



Juridische grenzen aan Cloud Computing?

mr. drs. Lesley C.P. Broos

senior IT-juridisch consultant Mitopics

onderzoeker / docent IT & Recht Universiteit Twente
faculteit Management en Bestuur
vakgroep Legal and Economic Governance Studies

Agenda

- Wie is er bang voor de “grote boze wolk”?
- Wat is er dan zo bijzonder?
- Van Cloud Service naar contract in 5 stappen
 - Voorbeeld: persoonsgegevens in de cloud
- Onderzoeksvoorstel C4C en UT:
 - Legal Analysis Tool voor Cloud Computing

Agenda

- Wie is er bang voor de “grote boze wolk”?
- Wat is er dan zo bijzonder?
- Van Cloud Service naar contract in 5 stappen
 - Voorbeeld: persoonsgegevens in de cloud
- Onderzoeksvoorstel C4C en UT:
 - Legal Analysis Tool voor Cloud Computing

Wie is er bang voor de grote boze wolk?

- **Uit toespraak van staatssecretaris Bijleveld op Govcert Symposium 2009:**

“...And then there is cloud-computing: cooperating and sharing information through the internet. It offers wonderful and promising possibilities but it is unprotected. Therefore it is unfit for private or confidential information and thus – at least for now - not suitable for official business, for local or national government.”

BRON: <http://www.rijksoverheid.nl/documenten-en-publicaties/toespraken/2009/10/07/toespraak-van-staatssecretaris-bijleveld-op-govcert-symposium-2009.html> (21-4-2011)

Wie is er bang voor de grote boze wolk?

- CIO online:
“Cloud-contracten: simpel maar gevaarlijk”
<http://cio.nl/nieuws/20095/cloud-contracten-simpel-maar-gevaarlijk.html> (23-4-2010)
- Forrester rapport, *The State of Emerging Enterprises Hardware 2009 to 2010*:
“Ondernemingen vinden cloud onveilig (...) Ruim 80 procent van de grote ondernemingen wil voorlopig niet investeren in cloud computing of cloud storage. De belangrijkste reden daarvoor is dat ze zich zorgen maken over de beveiliging van hun applicaties en gegevens.”
http://www.computable.nl/artikel/ict_topics/infrastructuur/3185410/2379248/ondernemingen-vinden-cloud-onveilig.html#ixzz1K8wxwX7D

Google apps

- Terms of service clause “11. Content license from you
 1. You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Services. By submitting, posting or displaying the content **you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services.** This license is for the sole purpose of enabling Google to display, distribute and promote the Services and may be revoked for certain Services as defined in the Additional Terms of those Services.
 2. You agree that this license includes a right for Google to make such Content available to other companies, organizations or individuals with whom Google has relationships for the provision of syndicated services, and to use such Content in connection with the provision of those services.”

dropbox.com/terms

- “You acknowledge and agree that you should not rely on the Site, Content, Files and Services for any reason. You further acknowledge and agree that you are solely responsible for maintaining and protecting all data and information that is stored, retrieved or otherwise processed by the Site, Content, Files or Services.”
- “All files stored online by Dropbox are (...) in multiple data centers located across the United States.” (<http://www.dropbox.com/help/7>)

Microsoft: EU moet cloud reguleren

Europa moet haar digitale wetgeving moderniseren en harmoniseren, want alleen dan kan cloud computing echt van de grond komen. Dat zei Microsoft's topjurist Brad Smith dinsdag tijdens een bijeenkomst voor overheidsambtenaren in Brussel. 'De wereld heeft een veilige en open cloud nodig. Overheden kunnen een sleutelrol spelen om die realiteit te bereiken', zei Smith.

Volgens de topjurist van [Microsoft \(177\)](#) zijn er vier uitdagingen die overheden moeten adresseren.



Smith riep de overheidsambtenaren op met [wetgeving \(178\)](#) te komen die consumenten van cloud providers beschermt. 'Waarom Microsoft Brussel om regelgeving vraagt? De reden daarvoor is pragmatisch. Voldoen aan één EU-richtlijn is veel gemakkelijker dan 27 verschillende wetten gehoorzamen.'

Wetgeving moet geharmoniseerd

Daarnaast is volgens Microsofts topjurist van belang om de Europese digitale [wetgeving \(179\)](#) te moderniseren en harmoniseren. Smith: 'De *data protection directive* is na vijftien jaar verouderd. Die Europese richtlijn is niet geschreven voor een wereld waarin data continu van plaats verandert. Voor de *data retention directive* geldt hetzelfde. Die houdt geen rekening met een situatie waarin een Italiaanse gebruiker data opslaat in een lers datacentrum dat wordt beheerd vanuit Amerika. Het is voor een bedrijf niet mogelijk met de wetgeving uit al die landen tegelijk rekening te houden. Die situatie kan de overgang naar breed gebruik van de cloud vertragen.'

Nieuwe EU-richtlijn voor Cloud computing?

Kroes kondigt nieuwe richtlijnen aan voor cloud computing

 **Jeroen Mulder**^[18] op 2 februari 2011 08:05 in Bijeenkomsten^[19], ISP^[20], Juridisch^[21], Politiek^[22], economie^[23]
Tags: Kroes; cloud computing; Europese Commissie; privacywetgeving^[24]

Cloud blijft ook in 2011 het magische woord. Grote bedrijven, zoals recentelijk nog Intel en HP, bombarderen de markt blijvend met nieuwe initiatieven. Tijd dus om eens goed te kijken naar de regelgeving omtrent diensten die vanuit de public cloud worden geleverd. En mogelijk is het ook tijd om de regels voor privacybescherming aan te passen. Eurocommissaris Neelie Kroes zei dit eind vorige week tijdens het World Economic Forum^[25] in het Zwitserse Davos.



Kroes vreest dat met name private cloud computing de huidige regelgeving voor privacybescherming uitholt. Services vanuit de public cloud betekenen immers impliciet ook transport van data vanuit de cloud – en wellicht data die normaliter onder privacywetgeving valt. Zeker met de huidige groei van cloud computing worden al snel de juridische grenzen bereikt omdat de huidige regelgeving nog geen rekening hield met deze ontwikkeling.

In haar toespraak voor de denktank in Davos stipte Kroes drie aandachtsgebieden aan: het juridische raamwerk voor privacybescherming, de technische grondslag met betrekking tot security en de technische standaarden voor API's (Application Programming Interfaces) en bestandsformaten.

In alle aandachtsgebieden zal de Europese Commissie de regelgeving bestuderen en zonodig met voorstellen voor nieuwe richtlijnen komen, aldus Kroes. Ze onderstreepte hierbij wel dat de commissie cloud computing wil stimuleren en ook doorgaat met de steun aan diverse proefprojecten.

Agenda

- Wie is er bang voor de “grote boze wolk”?
- **Wat is er dan zo bijzonder?**
- Van Cloud Service naar contract in 5 stappen
 - Voorbeeld: persoonsgegevens in de cloud
- Onderzoeksvoorstel C4C en UT:
 - Legal Analysis Tool voor Cloud Computing

Wat is er dan zo bijzonder?

- Inhoud afspraken over Cloud Services
- Proces van Cloud Contracting

Inhoud van de afspraken

Selectie van juridische bijzonderheden in Cloud contracten

- Aansprakelijkheid
- Subcontracting
- Opschortingsrechten
- Geheimhouding
- Intellectueel eigendom / licenties
- Privacy
 - bewerkersovereenkomst met maatregelen, instructiebevoegdheid, plaats van verwerking, meldingsplicht
 - beveiligingsincidenten, uitvoering controle- en correctierechten
 - betrokkenen, maximale bewaartermijnen en verplichting tot verwijdering
 - toegang tot data door derden (klanten van klant, toezichthouders, opsporingsdiensten)
- Continuïteit
 - backup, uitwijk, (data) escrow
 - exit-scenario's en daarvoor benodigde open cloud / open standaarden ter bevordering interoperabiliteit / dataportabiliteit
- Compliance
 - IFRS, SOx, Tabaksblat, civielrechtelijke en fiscale bewaartermijnen, bestuurdersverantwoordelijkheid
- Audit-rechten
 - SAS70 type I en II, ISAE3402/SSAE type A en B voor bevestiging verantwoordelijkheid, gang van zaken, gevolgen audit en financiën
- Transitie
- SLA
- Flexibiliteit
 - Voor zowel afnemer (schaalbaarheid) als aanbieder (bijv. releasebeleid)
- Toepasselijk recht
 - In geval van schending EU-privacy
 - in geval van tekortkomingen in de nakoming
 - in geval van onrechtmatige daad?
- Bevoegde rechter
- ...

Inhoud van de afspraken

Selectie van juridische bijzonderheden in Cloud contracten

- Aansprakelijkheid
- Subcontracting
- Opschortingsrechten
- Geheimhouding
- Intellectueel eigendom / licenties
- Privacy
 - bewerkersovereenkomst met maatregelen, instructiebevoegdheid, plaats van verwerking, meldingsplicht beveiligingsincidenten, uitvoering controle- en correctierechten betrokkene (maximale bewaartermijnen en verplichting tot verwijdering), toegang tot data (voor klanten van klant, toezichthouders, opsporingsdiensten)
- Continuïteit
 - backup, uitwijk, escrow, exit-scenario's en daarvoor nodig open cloud / open standaarden bevordering interoperabiliteit / datanood
- Compliance
 - IFRS, SOx, Tabak, etc. (rechtelijke en fiscale aansprakelijkheden, bestuurdersverantwoordelijkheid)
- Audit
 - SAS 70 type I en II, ISAE 4000 type A en B voor bevestiging verantwoordelijkheid, gang van zaken, gevolgen audit
- Transitie
- SLA
- Flexibiliteit
 - Voor zowel afnemer (schaalbaarheid) als aanbieder (bijv. releasebeleid)
- Toepasselijk recht
 - In ge val van schending EU-privacy, in geval van tekortkomingen in de nakoming, in geval van onrechtmatige daad?
- Bevoegde rechter
- et cetera

Inhoudelijk niet ingewikkelder dan bijvoorbeeld traditionele IT-outsourcingscontracten, wel meer diversiteit...

naamgeving

- Jaren 80/90... time sharing, client-server op afstand, EDI
- Ca 2000... Application Service Providing (ASP)
- Ca. 2005... Software as a Service (SaaS)
- ca 2009... Cloud Computing
 - Software as a Service (SaaS)
 - Gmail, BPOS (Microsoft), Projectplace, Salesforce (CRM)
 - Platform as a Service (PaaS)
 - Amazon Web Services, Google Apps, Microsoft Windows Azure
 - Infrastructure as a Service (IaaS)
 - Akamai, Amazon EC2, Rackspace
- maar ook: application hosting, Application Infrastructure Providing (AIP), managed services et cetera

<<Meer over naamgeving: whitepaper Mitopics op www.mitopics.nl>>

Proces van Cloud Contracting

- Cloud contracten komen vaak via de achterdeur naar binnen
- Minder ruimte voor specifieke wensen klant dan bij traditionele outsourcing
- Contractuele instemming technisch afgedwongen
- Standaardovereenkomst zonder betrokkenheid van juridische afdeling of afdeling security & compliance
- Voorwaarden CSP belangrijk selectie criterium!

Agenda

- Wie is er bang voor de “grote boze wolk”?
- Wat is er dan zo bijzonder?
- **Van Cloud Service naar contract in 5 stappen**
 - Voorbeeld: persoonsgegevens in de cloud
- Onderzoeksvoorstel C4C en UT:
 - Legal Analysis Tool voor Cloud Computing

Van Cloud Service naar contract in 5 stappen

1. Begrijpen service en context
2. Inventariseren toepasselijke rechtsregels
3. Analyseren risico's en maatregelen
4. Expliciteren managementkeuzes
5. Formuleren / beoordelen contractbepalingen

1. Begrijpen service en context

- Gedegen specificatie van
 - Type Service
 - IaaS, PaaS, SaaS
 - locatie(s) infrastructuur en (sub)provider(s)
 - Ondersteund bedrijfsproces
 - doelstelling Cloud Service, belang business
 - Betrokken data
 - (bijzondere) persoonsgegevens?
 - vertrouwelijkheid?
 - Gebruikers en gebruik
 - locatie
 - intensiteit
 - afspraken omtrent het gebruik
 - et cetera

2. Inventariseren toepasselijke rechtsregels

- Inventarisatie op alle niveau's:
 - Business, branche, nationaal, internationaal en supranationaal
- Voorbeeld: DMS o.b.v. SaaS door een financiële instelling
 - Compliance voorschriften van o.a. AFM en DNB
 - Algemeen: uitbesteding niet toegestaan als dit adequaat toezicht belemmert
 - Bankwet (systeemtoezicht)
 - Wet op het financieel toezicht (Wft)
 - Bazel II
 - Sarbanes-Oxley / SAS70 et cetera
 - Wet bescherming persoonsgegevens (EG 95/46/EG)
 - Vaststellen doel en middelen (art. 7 Wbp)
 - Passende technische en organisatorische maatregelen (art. 13 Wbp)
 - Sluiten bewerkersovereenkomst(en) (art. 14 lid 2 Wbp)
 - Toezien op naleving door bewerker (art. 14 lid 3 sub b Wbp)
 - Meldingsplicht (art. 27 Wbp)
 - Verplichtingen jegens betrokkenen (informatie, correctie, verwijderen)
 - Verbod op doorgifte naar landen buiten EER die geen “passend beschermingsniveau” bieden (art. 76 Wbp) et cetera

2. Inventariseren toepasselijke rechtsregels

- Passend beschermingsniveau
 - Alle EU lidstaten: Oostenrijk, België, Bulgarije, Cyprus, Tsjechië, Denemarken, Estland, Finland, Frankrijk, Duitsland, Griekenland, Hongarije, Ierland, Italië, Letland, Litouwen, Luxemburg, Malta, Nederland, Polen, Portugal, Roemenië, Slowakije, Slovenië, Spanje, Zweden, Verenigd Koninkrijk
 - Aangevuld met EER landen: IJsland, Liechtenstein en Noorwegen
 - Aangevuld met landen o.b.v. besluiten Europese Commissie: Guernsey, Isle of man, Argentinië, Canada, Zwitserland
 - Verenigde Staten indien en voor zover betreffende bedrijven en andere organisaties zich hebben verplicht tot het toepassen van de zogenaamde Safe Harbor regels
- Andere gevallen:
 - Gebruik maken van uitzonderingen (art. 77 lid 1 Wbp)
 - Bijvoorbeeld ondubbelzinnige toestemming betrokkenen, zwaarwegend algemeen belang, noodzaak ter vrijwaring vitaal belang betrokkene et cetera
 - Aanvraag vergunning Minister van Justitie na advies van het CBP

CHECK op regionalisatie opslag!

- Overeenkomst voor Google Apps for business, art. 2.2:
 - “(...) Gegevens die door Google worden verzameld, kunnen worden opgeslagen en verwerkt in de Verenigde Staten of in elk ander land waarin Google of de vertegenwoordigers van Google over voorzieningen beschikken, op voorwaarde dat dergelijke voorzieningen aan beveiligingsnormen voldoen die ten minste dezelfde bescherming bieden als de veiligheidsnormen van de voorzieningen waar Google de eigen informatie van een vergelijkbaar type opslaat en verwerkt. Door gebruik te maken van de Services geeft de Klant toestemming voor dergelijke overdracht, verwerking en opslag van gegevens. (...)”
- Amazon Web services Customer Agreement clause 3.2 Data Privacy (8-2-2011):
 - “We participate in the safe harbor programs described in the Privacy Policy. **You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you,** unless required to comply with the law or requests of governmental entities. You consent to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.”

3. Analyseren risico's en maatregelen

- Risico's
 - Niet (kunnen) voldoen aan compliancy-voorschriften
 - Ontberen goedkeurende verklaring
 - Onrechtmatige verwerking persoonsgegevens
 - Schending rechten betrokkenen
 - Verlies vergunning
 - ...
- Maatregelen
 - Afdwingen auditrechten (onaangekondigd en on site...)
 - Instructiebevoegdheden
 - Afdwingen nalevingsmogelijkheid rechten betrokkenen
 - Bewegen van shared naar meer dedicated oplossingen
 - ...

4. Expliciteren managementkeuzes

- Uitgangspunt: Intrinsiek verlangen om als rechtspersoon aan de wet te voldoen...
 - Compliance als visitekaartje van de onderneming
- Maar ook: kans vs impact inschattingen
 - Kans
 - Fraudeonderzoek?
 - Klachten van betrokkenen?
 - Onderzoek door CBP?
 - Impact
 - Imagoschade
 - Boetes
 - Interne kosten

5. Formuleren / beoordelen contractbepalingen

- Verplichte contractsbepalingen
 - Instructiebevoegdheid technische en organisatorische maatregelen
 - Medewerking ter uitoefening rechten betrokkenen
 - Verplichte medewerking aan audits
 - Geen export data naar landen zonder passend beschermingsniveau
 - Bepalingen ex bewerkersovereenkomst Wbp
 - ...
- Aanbevolen contractsbepalingen
 - Grenzen opschortingsrechten?
 - Kostenregelingen audits
 - Meldingsplicht in geval van beveiligingsincidenten?
 - QoS-bepalingen (SLA)
 - Releasebeleid
 - Omgang met subcontracting
 - Exit-scenario's
 - ...

Voorbeelden contractsbepalingen (1)

- Medewerking ter uitoefening rechten betrokkenen
 - Wederpartij verleent Opdrachtgever haar volledige medewerking om betrokkenen in de zin van artikel 1 onder f Wbp (i) inzage in hun persoonsgegevens te laten krijgen, (ii) persoonsgegevens te laten verwijderen of te corrigeren, en/of (iii) aan te laten tonen dat persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn of, indien Opdrachtgever het standpunt van betrokkene bestrijdt, vast te leggen dat betrokkene zijn persoonsgegevens als incorrect beschouwt.

Voorbeelden contractsbepalingen (2)

- Verplichte medewerking aan audits
 - Leverancier erkent de bevoegdheid van bepaalde toezichhoudende autoriteiten en/of instanties (zoals De Nederlandsche Bank, de AFM of de NMa) om:
 - (a) informatie in te winnen bij of van Leverancier respectievelijk door Leverancier ingeschakelde derden of de externe accountant van Leverancier omtrent de Diensten; en/of
 - (b) desgewenst onderzoek te doen of te laten doen bij Leverancier of de door Leverancier ingeschakelde derden, bijvoorbeeld onderzoeken naar de bedrijfsvoering en bedrijfsprocessen in het kader van de verlening van de Diensten;
- en verplicht zich om onverkort aan dergelijke verzoeken om informatie en onderzoeken zijn volledige medewerking te verlenen. Leverancier zal – voor zover nodig - er voor zorg dragen dat door haar ingeschakelde derden en haar (externe) accountant eveneens volledige medewerking verlenen aan deze controlewerkzaamheden.

Agenda

- Wie is er bang voor de “grote boze wolk”?
- Wat is er dan zo bijzonder?
- Van Cloud Service naar contract in 5 stappen
 - Voorbeeld: persoonsgegevens in de cloud
- **Onderzoeksvoorstel C4C en UT:**
 - Legal Analysis Tool voor Cloud Computing

Onderzoeksvoorstel

Universiteit Twente in opdracht van C4C

betreffende de ontwikkeling van een
"Legal Analysis Tool voor Cloud Computing"

- Mogelijkheden tool:
 - snelle structured analysis van juridisch relevante eigenschappen van een specifieke clouddienst
 - identificatie contractueel te regelen juridische bijzonderheden
 - Fase 1: Aanwijzingen voor bijbehorende contractsbepalingen
 - Fase 2: Tekstuele uitwerking model contractbepalingen
 - Fase 3: Internationalisatie
- Doelgroep:
 - Aanbieders (inclusief resellers / distributeurs) en afnemers (profit en non-profit) van Cloud-diensten

<Meer info / aanmelding voor valorisatiepartners en sponsors bij C4C>



Vragen?

IT-juridische dienstverlening:

L.Broos@mitopics.nl

Onderzoek:

L.C.P.Broos@utwente.nl