buiten de EU plaatsvindt. Een afnemer moet in dat geval zijn gebruikers (de "betrokkenen" volgens de WBP) nader informeren over de doorgifte van informatie. Dit kan een belemmering vormen voor afnemers van Clouddiensten omdat veel aanbieders van Clouddiensten datacenters hebben buiten de EU of omdat de afnemer bij gebruik van Clouddiensten niet weet waar de gegevens worden verwerkt/opgeslagen.

BB-11. GEEN OF SLECHTS BEPERKTE RIGHT-TO-AUDIT

Standaard voorzien aanbieders van Clouddiensten in het algemeen niet, of slechts beperkt, in mogelijkheden voor afnemers om audits uit te (laten) voeren. Het ontbreken van een right-to-audit, in combinatie met de vaak gebrekkige transparantie van aanbieders over informatiebeveiliging en geleverde prestaties, kan voor afnemers een belemmering vormen voor het gebruik van Clouddiensten.

BB-12. ONVOLDOENDE (/GEEN) ASSURANCEVERKLARINGEN EN/OF CERTIFICERING

Niet alle aanbieders van Clouddiensten beschikken over (voldoende) assuranceverklaringen en/of certificeringen. Voorbeelden van dergelijke verklaringen zijn SAS70-type I en II, ISAE3402/SSAE-Type A en B, etc.. Het ontbreken van assuranceverklaringen en/of certificering belemmert afnemers te voldoen aan wettelijke verplichtingen. Ook ontbreekt het de afnemer hierdoor aan inzicht in de mate waarin de aanbieder voldoet aan gemaakte afspraken of gedane belofte, bijvoorbeeld met betrekking tot informatiebeveiliging.

E3. C. Business continuïteit

BC-1. GARANTIES OVER VOORTBESTAAN VAN DE DIENST (BIJVOORBEELD BIJ EXIT/INSOLVENTIE)

Cloud Computing is een relatief nieuw fenomeen dat nog volop in beweging is. Innovaties volgen elkaar snel op. Ook blijkt dat diensten snel kunnen groeien, maar ook in korte tijd weer snel kunnen verdwijnen of sterk krimpen (bijvoorbeeld Secondlife). Ditzelfde geldt voor aanbieders van Clouddiensten. Deze snel veranderende omgeving, gecombineerd met de afhankelijkheid van een Clouddienst, vormt voor potentiële afnemers een belemmering voor het gebruik van deze diensten. Dit geldt vooral voor SaaS-diensten. Een afnemer heeft nauwelijks garanties rondom het voortbestaan van een Clouddienst, terwijl het wegvallen van deze dienst grote gevolgen kan hebben voor de continuïteit van de bedrijfsvoering.
Er is ook geen standaard vangnet in geval van faillissement van de aanbieder. Bij de traditionele toepassing van IT bleef de eigen IT omgeving doordraaien in het geval een leverancier van software failliet ging. Eventueel kon de broncode veiliggesteld worden door middel van een Escrow-regeling. Dit ligt anders in het geval van Clouddiensten waardoor de impact van een faillissement van de aanbieder, of het om een andere reden stopzetten van een Clouddienst door de aanbieder, direct gevolgen kan hebben voor de bedrijfsvoering van de afnemer.

BC-2. ZIJN MIJN GEGEVENS TE ALLEN TIJDE VOOR MIJ TOEGANKELIJK?

Beschikbaarheid heeft ook te maken met het te allen tijde toegang hebben tot de eigen gegevens. In belemmering BC-1 ging het hierbij om het volledig wegvallen van een dienst. Maar er zijn ook andere situaties denkbaar waarin de afnemer zeker wil weten dat de toegankelijkheid tot zijn eigen gegevens is gewaarborgd. Bijvoorbeeld bij een geschil tussen aanbieder en afnemer. Of omdat afnemer niet tevreden is met de geleverde prestaties. Afnemers vragen zich af of zij het recht hebben altijd over de eigen gegevens te kunnen beschikken.

BC-3. KAN DE OPGESLAGEN DATA SNEL, EN IN EEN STANDAARD (/BRUIKBAAR) FORMAAT WORDEN WEGGEHAALD?

Behalve de vraag of de eigen gegevens altijd toegankelijk zijn, is er de vraag in hoeverre de aanbieder aan afnemers de mogelijkheid biedt om snel, en in een standaard (/bruikbaar) formaat, alle eigen gegevens uit de Clouddienst weg te halen (te "downloaden" of te migreren naar een andere Clouddienst). Deze mogelijkheid zit niet standaard in iedere Clouddienst. Het ontbreken van de mogelijkheid om gegevens eenvoudig weg te kunnen halen creëert een situatie van "vendor lock-in", welke voor afnemers een belemmering vormt om van een Clouddienst gebruik te maken.

BC-4 ONVOLDOENDE BESCHIKBAARHEID GARANTIE

Veel Clouddiensten worden aangeboden zonder een garantie rondom de minimale beschikbaarheid van de dienst. Met beschikbaarheid wordt hier bedoeld de "uptime" van de dienst, ofwel de tijd dat alle functionaliteit met de gebruikelijke performance door de afnemer gebruikt kan worden.

Tot op heden worden Clouddiensten door organisaties nog vaak gebruikt voor niet bedrijfskritische toepassingen, zoals bijvoorbeeld e-mail of kantoorautomatiseringtoepassingen. Om afnemers over

de streep te trekken meer bedrijfskritische toepassingen in de Cloud te plaatsen zal de aanbieder meer werk moeten maken van het bieden van zekerheden met betrekking tot de beschikbaarheid van de dienst.
Daarbij komt dat aanbieders in het algemeen niet transparant zijn over de geleverde prestaties. Aanbieders publiceren zelden de werkelijk behaalde beschikbaarheid van de dienst in de afgelopen periode.

Opgemerkt wordt dat er wel Clouddiensten zijn waarvoor een minimale beschikbaarheid wordt gegarandeerd. Dit zijn voornamelijk IaaS diensten.

BC-5. TWIJFELS OVER FINANCIËLE POSITIE VAN DE AANBIEDER

De Cloud biedt niet alleen kansen voor organisaties om productiviteit te verhogen of te innoveren, het biedt ook een platform voor ondernemingen om nieuwe Clouddiensten aan te bieden. Zo ontstaan er in hoog tempo nieuwe Clouddiensten van onbekende ondernemingen. In het zelfde tempo waarin ondernemingen met Clouddiensten kunnen groeien, zo snel kan ook de populariteit van een Clouddienst weer afnemen. In deze volatiele markt van aanbieders en diensten loopt een afnemer het risico geconfronteerd te worden met een faillissement van een aanbieder. Grote organisaties hebben de kennis en middelen om vooraf onderzoek te kunnen doen naar de financiële situatie van een aanbieder. Voor MKB organisaties daarentegen is inzicht in de financiële situatie van een aanbieder veel moeilijker te verkrijgen.
Inzicht in de financiële positie van een aanbieder is relevant omdat de gevolgen van een faillissement van een aanbieder voor de afnemer groot kunnen zijn. Zie hiervoor ook de beschrijving van belemmering BC-1.

E4. D. Integratie en standaarden

BD-1. ONVOLDOENDE MOGELIJKHEDEN TOT "REVERSIBILITY" OF "PORTABILITY"

Afnemers van Clouddiensten kunnen te maken krijgen met beperkingen rondom het terugdraaien (reversibiliteit) of het porteren van de door hen afgenomen diensten. Doordat een leverancier van Clouddiensten keuzes maakt rondom de wijze van opslaan van gegevens van haar klant, kan een situatie ontstaan dat die gegevens niet zonder meer door een andere leverancier kunnen worden ingelezen en de dienstverlening kan overnemen. Bij een overstap naar Clouddiensten kan deze belemmering overigens ook zichtbaar worden. Wanneer een organisatie eigen dienstverlening wil gaan vervangen voor Clouddiensten kan zij te maken krijgen met dataconversie en migratie.
Deze situatie is overigens niet uniek voor Clouddiensten. Ook bij het gebruik van software in een eigen omgeving kunnen portabiliteitsvraagstukken ontstaan.

BD-2. ONVOLDOENDE STANDAARDEN VOOR INTEROPERABILITEIT

Het vraagstuk rondom portabiliteit is groter naarmate de Clouddiensten meer richting eindgebruiker worden afgenomen. Bij IaaS-diensten speelt het minder dan bij PaaS en zeker SaaS. Dit wordt vooral veroorzaakt door het gebrek aan (open) standaarden voor de integratie van Clouddiensten. Om dit probleem op te lossen werken op dit moment verschillende partijen aan het creëren van voorzieningen die de integratie van verschillende diensten (Cloud en niet-Cloud)

beter mogelijk maken. Een mooi voorbeeld is de dienstverlening die door SURFnet wordt ontwikkeld: SURFconext. SURFconext is een op open standaarden gebaseerde samenwerkingsinfrastructuur waarmee instellingen interne en externe online diensten kunnen integreren.
Een externe infrastructuur zal slechts in enkele gevallen dezelfde standaarden, beveiligingsmaatregelen en processen kennen als die van de interne IT van de afnemer. Integratie van deze afwijkingen verloopt in de praktijk dikwijls moeizaam door technische beperkingen van gesloten standaarden en gestandaardiseerde beveiligingsmaatregelen van de leverancier.

BD-3. GEVAAR VOOR VENDOR LOCK-IN

Eén van de risico's die afnemers zien is vendor lock-in. Door het opgeven van de eigen IT-omgeving en de gegevensopslag en –verwerking in de Cloud onder te brengen, is de afnemer in hoge mate afhankelijk geworden van de aanbieder(s) van de Clouddiensten. In combinatie met gebrekkige standaarden, interoperabiliteit en portabiliteit (zie onder andere BD-1 en BD-2) leidt deze afhankelijkheid van Clouddiensten tot een risico op vendor lock-in.

E5. E. Markt (aanbod, perceptie, vertrouwen)

BE-1. BEDRIJVEN WETEN ONVOLDOENDE WAAR ZE OP MOETEN LETTEN

Potentiële afnemers van Clouddiensten krijgen te maken met een veelheid aan vraagstukken waar zij over na moeten denken. Het aantal geïdentificeerde belemmeringen illustreert dit. Grote organisaties zijn in staat om voor veel van de vraagstukken een afgewogen besluit te nemen en in overleg met de leverancier van Clouddiensten oplossingen te bedenken. Voor kleine en middelgrote organisaties is dit veel lastiger. Zij beschikken zelf niet over voldoende kennis om die afgewogen keuzes te maken, of hebben überhaupt onvoldoende zicht op de mogelijke risico's van het gebruik van Clouddiensten.

BE-2. CONTROLEERBAARHEID: KRIJG JE IN WERKELIJKHEID WAT IS BELOOFD?

De beloftes die door aanbieders van Clouddiensten worden gedaan klinken veelomvattend en aantrekkelijk. Het is echter voor een potentiële afnemer van Clouddiensten vooraf niet eenvoudig om te doorgronden of die beloftes ook allemaal kunnen worden nagekomen. De belofte van "volledige integratie met bestaande systemen " of "naadloos opschalen", komt in de uitingen van aanbieders vaak terug. Hoe dat in de praktijk uitwerkt is vooraf niet goed te achterhalen. Ook dit geldt in mindere mate voor grotere organisaties.

BE-3. ONTBREKEN VAN SLA (RESPONSETIJDEN, BESCHIKBAARHEID, ...)

Het ontbreken van heldere prestatie-indicatoren en garanties op die indicatoren, kan worden gezien als een symptoom van de onvolwassenheid van de markt voor Clouddiensten. Wel zijn een aantal grote aanbieders van Clouddiensten op dit moment bezig de transparantie rondom hun prestaties te vergroten.
Anderzijds is het een kenmerk van publieke Clouddiensten dat zij worden aangeboden via het Internet. Het verkrijgen van garanties rondom de beschikbaarheid van *het* Internet bestaan niet. Specifiek voor de Cloud geldt dat door het delen van voorzieningen, acties van één klant van

invloed kunnen zijn op de geleverde prestaties aan andere klanten. Het "overboeken" van een bepaalde voorziening is een veelgeziene strategie om schaalvoordelen te realiseren.

BE-4. TE WEINIG / GEEN TRANSPARANTIE MET BETREKKING TOT GELEVERDE PRESTATIES

Aanbieders van Clouddiensten zijn nog niet heel erg transparant over de geleverde prestaties. Niet veel aanbieders hebben op hun website een overzicht staan van de gerealiseerde beschikbaarheid, aantal incidenten of responsetijden. De bereikbaarheid en deskundigheid van een servicedesk kan een belangrijk criterium voor een afnemer zijn, om voor een bepaalde leverancier te kiezen. In een volwassen markt is het waarschijnlijker dat leveranciers, of onafhankelijke derden, hier transparantie creëren.

BE-5. HOE IS ONDERHOUD EN ONTWIKKELING VAN APPLICATIES IN DE CLOUD GEWAARBORGD?

Wanneer eenmaal een bepaalde Clouddienst is afgenomen, rijst de vraag op welke wijze de Clouddienst zich ontwikkelt. Enerzijds verwacht je als afnemer juist dat je ontzorgd wordt op het vlak van het beheer van de dienst en dat doorontwikkeling gegarandeerd is. Anderzijds heb je daar als individuele afnemers niet of nauwelijks invloed op. Zo kan de aanbieder besluiten de dienst aan te passen, terwijl personeel net was getraind op een bepaalde manier, of dat koppelingen met andere systemen waren gemaakt. Door de wijzigingen moeten de gebruikers weer "wennen" of moeten koppelingen weer worden aangepast.

Bepaalde wijzigingen kunnen zich ook weer vertalen in het aanpassen van de tariefstelling (zie BF-2)

BE-6. BIJ INCIDENTEN (ONDERBREKING VAN DE SERVICE) IS NIET ALTIJD DUIDELIJK WAAR HET PROBLEEM LIGT EN WELKE PARTIJ HIEROP MOET WORDEN AANGESPROKEN.

Clouddiensten komen in de meeste gevallen tot stand door een samenspel van diensten van verschillende partijen. De meest in het oog springende is het onderscheid tussen het afnemen van het transportkanaal (het Internet) en de aanbieder van de Clouddienst. In de meeste gevallen levert een aanbieder van telecommunicatiediensten de toegang tot het Internet. Ook de aanbieder van de Clouddienst maakt gebruik van een aanbieder om hem de toegang tot het Internet te leveren. Zoals al eerder gesteld, is het vanuit de essentie van het Internet niet goed mogelijk om garanties af te geven over de beschikbaarheid van het Internet.
Als afnemer van een Clouddienst kan een organisatie bij problemen met de dienst dus te maken krijgen met een aantal aanbieders, die allen een rol spelen bij de totstandkoming van de dienst. Wanneer de dienst zelf "on-premise" tot stand wordt gebracht speelt dit probleem niet of veel minder.

BE-7. RECHTEN EN VERANTWOORDELIJKHEDEN TUSSEN AANBIEDER EN AFNEMER ZIJN NIET ALTIJD DUIDELIJK

Door de combinatie van moeilijk te doorgronden standaard voowaarden in contracten (zie BE-15), de spreiding van diensten over meerdere landen met verschillende juridictie (zid BB-6), en door van toepassing zijnde specifieke wetgeving zoals bijvoorbeeld de WBP (zie BB-1), kunnen onduidelijkheden ontstaat over de verdeling van rechten en verantwoordelijkheden tussen aanbieder en afnemer. Dit kan bijvoorbeeld zijn ten aanzien van de begrippen bewerker en

verantwoordelijke uit de WBP, of ten aanzien intellectueel eigendom of van eigendom van gegevens in het algemeen.

BE-8. FUNCTIONALITEIT / BEHEERMOGELIJKHEDEN ONTOEREIKEND

In tegenstelling tot de "on-premise IT" wordt bij Cloud Computing de IT-middelen (faciliteit, infrastructuur, platform, applicaties), inclusief beheer en beveiliging, zo doelmatig mogelijk gedeeld door meerdere afnemers ("Multi-tenacy"). Dit delen van IT-middelen vereist een goede scheiding van toegang en autorisaties tussen verschillende afnemers.
Het op een goede wijze bieden van toegang tot diensten voor gebruikers (identity and access management) is een complexe materie waar veel organisaties mee worstelen. De introductie van Clouddiensten maakt dit vraagstuk mogelijk nog complexer. Clouddiensten sluiten niet altijd (technisch of procedureel) aan bij de eigen middelen voor toegangsbeheer. Zo lopen organisaties het risico dat vertrokken medewerkers nog steeds, via het Internet, toegang krijgen tot gegevens van de organisatie.

Ook hebben organisaties goede beheermogelijkheden nodig wanneer "eigen" toepassingen draaien op Clouddiensten (IaaS of PaaS). De onderliggende IaaS en/of PaaS infrastructuur moet in combinatie met de toepassing door de afnemer beheerd kunnen worden zodat de beschikbaarheid, veiligheid en performance (tegen acceptabele kosten) is gewaarborgd.

Daarnaast betekent het delen van middelen dat op enigerlei wijze generieke, standaarddiensten worden geleverd, waardoor afnemers minder mogelijkheden hebben specifieke functionaliteiten en/of wijzigingen in de IT-omgeving door te voeren.

BE-9. ER IS ONVOLDOENDE MARKTAANBOD GERICHT OP DE (BEHOEFTE VAN) DE OVERHEID

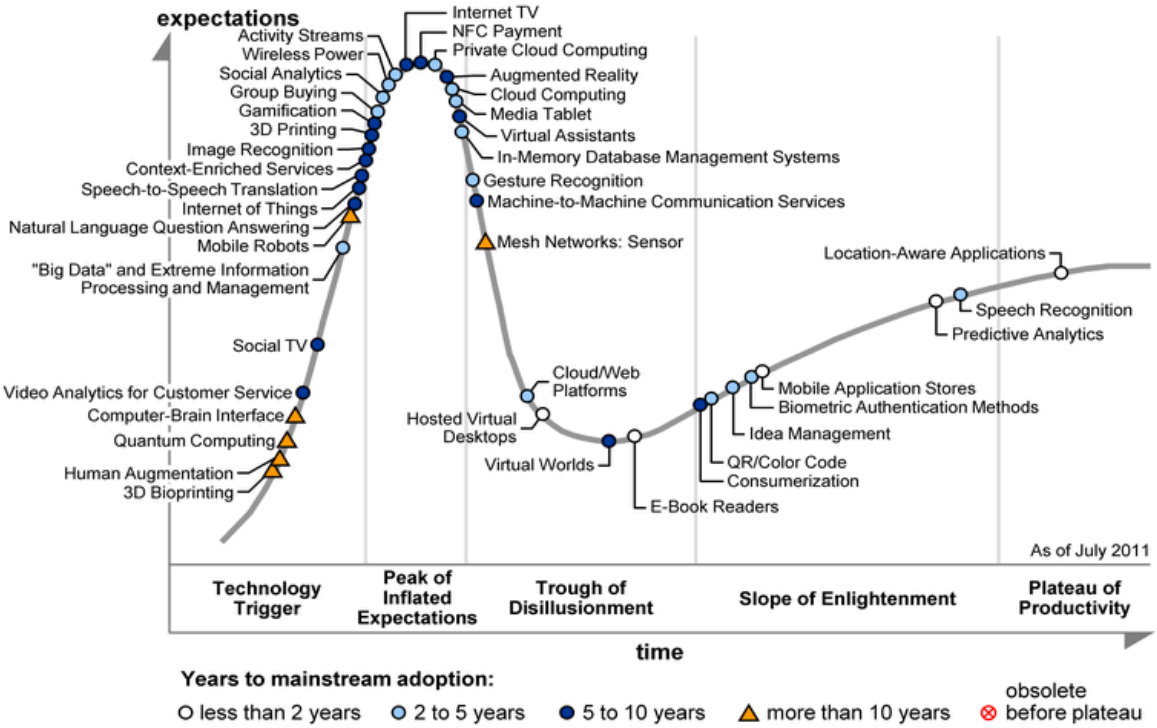
In de brief naar de kamer (20 april 2011) geeft de minister van BZK, mede op basis van het onderzoek van KPMG, aan dat het aanbod van ‘open’ Cloud Computing met voor de overheid toepasbare IT-oplossingen nog beperkt is. Slechts een klein deel van de aanbieders is volgens de minister bedrijfsmatig volwassen genoeg om daadwerkelijk ingezet te kunnen worden voor de Nederlandse overheid. De huidige Openbare Cloudtoepassingen komen nog niet tegemoet aan de specifieke wensen en verantwoordelijkheden van de overheid.

BE-10. ER IS ONVOLDOENDE VERTROUWEN IN CLOUDDIENSTEN

In veel publicaties en gesprekken wordt verwezen naar het beperkte vertrouwen dat mensen hebben in Clouddiensten. Vooral door breed uitgemeten verstoringen en inbraken bij grote aanbieders (RIM's Blackberry, Sony's Playstation, Microsoft's Office 365, Amazon's AWS en Google's Gmail) worden vraagtekens gezet bij de betrouwbaarheid van aanbieders van Clouddiensten. Belangrijke vraag hierbij is of de beschikbaarheid en veiligheid van die aanbieders nu daadwerkelijk kleiner is dan bij de voorzieningen die de organisatie zelf worden beheerd. Onvoldoende mogelijkheden voor afnemers om deze vergelijking te maken leidt tot een gebrek aan vertrouwen in Clouddiensten.

BE-11. CLOUDOPLOSSINGEN VALLEN VAAK TEGEN (MINDER AANTREKKELIJK DAN IN EERSTE INSTANTIE GEDACHT)

In de media verschijnen steeds vaker onderzoeksresultaten waaruit blijkt dat gebruikers van Clouddiensten teleurgesteld zijn met de resultaten. Symantec, een leverancier van beveiligingsoplossingen constateerde dat organisaties die Cloudtechnologieën hebben geïmplementeerd, niet de resultaten en voordelen zien die ze op voorhand verwacht hadden. Achtentachtig procent van de onderzochte organisaties (totaal onderzoek was 5.300 reacties uit 38 landen) had verwacht dat de Cloud hun IT-flexibiliteit zou verbeteren, maar slechts 47 procent geeft aan dat dit daadwerkelijk het geval is. Resultaten vielen ook tegen op het gebied van disaster recovery, efficiency, lagere operationele kosten en betere beveiliging.



(Bron: http://www.gartner.com/hc/images/215650_0001.gif)

In Gartners bekende hype cycle diagram uit juli 2011 bevinden Clouddiensten zich al op het pad naar de "kloof van de teleurstelling". Overigens geeft de grafiek ook aan dat de grootschalige adoptie niet verder dan 2-5 jaar voor ons ligt.

BE-12. TE WEINIG MOGELIJKHEID OM SPECIFIEKE (INDIVIDUELE AFNEMER) FUNCTIONALITEIT EN/OF WIJZIGINGEN DOOR TE VOEREN

Een van de kernelementen van Clouddiensten is dat de aanbieder tracht schaalgrootte te ontwikkelen. Door zijn IT-middelen te delen met meerdere gebruikers kan hij efficiënter werken dan een enkele afnemer. Dit concept betekent echter ook dat er weinig ruimte is voor een individuele afnemer om specifieke maatwerk-oplossingen in de afgenomen diensten aan te (laten) brengen. Voor organisaties betekent dit in veel gevallen dat zij processen en/of systemen moeten aanpassen aan datgene dat door de aanbieder geboden wordt. Wanneer een organisatie zelf een

bepaalde toepassing ontwikkelt kan echt maatwerk worden ontwikkeld. Bij het kiezen voor een Clouddienst moet dan ook worden afgewogen of de kosten van het aanpassen van bestaande bedrijfsprocessen opweegt tegen de voordelen van de Cloud. Juist de voordelen van Clouddiensten, zoals flexibiliteit, kan bij de gebruiker leider tot het besef dat "goed, goed genoeg is".
Voor sommige organisaties geldt ook dat zij zich door die specifieke toepassing zelfs van haar concurrenten kan onderscheiden. Wanneer veel organisaties van dezelfde Clouddienst gebruik maken, wordt het maken van een onderscheid op dat terrein natuurlijk lastig.

Opgemerkt wordt dat de beperkte invloed op de geboden functionaliteit met name van toepassing is op SaaS-diensten. Afnemers kunnen volledig naar eigen inzicht maatwerk toepassingen maken en deze "in de Cloud" onderbrengen door gebruik te maken van IaaS of PaaS Clouddiensten.

BE-13. ONVOLDOENDE TOOLING EN KENNIS BIJ DE INTERNE ORGANISATIE; PAAS

Om toepassingen te kunnen ontwikkelen op basis van PaaS diensten dient een organisatie te beschikken over tools en kennis. Het ontbreken hiervan vormt voor sommige organisaties een belemmering om van PaaS diensten gebruik te maken.

BE-14. AFHANKELIJKHEID MET DE BESCHIKBAARHEID/PRESTATIES VAN HET TRANSPORTNETWERK / INTERNET

Doordat, zeker bij Openbare Clouddiensten, de diensten tot stand komen door gebruik te maken van het publieke Internet, is er een afhankelijkheid van de goede werking van het Internet. (zie ook BE-6). Zeker indien de geografische afstand tot de aanbieder van de Clouddienst groot is en de bandbreedte gering, kunnen er prestatieproblemen ontstaan. Gebruikers ervaren dan bijvoorbeeld dat de toepassing te traag reageert.

BE-15. STANDAARDVOORWAARDEN VAN DE CLOUDAANBIEDER (VOLSTREKT) EENZIJDIG (& TE COMPLEX)

In zijn algemeenheid kan worden gesteld dat voor de afnemers een aantal belangrijke bezwaren kleeft aan de voorwaarden waaronder vooral grote Amerikaanse aanbieders (Google, Microsoft, Amazon, e.d.) Cloud Computing in Nederland aanbieden. De betreffende voorwaarden worden doorgaans als sterk eenzijdig, niet onderhandelbaar en weinig transparant beschouwd. De voorwaarden zijn in de regel gemodelleerd naar de contractmodellen welke door de betreffende aanbieders in de Verenigde Staten worden gebruikt en kenmerken zich door weinig toegankelijk taalgebruik, mede gekleurd door veel (vertaalde) Angelsaksische begrippen, en een voor de lezer complexe structuur in termen van gelaagdheid en doorverwijzing naar andere relevante (contract) documenten, zoals privacy policies.
Voor de individuele eindgebruiker zijn de voorwaarden in de praktijk niet onderhandelbaar.

E6. F. Business Case

BF-1. BESTAANDE LICENTIES REMMEN OVERGANG NAAR DE CLOUD

Leveranciers hanteren in het algemeen licentiestructuren voor de afname van software. Deze structuren zijn vaak afgestemd op de traditionele manier van het toepassen van IT. Bijvoorbeeld

een licentiestructuur waarbij per server wordt betaald voor software. Door de toenemende virtualisatie, een technologie die ten grondslag ligt aan openbare en private Clouds, passen de traditionele licentiestructuren vaak niet. Vervolgens worden de licentiestructuren door de leveranciers dusdanig aangepast dat in een gevirtualiseerde omgeving per saldo hetzelfde moet worden betaald voor de software. Om dezelfde reden kunnen bestaande licentiestructuren een belemmering vormen voor de overgang naar de Cloud.

BF-2. ONZEKERHEID TEN AANZIEN VAN PRIJSONTWIKKELING IN DE TOEKOMST

Een van de kenmerken van het afnemen van Clouddiensten is dat de afnemer flexibiliseert in zijn kosten. Hij doet niet eenmalig investering in hard- en software, maar neemt diensten af en betaalt per gebruiker, transactie of gebruikte opslagcapaciteit. De flexibiliteit heeft ook een keerzijde wanneer een aanbieder in de loop van tijd aanpassingen aan dat flexibele tariferingmodel doorvoert. Hoewel onderhoudscontracten op eigen IT-systemen ook in de loop van de tijd aangepast kunnen worden, is de impact bij Clouddiensten mogelijk veel groter. Bij eigen IT-middelen zijn de kosten voor het gebruik van de middelen, na aanschaf/ontwikkeling, redelijk goed in te schatten en stabiel.

BF-3. CLOUD ZEGT MKB WEINIG ==> VOOR WELKE THEMA'S IS CLOUD VOOR MKB RELEVANT?

Het thema Cloud Computing is voor veel ondernemers in het midden- en kleinbedrijf nog een relatief vaag begrip. Hoewel het gebruik van Clouddiensten, wellicht ongemerkt, ook in het MKB al sterk is gestegen, bestaat de indruk dat veel mogelijkheden van het toepassen van Clouddiensten ombenut blijven. Bij organisaties gericht op het ondersteunen van het Nederlandse bedrijfsleven (MKB Nederland, Syntens) wordt Cloud gezien als een belangrijke ontwikkeling. Het aantal vragen over Clouddiensten dat door het bedrijfsleven aan deze organisaties wordt gesteld is nog klein. Grote bedrijven hebben daarentegen al een heel goed beeld van de mogelijkheden van Clouddiensten.

BF-4. GEDANE INVESTERINGEN IN IT-SYSTEMEN MAKEN OVERSTAP NAAR CLOUDDIENSTEN NIET RENDABEL

Zoals voor veel vervangingsvragen geldt, geldt ook voor Clouddiensten dat reeds gedane investeringen een belemmering kunnen vormen voor het afnemen van Clouddiensten. Wanneer een organisatie bijvoorbeeld heeft geïnvesteerd in het opzetten van een eigen e-mailomgeving, zal zij vanaf dat moment tegen relatief geringe kosten de e-maildienst kunnen leveren. Mogelijk zal pas bij een vervangingsvraag ook de optie van Clouddiensten worden overwogen.

BF-5. HOGE MATE VAN COMPLEXITEIT, ZEKER BIJ INTEGRATIE MET VERSCHILLENDE AANBIEDERS EN EIGEN SYSTEMEN (LEGACY)

Wellicht in mindere mate bij IaaS, maar zeker bij PaaS en SaaS geldt dat de afnemer zich moet aanpassen aan de standaarden, beveiligingsmaatregelen en processen van de Cloudaanbieder. Wanneer voor een integratie met de eigen IT-omgeving moet worden gekozen neemt de complexiteit van de gehele oplossing snel toe.

E7. G. Overig

BG-1. GEBRUIK VAN CLOUDDIENSTEN DOOR DE OVERHEID

De overheid kan een voorbeeldfunctie vervullen door zelf actief van Clouddiensten gebruik te maken. Echter, veel van de belemmeringen genoemd in deze bijlage zijn ook op de overheid als (potentiele) afnemer van Clouddiensten van toepassing. Terughoudendheid van de overheid als het gaat om het gebruik van Clouddiensten kan een negatief signaal afgeven aan de markt en daarmee de groei van Cloud Computing afremmen.

BG-2. UITROL FTTH TE LANGZAAM

Clouddiensten worden aangeboden via een keten van aanbieders, niet op de laatste plaats de aanbieder van internettoegang. Het ontbreken van een zeer breedbandige netwerk naar huishoudens in Nederland betekent dat Clouddiensten die gebruik zouden maken van zo´n netwerk nu (nog) niet tot stand komen. In die zin zit de belemmering hier wellicht eerder aan de aanbiederzijde. Afnemers ervaren de belemmering nog niet of nauwelijks. Zeker zakelijke afnemers van Clouddiensten, zullen indien nodig, een glasvezelverbinding kunnen afnemen.

BG-3. (TOEKOMSTIGE) STRUCTURELE SCHAARSTE AAN IT-PROFESSIONALS IN NEDERLAND

Volgens de brancheorganisatie ICT-Office zullen er in 2015 ruim 8.600 te weinig ict'ers zijn en dat tekort zal de jaren erna verdubbelen. De Nederlandse kenniseconomie staat hierdoor onder druk. [R-37]. Het ontwikkelen en toepassen van Clouddiensten vraagt een ruim contingent van ict'ers met actuele kennis.

Ook de TaskForce e-Skills van het ministerie van Economische Zaken wijst op het toekomstige tekort. Voorzitter Peter Hagedoorn citerend: 'We weten niet hoe we complexe IT-projecten moeten aanpakken en aansturen omdat we daar de juiste mensen niet voor hebben. Vandaar dat ook veel van die projecten in mislukken en megafusies vastlopen.'

Naast de ict-professionals moeten volgens Hagedoorn steeds meer mensen in de 'klassieke' beroepen, zoals, artsen, ingenieurs en juristen, zelf kunnen omgaan met ict om tot verbeteringen in hun vak te komen. Taskforce e-Skills betrekt bij haar berekeningen ook deze beroepsgroepen en komt daarmee voor het innovatief vermogen op een tekort van 25-duizend tot 40-duizend mensen met ict-kennis en - vaardigheden (e-skills).

BG-4. TE WEINIG ONDERZOEKSPROJECTEN IN EUROPA

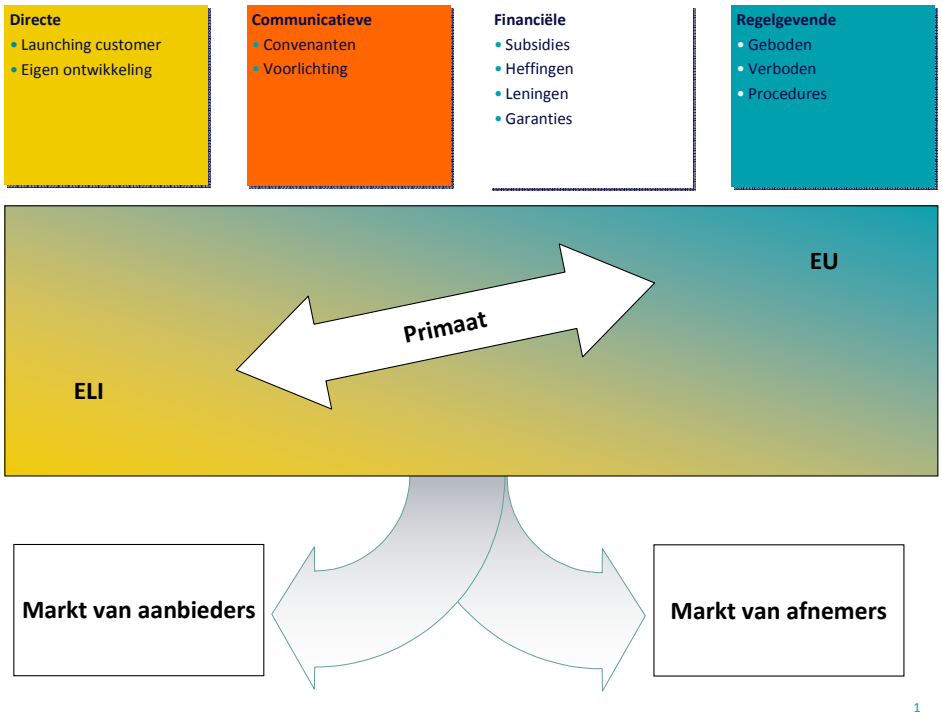
Vergeleken met de Verenigde Staten en Japan, wordt er in Europa te weinig uitgegeven aan onderzoek. Nederland gaf in 2010 1.7% van zijn BBP uit aan onderzoek. Dit ligt onder het EU gemiddelde en ver van de 3% doelstelling. En terwijl wij ons in Europa druk maken over de 3%, gaat Zuid-Korea voor 5% en zijn de R&D uitgaven in China de laatste jaren zelfs met 25% gestegen. Middels R&D zouden ook Clouddiensten verder ontwikkeld kunnen worden.
Bron: Robert-Jan Smits, Directeur-Generaal Onderzoek en Innovatie, Europese Commissie, Opening Academisch jaar Universiteit Utrecht, Utrecht, maandag 5 september 2011.

BG-5. IS ER VOLDOENDE KENNIS IN HUIS OM DE INTEGRATIE MET CLOUDDIENSTEN TE REALISEREN

Uit onderzoek blijkt dat organisaties zich veel zorgen maken over het mogelijke gebrek aan deskundig personeel om de zorgen rondom beveiliging bij het gebruik van Clouddiensten goed op te kunnen pakken. Om die reden zouden zij afzien van de inzet van Clouddiensten. [R-38]

F Beleidsinstrumentarium

De aanbevelingen worden gedaan vanuit het perspectief van EL&I, waarbij vooral is gekeken naar het beschikbare beleidsinstrumentarium: Directe, Communicatieve, Financiële en Regelgevende instrumenten. De verschillende beleidsinstrumenten kunnen direct worden gericht op de markt van aanbieders, maar ook op de markt van de afnemers.



Figuur 10 Beleidsinstrumentarium

In bovenstaande figuur is aangegeven waar het primaat voor bepaalde instrumenten ligt. Voor Regelgevende instrumenten ligt het primaat vooral bij de EU. Voor directe instrumenten en communicatieve instrumenten ligt het primaat eerder bij EL&I.