Cloudcomputing

Een kans voor de Belgische economie

economie
FOD Economie, K.M.O., Middenstand en Energie

.be

Cloudcomputing

Een kans voor de Belgische economie

economie
FOD Economie, K.M.O., Middenstand en Energie

Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie
Vooruitgangstraat 50
1210 Brussel
Ondernemingsnr.: 0314.595.348
http://economie.fgov.be

tel. 02 277 51 11

Vanuit het buitenland:
tel. + 32 2 277 51 11

Verantwoordelijke uitgever: Jean-Marc Delporte
Voorzitter van het Directiecomité
Vooruitgangstraat 50
1210 Brussel

Internetversie

E9-1055/0370-13

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Disclaimer

Dit verslag werd opgesteld door Unisys Corporation voor de FOD Economie, K.M.O., Middenstand en Energie. Het geeft het standpunt weer van de auteurs op basis van de vermelde bronnen. Noch de FOD Economie, noch de auteurs van dit verslag, kunnen aansprakelijk worden gesteld voor het gebruik dat van de inhoud van dit verslag wordt gemaakt.

Auteurs:

UNISYS

Patrice-Emmanuel Schmitz – juridisch expert, directeur Europese studies

Giedré Kazlauskaite – Sr. juridisch consultant

Michel Hoffmann – Sr. veiligheidsconsultant

Pierre Franck – Sr. consultant informatietechnologieën

Revisietabel

Versie	Datum	Auteur	Beschrijving	Actie*	Pagina's
0.1 – 0.3	15.03.2013	Allen	Eerste interne versie	I	Alle
0.4	04.04.2013	Allen	Draft, definitieve versie	I	Alle
1.0	05.04.2013	Allen	Definitieve versie gestuurd aan de FOD Economie	I	Alle
1.1	30.04.2013	Allen	Versie met de correctie van de FOD, alsook de punten besproken tijdens de presentatie van 25 april 2013	I	Alle
1.2	08.05.2013	Allen	Finale versie nagelezen door de FOD Economie	I	Alle

(*) Actie: I = Insertion R = Replacement

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Inhoudsopgave

1 Inleiding ... 1
2 Samenvatting ... 3
3 Wat is *cloud*computing? ... 6
3.1 Gedistribueerde computing ... 6
3.2 Diverse implementatiemodellen ... 7
3.2.1 Private *cloud* ... 7
3.2.2 Gemeenschappelijke *cloud* ... 7
3.2.3 Publieke *cloud* ... 7
3.2.4 Hybride *cloud* ... 7
3.2.5 Andere categorieën: soevereine(?) *cloud* ... 8
3.3 Diverse servicelagen ... 8
3.3.1 De infrastructuur (IaaS of "Infrastructure as a Service") ... 9
3.3.2 Het platform (PaaS of "Platform as a Service") ... 9
3.3.3 De software (SaaS of "Software as a Service") ... 9
3.4 Diverse financieringswijzen ... 10
3.5 Specifieke cloudkenmerken ... 10
3.5.1 Basiskenmerken: ... 10
3.5.2 Nieuwe elementen ... 11
3.5.3 Ecologische aspecten ... 12
3.5.4 Economische aspecten ... 14
3.5.5 De aan de *cloud* verbonden functies of beroepen ... 16
4 Kansen en risico's van *cloud*computing ... 19
4.1 Kansen van cloudcomputing ... 19
4.2 Risico's van cloudcomputing ... 20
4.2.1 classificatie van de risico's ... 20
4.2.2 Fiches risicobeschrijving ... 21
4.3 Risicobeheer ... 28
4.3.1 Risicobeoordeling ... 29
4.3.2 Herziening van het beveiligingsbeleid ... 30
4.3.3 Risicobeheersing ... 31
4.3.4 Gecontroleerd gebruik van de *cloud* ... 32
5 De *cloud*markt ... 33
5.1 Stand van zaken in Europa en in België ... 33
5.1.1 Stand van zaken van de *cloud*markt in Europa ... 33
5.1.2 Remmingen voor de ontwikkeling van de *cloud* ... 35
5.2 Evolutie van de Belgische en Europese cloudmarkt ... 36
5.2.1 Mogelijke scenario's ... 36
5.2.2 Het pessimistische scenario ... 36
5.2.3 Het lineaire scenario ... 37
5.2.4 Het optimistische / interventiescenario ... 38
5.2.5 De kans van een directe overheidsinterventie? ... 39
6 Het rechtskader van *cloud*computing ... 41
6.1 Stand van zaken in België ... 41
6.1.1 Bescherming van persoonsgegevens ... 41
6.1.2 Het stelsel van de gegevensdoorgifte ... 44
6.1.3 Wat is de "toepasselijke wet" op gegevensverwerking? ... 47
6.1.4 De aansprakelijkheid van de *cloud*provider die gegevens host ... 48
6.1.5 Het bijzondere geval van elektronische communicatie ... 50
6.2 Europees kader (huidige situatie en projecten) ... 50
6.2.1 Gegevensbescherming ... 51
6.2.2 Bescherming van de consument en contractenrecht ... 60
6.2.3 Elektronische handel ... 62
6.2.4 Standaarden en certificering ... 64
6.2.5 Het Europese *Cloud*partnerschap ... 65
6.2.6 Lopende studies met betrekking tot Cloudcomputing ... 66

7 Aanbevelingen 67
7.1.1 Aansluiten op de Europese benadering 67
7.1.2 De dialoog met en tussen de economische actoren versterken 68
7.1.3 Contracten 68
7.1.4 Informatie voor het publiek 69
7.1.5 Veiligheid 71
8 Checklist 74
9 Modelcontractbepalingen 79
10 Tabel van de voornaamste actieve spelers 85
11 Bibliografie 98
12 Lijst van gebruikte afkortingen 102

Lijst van de afbeeldingen

Afbeelding 1 - De cloud geïllustreerd 6
Afbeelding 2 - Google datacenter (St. Ghislain, België) 14
Afbeelding 3 - Fiche risicobeschrijving 21
Afbeelding4 - risicobeheer 28
*Afbeelding 5 - Stand van zaken van de cloud*markt *in Europa* 33
Afbeelding 6 - IT-uitgaven in Europa 34
*Afbeelding 7 - Evolutie van de cloud*markt *in Europa - Pessimistisch scenario* 37
*Afbeelding 8 - Evolutie van de cloud*markt *in Europa - Lineair scenario* 38
*Afbeelding 9 - Evolutie van de cloud*markt *in Europa - Optimistisch scenario* 39
Afbeelding 10 – De cloud en de lopende evoluties 51
Afbeelding 11 – De risico-evaluatie (RA), de invoering van maatregelen (SM) en de raportering van incidenten (IR) (bron : Rapport ENISA, december 2012) 72

Lijst van de tabellen

Tabel 1 – Risicobeoordelingsschaal 29
Tabel 2 – Belgische normen (gegevensbescherming) 42

1 Inleiding

Dit document is het eindverslag van een studie over "*cloud*computing" (uit vertaaloverwegingen zullen wij deze term gebruiken eerder dan "informatica in de wolken". Deze studie werd uitgevoerd door Unisys in opdracht van de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie (FOD Economie)[1].

*Cloud*computing wordt vaak gezien als de opslag van gegevens op de servers van een externe host. De door middel van *cloud*computing opgeslagen gegevens, kunnen via verschillende elektronische toestellen en een internetverbinding worden geraadpleegd. Hier denken we vooral aan het groeiend gebruik van tablets en smartphones, maar ook aan zwaarder materieel zoals de pc's en servers van bedrijven of departementen die *cloud*computing gebruiken voor de centralisatie, consolidatie of back-up van hun gegevens.
Tal van toepassingen voor het "grote publiek" doen reeds een beroep op *cloud*computing: Hotmail, i*Cloud*, Facebook, enz. Zo gebruiken al veel burgers, vooral de "jonge generatie Y" deze technologie zonder er echt bij na te denken, en zullen die later natuurlijkerwijs gebruiken wanneer ze in een bedrijf of overheidsdienst een verantwoordelijke functie zullen vervullen.

Ondanks de onmiskenbare economische en technische voordelen van de aangeboden diensten, zowel voor bedrijven als particulieren, heeft *cloud*computing nog niet zijn volle rijpheid bereikt. De belangrijkste oorzaken hiervan zijn het gebrek aan vertrouwen met betrekking tot de beveiliging en bedrijfszekerheid van het systeem, alsook tot het billijke en duurzame karakter van de betrekkingen met de *cloud*provider. Sommigen durven zelfs zover te gaan de *cloud* voor te stellen als een nieuw feodalisme waarbij de leenman zich aan zijn leenheer onderwerpt (door zijn regels, berichten en reclame te aanvaarden) en de leenheer, in ruil, zich bewaker verklaart van de rechten van de leenman en hem onder zijn bescherming neemt. Binnen deze pessimistische visie, bestaat de enige vrijheid van de klanten in de "keuze van hun meester" en worden ze zelf een soort koopwaar: een verpachting van afhankelijke leden[2]. Behalve deze contractuele wanverhouding, is er ook de rechtsonzekerheid want de hosts van de *cloud*gegevens, de mobiele veranderende plaatsen waar de servers zich bevinden, bevinden zich vaak in landen met minder strenge voorschriften inzake gegevensbeveiliging en bescherming van de persoonlijke levenssfeer, met het reële of vermeende risico dat iemand zich toegang verschaft tot vertrouwelijke documenten zonder medeweten van hun wettelijke eigenaar.

Het komt er dus op aan alle stakeholders, zowel de regelgevende autoriteiten als de economische operatoren van de *cloud* en hun klanten (overheidsdiensten, grote en

[1] In het federaal België is de term FOD het equivalent van de term "ministerie" in de andere lidstaten van de Europese Unie.
[2] Wired opinion: When It Comes to Security, *We're* Back to Feudalism
www.wired.com/opinion/2012/11/feudal-security

kleine bedrijven, burgers) bewust te maken van de noodzaak een efficiënt en duurzaam rechtskader in te creëren voor *cloud*computing. Door dit kader, en het eventueel gebruik van zichtbare labels die op de toepassing ervan zouden wijzen, kunnen de gebruikers van het systeem weten dat de operatoren op contractueel niveau overeenkomstig "zo eerlijk mogelijke" criteria werken (fair trade of eerlijke handel), en op niveau van de beveiliging en gegevensbescherming overeenkomstig "zo veilig mogelijke" criteria, rekening houdend met de vooruitgang van state-of-the-art-technologie.

Deze studie werd uitgevoerd op basis van de volgende prioriteiten:

- De analyse van het begrip, de voordelen en de risico's van *cloud*computing
  1. Het begrip *cloud*computing (definitie en specifieke kenmerken)
  2. De risico's en de kansen (of voordelen) van *cloud*computing
  3. De mogelijke gevolgen van de ontwikkeling van *cloud*computing
  4. De *cloud*markt in België en in Europa
- De analyse van de juridische aspecten en de aanbevolen contractuele bepalingen
  1. Rekening houdend met wat bestaat in het Belgisch recht
  2. Rekening houdend met de hervormingen op Europees niveau
- De vermelding van de te nemen maatregelen door privateen publieke actoren en door de FOD Economie.

Het tussentijdse verslag van december 2012, heeft zich toegespitst op de eerste prioriteit, terwijl dit verslag de overige twee prioriteiten behandelt, na overleg met vertegenwoordigers van de Europese Commissie en met de lokale actoren van *cloud*computing in België (vergaderingen van december 2012 en februari 2013).

Wij wensen erop te wijzen dat tussen de toewijzing van de studie (zomer 2012) en de opstelling van dit verslag (eerste drie maanden van 2013), de Europese Commissie, gespecialiseerde Agentschappen van de Europese Unie, deskundigengroepen en lidstaten heel wat standpunten en verslagen ter zake hebben uitgegeven. Wij hebben het dus over een topic waar veel beweging in zit en waarbij de "grote landen" de neiging hebben zich op de nationale markt te verlaten zonder op een gemeenschapsdynamiek te wachten. Voor kleinere landen die niet over dezelfde interne (onder meer publieke) markt beschikken en waar de besluitvorming versnipperd is, maakt dat het alleen maar moeilijker om zich een innovatieve en zelfstandige weg te banen.

2 Samenvatting

*Cloud*computing is ***de toegang op verzoek tot computerresources via een netwerk***.

Het betreft hoofdzakelijk een dienst waarbij de klant (de gebruiker van de *cloud*) resources gebruikt die online beschikbaar worden gesteld (eerder dan dat die lokaal fysiek bij hem worden geïnstalleerd).

De *cloud*diensten kunnen in verschillende modellen worden geïmplementeerd: privaat (hier de klant de enige gebruiker van de ter beschikking gestelde resources), gedeeld (met een min of meer grote gemeenschap), en publiek (wanneer de dienst voor iedereen beschikbaar wordt gemaakt). Deze modellen kunnen olnderling worden gecombineerd in een hybride vorm.

De *cloud*diensten zelf bestaan uit verschillende combineerbare servicelagen: de infrastructuur die de rekenkracht, de opslagcapaciteit, de back-up en de bandbreedte biedt (IaaS), het beheerplatform (PaaS) waarmee online applicaties of software (SaaS) voor gegevensverwerking kunnen worden aangeboden.

Het economische principe van de *cloud* bestaat erin dat de klant geen zware kapitaalinvesteringen moet doen om over een geavanceerd IT-systeem te beschikken en te handhaven (zodat hij zich tegen voordelige voorwaarden op zijn kernactiviteit toeleggen). Hij betaalt alleen voor de diensten (operationele kosten) indien en wanneer hij die nodig heeft. Merk ook op dat sommige diensten, hoofdzakelijk bestemd voor het grote publiek, "gratis zijn in ruil voor reclame", zoals e-mail, sociale netwerken of zoeken op internet.

Het contractuele principe van de *cloud* gaat, naarmate men van de "private *cloud*" naar een "gedeelde of publieke *cloud*" evolueert van een onderhandelde overeenkomst naar een overeenkomst door lidmaatschap (waarvan men de voorwaarden te nemen of te laten zijn en deze soms eenzijdig door de provider kunnen worden gewijzigd) waardoor het noodzakelijk wordt een "billijk kader" in te voeren.

Het technische principe van de *cloud* of het online gebruik, vereist de mobiliteit van de gegevens (in de datacenters van de provider die op het gewenste moment over het nodige vermogen beschikken) wat voor de klant dus een verlies van controle kan betekenen op de exacte locatie waar ze zijn opgeslagen.

Naast het scheppen van nieuwe banen op de locaties waar de datacenters zijn gevestigd (nieuwe bedrijfstak die het verlies van werkgelegenheid binnen de bedrijfsorganisatie van de klanten compenseert), vloeien de voordelen van *cloud*computing voort uit de economische pricipe, met voor de klanten een beter beheer/verdeling van de kosten van elke taak, een soepeler besluitvorming (zonder begrotingstermijnen/beheer), een betere beveiliging tegen cyberaanvallen en/of

schade (brand, overstroming, inbraak) dan bij het gebruik van een geïsoleerde IT-infrastructuur op eenzelfde locatie.

De risico's zijn echter niet van de baan en hebben met de *cloud* - rekening houdend met de capaciteit van datacenters die de gegevens van duizenden klanten kunnen opslagen en dus volledige sectoren van een economie - een nieuwe dimensie gekregen. Sectie 4 van deze studie analyseert deze risico's per servicelaag (IaaS, PaaS, SaaS) en per implementatiemodel (privaat, publiek, hybride) en biedt een aanpak aan voor de risicobeoordeling, voor de herziening van het beveiligingsbeleid van de klant, voor de risicobeheersing en voor een gecontroleerd gebruik van de *cloud* met periodieke controles.

In het afgelopen jaar was de markt voor *cloudcomputing* het voorwerp van talrijke studies: hieruit blijkt dat deze een sterke groei optekent, met in Europa voor de publieke of gemeenschappelijke *cloud* een stijging van 4,6 miljard euro in 2011 tot 6,2 miljard euro in 2012 (of 33 % op een jaar tijd). Het Belgisch marktaandeel wordt geschat op 2,5 %, of 153 miljoen euro in 2012. Deze groei kan echter van conjuncturele aard zijn (de bedrijven willen bezuinigen) en zijn behoud of verdere ontwikkeling zal zowel afhankelijk zijn van de wereldeconomie (herstel, al dan niet uitweg uit de crisis), als van de afwezigheid van ernstige incidenten (geen negatieve reclame) en het uit de weg ruimen van remmingen, onzekerheden en gebrek aan vertrouwen ten opzichte van de *cloud*.

Wat dit laatste domein betreft, kan de regelgevende autoriteit een belangrijke rol spelen, naarmate zij (en de betrokken operatoren) al dan niet bijdraagt tot de invoering van een rechtskader ter bevordering van het vertrouwen in de markt. Drie scenario's zijn hier mogelijk: een pessimistisch, lineair of optimistisch scenario, waarbij de Belgische *cloud*markt tegen 2020 respectievelijk slechts een matige groei (880 miljoen euro), een lineaire groei (1,5 miljard euro) of een forse groei (2 miljard euro in 2020) zou optekenen.

Hoe dit nieuwe rechtskader definiëren? Bij de formulering van de huidige wetten werd geen rekening gehouden met *cloud*computing. De wetgeving - althans sinds de richtlijn 95/46 - vloeit voort uit het Europees recht waardoor een afzonderlijk lidstaat er minder belang bij heeft om een eigen wetgeving uit te werken. Terwijl de rol van elk van de partners van de *cloud* (klant en provider) al uit het bestaande recht kan worden afgeleid (verantwoordelijke voor de verwerking en verwerker), zal het rechtskader van de *cloud* door een aantal lopende Europese hervormingen of acties worden beïnvloed:

- Een nieuwe algemene verordening over gegevensbescherming (voorstel bekendgemaakt in 2012);
- De aanpassing van de rechten van de consument over het aan de *cloud* toevertrouwen van zijn privébestanden, en de toepassing van billijke contractuele bepalingen;
- De aanpassing van de voorschriften over elektronische handel en het beheer van op de *cloud* vastgestelde "illegale content";
- De bepaling van de standaarden van de "Europese *cloud*" op technisch niveau (met het oog op gegevensportabiliteit), op contractueel niveau (voor een billijke SLA of Service Level Agreement) en op beveiligingsniveau (rapportage van incidenten, maatregelen en audit);

- Een "Europees *cloud*partnerschap", niet voor de oprichting van een "Europese super*cloud*" maar om gemeenschappelijke regels en standaarden te bepalen met het oog op de harmonisatie van de specificaties (onder meer van de overheidssector), alsook de rechten ten opzichte van het aanbod van de *cloud*providers.

Al deze hervormingen of acties (in sommige landen soms door louter nationale initiatieven op zeer geïsoleerde voorbijgestreefd) zullen gepaard gaan met studies en verslagen (waarvan een aantal in uitvoering is en de resultaten verwacht worden in 2013-14). Ze zullen echter niet van de ene op de andere dag worden toegepast, dat zal jaren vergen.

Wat kan de Belgische regelgevende autoriteit doen?

Ten eerste moet zij één lijn trekken met de Europese aanpak, door de toepassing van een technologische monitoring, de opstelling van snel evoluerende samenvattende documenten en zich bereid verklaren tot elke vorm van bundeling (pooling) van *cloud*projecten met de overheidsdiensten van de buurlanden.

Er moet ook een samenwerking tot stand komen met de vertegenwoordigers van de *cloud*beroepen die in de verschillende regio's en specialisaties hun eigen organisatie moeten verbeteren structureren teneinde representatief te zijn voor de gehele sector.

Het kan nuttig zijn om vooruit te lopen op de verwachte conclusies in het kader van lopende studies en van het Europees *cloud*partnerschap door op basis van de werkzaamheden van de Commissie, van deze studie en van de werkzaamheden van de werkgroep "Artikel 29", een referentielijst op te stellen van billijke contractvoorwaarden, en door de lancering van een "Fair *Cloud*" label waarop de leden zich kunnen beroepen.

De publicatie van een "checklist" betreffende de te controleren punten bij een migratie naar de *cloud*, is eveneens wenselijk want. Naast een efficiënte voorlichting voor het publiek zal dat bijdragen tot een harmonisatie van de door de providers aangeboden voorwaarden.

Ten slotte, op het vlak van beveiliging zou de regelgevende autoriteit, op basis van de aanbevelingen van het ENISA, een verplichte rapportagecyclus moeten invoeren en doen controleren betreffende de incidenten (volgens bepaalde grenzen of ernstgraad), de inschatting van de risico's die hieruit kunnen voortvloeien en de te nemen maatregelen om deze risico's te beperken of te annuleren.

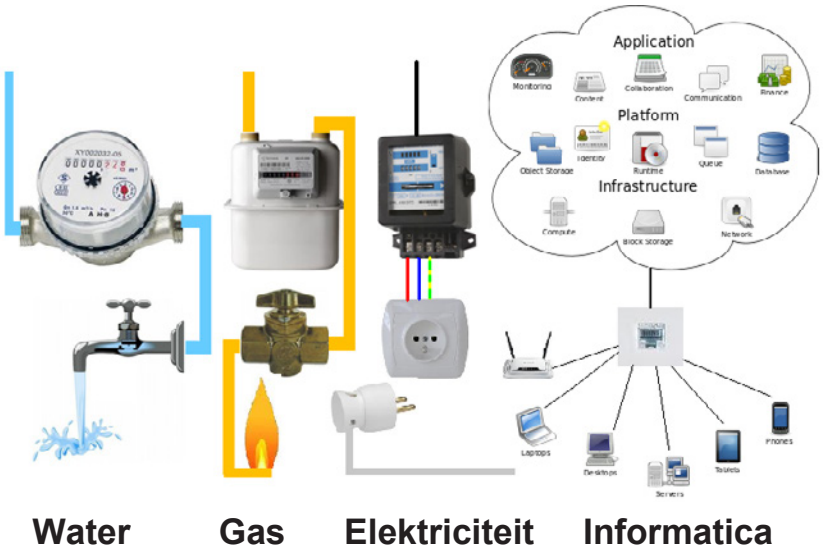
3 Wat is *cloud*computing?

3.1 Gedistribueerde computing

*Cloud*computing is een woord dat in de mode is en een waaier van technologieën kan omschrijven.
Het is dan ook belangrijk het begrip en de grenzen ervan te definiëren en te bepalen waardoor *cloud*computing innovatief is in verhouding tot de klassieke outsourcing.

Algemeen gesproken is *cloud*computing ***de toegang op verzoek tot computerresources via een netwerk***.

Met andere woorden, in een bedrijf dat op de "*cloud* geabonneerd is", wordt de dienst net als water, gas of elektriciteit ter beschikking gesteld: men hoeft zich alleen maar aan te sluiten om de dienst te kunnen gebruiken, facturatie gebeurt op basis van het verbruik. Tijdens perioden van niet-gebruik (verlof, vakantie) kan men de meter gewoon dichtdraaien.



Afbeelding 1 - De cloud geïllustreerd

Naast deze zeer algemene omschrijving kan *cloud*computing praktisch worden gedefinieerd aan de hand van zijn implementatiemodellen, van zijn verschillende servicelagen en van zijn andere specifieke kenmerken.

3.2 Diverse implementatiemodellen

Hierbij wordt een onderscheid gemaakt tussen de private *cloud* (voorbehouden aan een klant) en de publieke *cloud* (voor iedereen beschikbaar). Tussen deze twee diensten treft men de zogenaamde "gemeenschappelijke", "hybride" en zelfs "soevereine" modellen aan.

3.2.1 Private *cloud*

Dit model sluit het dichtst aan bij traditionele outsourcing: de klant is de enige gebruiker van de dienst die beschikbaar wordt gesteld. Het materieel (hardware: de servers, de kopieersystemen, firewall, enz.) kan door een *cloud*provider krachtens een outsourcingovereenkomst worden bestuurd en onderhouden. De toegang tot de resources kan met een fysiek of virtueel lokaal netwerk (wide area network), tot het personeel van de klant worden beperkt. Binnen dit model wordt de overeenkomst vaak onderhandeld (aangepast aan de specifieke behoeften van de klant).

3.2.2 Gemeenschappelijke *cloud*

Met dit model heeft een groep klanten toegang tot de resources van een zelfde provider. Meestal komt het aan bijzondere behoeften tegemoet zoals de naleving van wettelijke bepalingen of een specifiek beveiligingsniveau. De groep kan openstaan voor nieuwe klanten die dezelfde behoeften delen. De toegang tot dergelijke gemeenschappelijke diensten is meestal beperkt tot de gebruikers van het netwerk (wide area network).

3.2.3 Publieke *cloud*

Infrastructuur, platform en software worden geïnstalleerd en beheerd door de *cloud*provider die op het grote publiek (bedrijven, klanten of eindgebruikers) een beroep doet om de dienst te gebruiken. Deze kan tot op zekere hoogte gratis zijn, of betalend. De toegang tot deze dienst gebeurt meestal via internet.

3.2.4 Hybride *cloud*

De hybride *cloud* is een combinatie van private, gemeenschappelijke en publieke *clouds*. Een klant kan dan de gegevens en toegang tot de applicaties tussen de verschillende *cloud*types verdelen; deze toegang kan afhankelijk van het geval al dan niet beperkt zijn.

Het is ook mogelijk, en vaak onvermijdelijk, om de verschillende externe (publieke en/of private) *cloud*diensten met een interne infrastructuur te combineren. Vaak is voor de meeste bedrijven een volledig extern model niet realistisch, hun werking berust immers op een zware procesautomatisering die oorspronkelijk niet werd ontworpen om voordeel te trekken van de mogelijkheden van de *cloud*. Het hybride model dringt zich vaak op en de bedrijven moeten zich aan aanzienlijke investeringen verwachten om interne en externe, private en publieke diensten te integreren. Het vermogen om een hybride omgeving te beheren zal het verschil maken tussen succes en mislukking.

3.2.5 Andere categorieën: soevereine(?) *cloud*

Daarnaast bestaan nog andere categorieën zoals de zogenaamde "soevereine[3] *cloud*" die de publieke en gemeenschappelijke *cloud* op niveau van een land combineert om onder meer bij een specifiek rechts- en economisch kader aan te sluiten. Het zal niemand uitermate verbazen te vernemen dat de Franse regering haar Caisse de Dépôts opdracht heeft gegeven een oproep tot het indienen van projecten te leiden waarbij zij zelf partner is in diverse consortiums gevormd door Franse bedrijven[4]. Dit initiatief wordt geacht een alternatief te bieden voor de *cloud*diensten aangeboden door Amerikaanse operatoren, en de soevereiniteit te garanderen van de gegevens van de Franse overheidsbesturen en bedrijven, waarbij wordt aangenomen dat alleen een Franse *cloud*provider (onder directe controle van de Franse regering) op het nationale grondgebied infrastructuren mag installeren die de garantie bieden dat de opgeslagen gegevens veilig en wel op het nationale grondgebied zullen blijven. Hoewel de ontvankelijkheidscriteria van de projecten "niet-Franse" bedrijven niet uitdrukkelijk uitsluiten en naar de Europese samenwerkingsregels verwijzen, doet een dergelijk concept op gebied van het gemeenschapsrecht[5] uiteraard vragen rijzen. Dit voorstel heeft dan ook in Frankrijk veel kritiek gekregen, onder meer van Franse dochterondernemingen van buitenlandse bedrijven.

3.3 Diverse servicelagen

*Cloud*computing biedt een groot aantal oplossingen aan dat in drie grote servicelagen kan worden ingedeeld: infrastructuur, platform en applicaties (of software).

---

[3] Deze uitdrukking werd onder meer gebruikt door Isabelle Renard (advocate – cabinet Racine) ter aanduiding van de "Franse cloud" in haar uiteenzetting - Le cloud computing en France – 16 oktober 2012.

[4] Uit deze oproep, afgesloten op 2 november 2011, met als thema "Investissements d'Avenir, Développement de l'Economie Numérique", is een aantal initiatieven voortgevloeid waarbij de Franse overheid partner is: hoofdzakelijk de consortiums Numergy (Caisse des dépôts, SFR, Bull) en CloudWatt (Caisse des dépôts, Orange, Thales) waaruit de handelsvennootschap Andromède is ontstaan, het resultaat van een publiek-privaat partnerschap.

[5] IBM France heeft snel een "concurrentieverstoring aangevoerd en meende daarbij dat de Staat de belastingplichtigen technologische investeringen doet steunen, om nadien een kunstmatige prijsdaling te kunnen toepassen" - les Echos - http://archives.lesechos.fr/archives/2012/lesechos.fr/01/31/0201873061845.htm.
Om totaal andere redenen, hebben bepaalde Franse actoren zich afgevraagd hoe de komt dat de Franse Staat gelijke aandeelhouder kon zijn in twee concurrerende structuren (oorspronkelijk lid van het project gevormd met SFR, Dassault Systèmes uit welke de Staat zich uiteindelijk vanwege die dualiteit heeft teruggetrokken, terwijl één enkel project hem wenselijk leek http://www.latribune.fr/technos-medias/20120405trib000692197/dassault-systemes-claque-la-porte-du-cloud-a-la-francaise.html)

3.3.1 De infrastructuur (IaaS of "Infrastructure as a Service")

Dit aanbod geeft een gedeelde toegang tot een grote rekenkracht, opslagcapaciteit of communicatiesnelheid. Eerder dan al dit vermogen te moeten aankopen (vermogen dat hij vermoedelijk slechts af en toe, periodiek of voor kortstondige tests nodig heeft) koopt de klant een toegangsrecht waarmee hij op het gewenste moment over al de nodige rekenkracht, opslagcapaciteit of communicatiesnelheid kan beschikken.

3.3.2 Het platform (PaaS of "Platform as a Service")

Dit aanbod geeft toegang tot een ontwikkelplatform: een specifieke omgeving waar de gebruiker applicaties kan schrijven en uittesten die later op dit platform of op een gelijksoortige installatie zullen draaien. Dat is bijvoorbeeld het geval voor een sociaal netwerk of voor een ontwikkelaar die een platform aanbiedt waar gebruikers applicaties kunnen ontwikkelen die bestemd zijn om met dit netwerk, het ecosysteem of het functionele universum van deze ontwikkelaar samen te werken.
Het platform (middleware) bepaalt de standaarden waarmee men op een ruime en interoperabele wijze talrijke klanten kan bereiken en hun keuze qua software uitbreiden. Uiteraard kan dergelijke PaaS-service op een IaaS-infrastructuur worden gehost.

3.3.3 De software (SaaS of "Software as a Service")

Hier krijgt elke gebruiker via zijn webbrowser of een andere clienttoepassing toegang tot een complete en operationele applicatie. . Hierdoo verdwijnt of vermindert de noodzaak om op elke terminal van de klant software te installeren. Bovendien is de SaaS-service meestal voor een zeer brede waaier van apparaten beschikbaar: pc's, tablets, smartphones, enz. Zo kan een jong bedrijf bijvoorbeeld over een krachtige klantenbeheersoftware beschikken die het voor zijn exclusief gebruik niet had kunnen verwerven.

Uiteraard kan deze SaaS-service ook op een PaaS-platform en een IaaS-infrastructuur worden gehost, wat betekent dat men ook "trapsgewijs" voor elke servicelaag verschillende overeenkomsten en providers kan hebben: zo kan bedrijf A toegang bieden tot een software die het van bedrijf B heeft gekocht dat de standaarden gebruikt van het platform C en dat het doet draaien op een infrastructuur bestuurd door bedrijf D.

3.4 Diverse financieringswijzen

Kenmerkend voor *cloud*computing is de betaling van de leveringen "op basis van het verbruik". Een aantal diensten is echter, tot nu toe, hetzij altijd gratis (zoals zoeken op internet via een zoekmotor), hetzij meestal gratis (zoals de basistoegang tot een sociaal netwerk), hetzij gratis binnen een bepaald volume of aantal pagina's (zoals e-mail of e-agenda). De "gratis" diensten kunnen slechts door reclame worden gefinancierd of door het gebruik van het profiel zelf van hun gebruikers als "verhandelbaar kapitaal". Hieruit vloeit voort dat de gratis dienst op lange termijn alleen maar haalbaar is wanneer die dient als lokmiddel of drager van andere activiteiten en een grote massa gebruikers kan concentreren of samenbrengen: gratis *cloud*computing, bestemd voor het grote publiek, is een domein bij uitstek waar het potentieel van concentratie in handen van enkele belangrijke actoren enorm is.

3.5 Specifieke *cloud*kenmerken

Omdat een algemene definitie van *cloud*computing altijd vaag zal blijven, kunnen wij voor een beter begrip naar zijn belangrijkste kenmerken verwijzen waarvan sommige al eerder in dit document werden toegelicht en andere nieuw zijn.

3.5.1 Basiskenmerken:

- De klant van de *cloud* heeft met zijn eigen randapparatuur (desktop, laptop, tablet, telefoon, online-server) toegang tot drie servicelagen (infrastructuur, platform, applicaties);
- Behalve de randapparatuur, zijn de infrastructuur, de platforms en de applicaties de eigendom van de *cloud*provider en geen eigendom van de gebruiker;
- De gebruiker interageert met de geleverde diensten via een netwerk, meestal via internet. De gegevens bevinden zich op afstand: de gebruiker heeft geen directe controle op de gegevensdrager;
- De toegang is van overal mogelijk (ongeacht waar de randapparatuur zich bevindt);
- De toegang is op elk moment van de dag mogelijk. Er zijn geen "kantooruren" noch "werkuren" in verhouding tot rust- of periodes van onbeschikbaarheid. Net als voor water of elektriciteit, is de infrastructuur in regel constant beschikbaar;
- De infrastructuur zorgt voor de gegevensopslag op afstand, terwijl de softwareapplicaties de toegang of de verwerking mogelijk maken;
- Het gebruik van de geleverde software voor de toegang tot en de verwerking van gegevens is op verzoek;

- De betaling van de diensten gebeurt normaliter op basis van hun gebruik (overgedragen volumes, schijfruimte, aantal gebruikers) waardoor nieuwe klanten de kosten kunnen besparen die voortvloeien uit exclusief gebruik. Sommige providers bieden het grote publiek een volledig gratis toegang aan (hoewel beperkt in volume) en financieren deze door reclame.

3.5.2 Nieuwe elementen

Er zijn echter nog andere, bijzonder belangrijke, kenmerken die *cloud*computing van de traditionele outsourcing onderscheiden:

- **Geografische veranderlijkheid**
  Het gebruik van de diensten, in het bijzonder de infrastructuur, wordt in een servernetwerk dynamisch geoptimaliseerd, waardoor de locatie van de gegevens en van de machine die op een gegeven moment de verwerking ervan verzekert, vaak verandert (butien medeweten van de gebruiker die zich er meestal niet over hoeft te bekommeren). Deze dynamische verdeling komt aan een zekere behoefte tegemoet. Een effectieve "mondiale" distributie van de netwerkinfrastructuur, is de meest efficiënte oplossing, en wel om de eenvoudige reden dat - vanwege de wenteling van de aarde en de verschillende culturen of behoeften - de enen druk werken terwijl de anderen slapen, eten of weinig of niets doen. Zo komt het dat de operatoren de werkbelasting constant van het ene datacenter naar het andere migreren om tot een optimale benutting van de hardware te komen. Dit heeft wel zijn gevolgen op niveau van het rechtskader dat van toepassing is op de gegevensverwerking.
- **Flexibiliteit**
  Dat is het vermogen de dienst (infrastructuur, platform, applicaties) constant aan de veranderende behoeften aan te passen, zoals de door een applicatie te verwerken hoeveelheid gegevens, het aantal simultane gebruikers die kunnen interageren, enz. Hier kan een onderscheid worden gemaakt tussen het "horizontale" aanpassingsvermogen (het aantal te verwerken transacties of verzoeken) en het "verticale" aanpassingsvermogen (de grootte van de transacties).
- **Deling**
  In tegenstelling tot de traditionele outsourcing, worden de resources gebundeld om beschikbaar te worden gemaakt voor een variërend en onbepaald aantal "consumenten". Hierbij heeft het gebruik van de enen een invloed op de prestaties die de anderen kunnen bekomen, aangezien de fysieke en virtuele resources continu opnieuw worden toegewezen op basis van de vraag worden hertoegewezen.
- **Specifieke contractuele praktijken**
  Op gebied van de overeenkomsten die tussen *cloud*provider en gebruiker worden gesloten, sluiten de kenmerken aan bij die van outsourcing: een recurrente dienstenovereenkomst voor de volledige of gedeeltelijke uitbesteding van het beheer van het informatiesysteem.

Hoe meer we echter van de "private *cloud*" (op maat) naar de "publieke *cloud*" evolueren, hoe meer de overeenkomst wegheeft van een overeenkomst van lidmaatschap, dit wil zeggen een lijst van voorwaarden die te nemen of te laten zijn. In feite beperkt het lidmaatschap zich tot een klik met de muis in een vakje "ik aanvaard de voorwaarden" waarmee men zijn akkoord geeft.

Bovendien gebeurt het dat de *cloud*provider zich hierbij het recht voorbehoudt om de contractvoorwaarden eenzijdig te wijzigen waarbij de gebruiker, in zekere zin geïnformeerd, zijn lidmaatschap stilzwijgend vernieuwt volgens het principe "wie zwijgt stemt toe".

Deze kenmerken onderscheiden de *cloud* van de traditionele outsourcingovereenkomst die meestal bepalingen opneemt zoals:

- Regelmatige meting en mededeling ann de gebruiker van het dienstenniveau ;
- Op verzoek, de onafhankelijke audit van de prestaties;
- Boetes voor gebrekkige prestaties;
- Garanties van omkeerbaarheid.

Er moet worden opgemerkt dat het voor de *cloud*provider vaak technisch niet anders kan. Wij hebben hier te maken met een situatie die vergelijkbaar is met de distributie van water, gas of elektriciteit: wanneer duizenden en zelfs miljoenen gebruikers een infrastructuur delen, is het moeilijk om bijzondere voorwaarden te onderhandelen want de provider kan de gebruikers individueel niet bevoorrechten. Wat wel voorkomt is dat de provider verschillende gebruiksklassen bepaalt die afhankelijk van hun abonnement al dan niet bepaalde voordelen genieten.

3.5.3 Ecologische aspecten

Het is geruststellend te hopen dat het gebruik van de *cloud* zal toelaten om de versnippering te verminderen van individuele machines die vaak - in het geval van kleine servers - meestal "leeg" draaien.

Sommige verslagen benadrukken dat de nieuwe generatie machines die in de *cloud* datacenters worden gebruikt, ook energie-efficiënter zijn[6].

De actoren van de *cloud* voeren ecologische en energetische voordelen aan als verkoopargument, waarbij sommigen wijzen op besparingen gaande tot 90 %, wetende dat inzake reclame "tot" nooit een vaste verbintenis inhoudt ("*our system cuts power usage by up to 90 % compared to traditional systems*"[7]).

Om een reëel globaal verschil te kunnen vaststellen, zou de randapparatuur fors vooruitgang moeten maken (bijvoorbeeld een meer algemeen gebruik van tablets

[6] Verslag van de deskundigengroep in opdracht van de Europese Commissie – DG Informatiemaatschappij en Media (Lutz Schubert et al.) “The Future of cloud Computing (opportunities for European cloud Computing Beyond 2010)” p. 14
[7] Amplidata op Belgium Cloud http://www.belgiumcloud.com/?page_id=1956

zonder interne harde schijf) want een pc of een server gebruikt als randapparatuur in een netwerk, verbruikt niet minder dan hetzelfde toestel op zich.. Wij hebben echter vastgesteld dat de meeste bedrijven die een beroep doen op de *cloud*, zich verplicht zien een hybride oplossing te kiezen (de "100 % *cloud* is niet aan de orde"). De nieuwe randapparatuur komt ter aanvulling van de traditionele randapparatuur, niet ter vervanging.

Sommigen wijzen dan ook op de keerzijde van de ecologische medaille en voeren hierbij de volgende argumenten aan[8]:

- De *cloud* is samengesteld uit grote en ver verwijderde datacenters die via netwerken met grote bandbreedtes met elkaar verbonden zijn en waarbij elk samenstellend onderdeel energie verbruikt.
- Deze grote "·datacenters" zijn energieverslindend en hun werking is onderworpen aan extra vereisten (vloeroppervlakte, klimaatbeheersing, koeling, ventilatie, bescherming, nachtverlichting, bewaking);
- Een groot gedeelte van de energie wordt toch verspild en dient alleen om tegemoet te komen aan piekbelastingen;
- Behalve het energieverbruik, moet de installatie redundant worden uitgevoerd om een ononderbroken werking te kunnen garanderen, met batterijen en noodstroomaggregaten die een aanzienlijke hoeveelheid verontreinigende stoffen bevatten (en uitstoten wanneer in werking);
- Deze ecologische voetafdruk wordt toegevoegd aan het voorgaande en komt niet in vervanging ervan.

Eén van de grote actoren gevestigd in België (Google) slaat een heel andere toon aan. Hun versie is dat geen ontkenning, eerder een illustratie van de uitzondering die deze vestiging vertegenwoordigt: "ons datacenter (van St. Ghislain dicht bij Bergen) is het eerste datacenter ter wereld dat zonder koeling functioneert en in plaats daarvan gebruik maakt van een systeem op basis van de verdamping van industrieel water van een nabij kanaal. Dat helpt onze computers om met een optimale efficiëntie te draaien en hun totaal energieverbruik te verminderen"[9].

[8] Isabelle Renard – Le cloud computing en France – 16 oktober 2012 (uiteenzetting).
[9] http://www.google.com/about/datacenters/locations/st-ghislain/

Afbeelding 2 - Google datacenter (St. Ghislain, België)

3.5.4 Economische aspecten

Uit het oogpunt van de klant

- **Beperking van de aanloopkosten**
  De beperking van de kosten voor de aankoop en het onderhoud van een IT-infrastructuur, wordt voorgesteld als de belangrijkste stimulans voor potentiële *cloud*afnemers. Deze beperking (of verwijdering) van de aanloopkosten is bijzonder voordelig voor kmo's en start-ups die op deze wijze hun financiële middelen kunnen besteden aan de ontwikkeling van hun kernactiviteiten en onmiddellijk, zonder zware investeringen, gebruik kunnen maken van geavanceerde IT-oplossingen.

- **Sneller "operationeel"**
  Om dezelfde redenen, vooral voor jonge bedrijven (kmo's en start-ups) wordt de inspanning om operationeel te zijn en de hiervoor nodige tijd (time to market), aanzienlijk ingekort. Zo kunnen ze onmiddellijk concurreren met gevestigde bedrijven. Voor bestaande bedrijven biedt de *cloud* de mogelijkheid om concurrerend te blijven zonder te veel tijd en resources te hoeven besteden aan change management.

- **Facturatie op basis van het gebruik.**
  Het gebruik van de *cloud* is een voorbeeld van de overschakeling van kapitaalinvestering (CAPEX) naar operationele kosten (OPEX).

- **Beperking van de totale eigendomskosten (TCO)**
  *Cloud*providers benadrukken de aanzienlijke totale besparingen (totale eigendomskosten of "TCO") verbonden aan het gebruik van de *cloud* in plaats van een traditionele IT-infrastructuur: "*our system reduces TCO with up to 70 % compared to traditional systems*"[10]. Dergelijke besparingen vormen uiteraard een aanzienlijk voordeel, vooral in tijden van crisis of van (publieke en private) budgettaire bezuinigingen
  In sommige uiteenzettingen hebben de vertegenwoordigers van de Europese Commissie en van sommige regeringen het zelfs over mogelijke besparingen (voor de overschakeling van de overheidssector op de *cloud*) van vrijwel 90 %[11]. Maar ook dan moeten de kosten, voor zover de opdracht van de betrokken ambtenaren niet wordt beëindigd, volledig op andere projecten kunnen worden hertoegewezen. De verantwoordelijke van de publieke *cloud* in Noorwegen (land met 5 miljoen inwoners) vermeldt een studie uitgevoerd in opdracht van de regering volgens welke de overschakeling op de *cloud* een jaarlijkse besparing zou vertegenwoordigen van 825 miljoen euro[12]. Uiteraard is het besparingspotentiëel afhankelijk van het diensttype (functionaliteit, SLA, garanties) en van het vermogen de kosten verbonden aan het oude systeem volledig te besparen (of aan andere taken toe te wijzen) onder meer op niveau van human resources.

Uit het oogpunt van de *cloud*actoren

- **Een aanzienlijke investering**
  De oprichting van een publieke *cloud* door een "verkoper van resources" zal een grotere begininvestering vergen dan voor een privé-infrastructuur: enerzijds moet hij voldoende flexibel zijn om op de zeer uiteenlopende behoeften van zijn klanten te kunnen inspelen en hun een ruime interoperabiliteit aan te bieden, en anderzijds moet hij voldoende schaalbaar zijn om tegemoet te komen aan een variabel gebruik in volume zonder vooraf bepaalde grenzen. De noodzakelijke permanente beschikbaarheid en invoering van de nodige beveiligingsmiddelen en redundantie verhogen zijn investeringskosten.

  Het bedrag van de investering varieert sterk afhankelijk van de betrokken actoren. Het feit een toonaangevend bedrijf zoals Google in België te hebben aangetrokken - dat er één van zijn drie grootste Europese datacenters heeft gevestigd, vertaalt zich als volgt:
  - Een investering van een kwart miljard euro;
  - 85 bedrijven en onderaannemers actief gedurende twee jaar voor de bouw van het datacenter (ongeveer 2.000 banen gedurende deze periode);

[10] Amplidata op Belgium Cloud http://www.belgiumcloud.com/?page_id=1956
[11] Uiteenzetting van dhr. Ken Ducatel, Eenheidshoofd "Software & services" – DG Connect - op het ECIS-symposium (European Committee for Interoperable Systems) "Bringing the cloud down to earth" van 24 april 2013.
[12] Uiteenzetting van mevr. Katarina de Brisis, Deputy Director General, belast met de cloud, - Ministry of Government Administration and Reform, Noorwegen – ECIS-symposium van 24 april 2013

- 120 vaste banen sinds het datacenter operationeel is (om de 24/7 werking ervan te verzekeren).

- **Facturatie op basis van het gebruik**
  De afstemming van de kosten op het effectief gebruik van de resources, vereist een ondersteuning van kwaliteit van de gebruikers en een nieuw facturatiesysteem verbonden aan de gebruiksindicatoren.

- **Een "variabele" return on investment**
  Volgens analisten is dit voor veel investeerders een kritiek punt dat momenteel niet kan worden gegarandeerd. De return on investment is afhankelijk van de financieringswijze (door de klanten of door gemengde reclame). Aangezien de reclameresources direct verbonden zijn aan de gebruikersmassa, kan zich dat voor de *cloud*actoren vertalen in een "wedloop" om klanten te winnen, door van meet af aan aantrekkelijke voorwaarden aan te bieden zonder dat de haalbaarheid van het systeem verzekerd is. Als gevolg hiervan zal er onvermijdelijk een tijdstip komen waarop de voorwaarden moeten worden herzien, wat de klant in een lastig parket kan brengen: ofwel vertrekt hij (zoals hij daar recht op heeft) waarbij hij hoge kosten kan oplopen (vanwege de moeilijkheid de gegevens naar een andere provider te migreren die niet noodzakelijkerwijs een totale interoperabiliteit, open standaarden, en procesverandering aanbiedt), ofwel blijft hij en betaalt meer.

3.5.5 De aan de *cloud* verbonden functies of beroepen

De aan de *cloud* verbonden economische en technische activiteiten bieden de actoren (en personen) de mogelijkheid diverse functies en beroepen uit te oefenen en vormen hierdoor een bron van werkgelegenheid. Een deel van deze werkgelegenheid (hoofdzakelijk de banen die nodig zijn voor de werking, de beveiliging en de audit van de provider) kunnen in de plaats komen van traditionele IT-banen in de bedrijven of departementen, en kunnen bij die gelegenheid d worden gedelocaliseerd (rekening houdend met de mobiliteit van de *cloud*infrastructuren). Dit punt moet in aanmerking worden genomen om deze activiteit in België aan te trekken en te behouden.

***Cloud*provider** is hij die aan zijn klanten een *cloud*dienst aanbiedt, en dit hetzij via een applicatiegerichte technische interface (API's of PaaS-platforms), via het aanbod van (gedeelde) virtuele machines of via het aanbod van de directe toegang, al dan niet privaat, tot infrastructuurresources (IaaS: rekenkracht, opslag, enz.) van een platform of applicaties. De beroepen zijn talrijk en gevarieerd, afhankelijk van de omvang van het datacenter: tijdens zijn bouw (bouwvakberoepen) en tijdens zijn werking (ingenieurs, bestuurders, operatoren, bewakingsagenten, enz.).

***Cloud*integrator** (of "doorverkoper") is de dienstverlener die zich belast met de operationele implementatie van een *cloud*dienst bij een klant. Hij kan voor de klant een unieke interface ontwikkelen die toegang geeft tot diverse *cloud*types (bijvoorbeeld wanneer dezelfde klant verschillende diensten gebruikt voor zijn klantenbeheer (CRM), zijn e-mail, zijn gegevensopslag). Hij biedt de klant ondersteuning bij de keuzen die het best bij zijn behoeften aansluiten. Hij kan zich belasten met opleidingstaken, change management, en dergelijke.

De integrator kan ook een **consultant** zijn, hoewel dergelijke consultancy onafhankelijk van elke verkoop moet gebeuren. Ook hier gaat het erom, vooral tijdens voorafgaande studies of audits, de diensten te beoordelen die het best aansluiten bij de behoeften van de klant, met inachtneming van de economische (aan wie de gegevens toevertrouwen, met welk voordeel), technische (met welke standaarden, interoperabiliteitsniveau) en juridische perspectieven (binnen welk contractueel en rechtskader, binnen welk Europees ecosysteem en met welke garanties).
Deze analyse moet uitvoerig zijn, afhankelijk van de aard van de bedrijfsactiviteiten: het verwachte beveiligingsniveau van de gegevens, de transparantiegraad van het systeem, de prestaties en de beschikbaarheid van de diensten, de overeenstemming van de bedrijfstoepassingen met het model van *cloud*computing en het beheer van het risico "gevangene te worden van zijn provider (vendor lock-in)".
Een *cloud*dienst gebruiken om standaardapplicaties en de opslag van documenten (de burotica-applicaties van Google bijvoorbeeld) beschikbaar te maken is eenvoudig, maar *cloud*diensten in het kritische IT-systeem van een productiebedrijf integreren en hier werkelijk voordeel uit trekken is heel wat complexer.
Bedrijven die sommige van hun applicaties naar de *cloud* migreren, hebben nood aan deskundig advies om de door de providers aangeboden SLA's (dienstenniveau-overeenkomst) te beoordelen. Hoewel de overeenkomsten thans hoofdzakelijk de provider beschermen, zal deze situatie snel veranderen onder druk van de klanten die van de provider bepalingen en voorwaarden zullen gaan eisen aangepast aan hun behoeften, alsook een transparanter beheer.

De expertise over **gegevensbeveiliging en audit** is een beroep op zich. De grootste klanten zullen van geen compromis willen weten en strenge eisen stellen aan hun provider(s) om de nodige capaciteit en prestaties te leveren voor een hoog tevredenheidsniveau bij de gebruikers en tegelijkertijd de gegevensbeveiliging van de gegevens. Zo zullen ze zeker eisen om bepaalde parameters op niveau van de algemene werking van het systeem te kunnen controleren en meten.

Het **softwarehuis** kan applicaties ontwikkelen (of bestaande applicaties aanpassen) die op de *cloud* kunnen draaien. Het kan die software vervolgens bij een *cloud*provider installeren zodat deze die aan zijn klanten kan aanbieden en het softwarehuis in ruil een gedeelte terugbetalen van de rekeningen betaald door de klanten die de SaaS-service gebruiken. Zo kan een softwarehuis bij verschillende *cloud*providers software voor klantenbeheer of projectmanagement installeren. Deze nieuwe markt biedt softwarehuizen een alternatief aan voor de directe verkoop van licenties aan de finale klant.

In dit kader zijn de aanpassing of het herschrijven van applicaties een niet uit te vlakken activiteit. Een van de voordelen van de *cloud* is de dynamische aanpassing van de resources in functie van de werkbelasting van de toepassingen. Deze aanpassing is des te belangrijker naarmate de belasting varieert. De bedrijven hebben er dus baat bij (zowel uit financieel oogpunt als uit het oogpunt van de dienstkwaliteit die zij hun personeel, klanten en leveranciers aanbieden) om dit soort applicaties van hun interne infrastructuur, noodzakelijkerwijs overgedimensioneerd om variaties in werkbelasting te kunnen opvangen, naar een *cloud*dienst te migreren. Dergelijke strategie zal echter pas efficiënt zijn indien de applicaties (en in het bijzonder hun architectuur) aan de specifieke functionele kenmerken van de *cloud* zijn aangepast. De ontwikkeling van deze nieuwe toepassingen moet hier dan ook rekening mee houden.

Ook voor andere **leveranciers van *cloud*apparatuur of *cloud*componenten** (hardware of software) houdt deze nieuwe markt een economische kans in: servers, opslagsystemen, telecominfrastructuur, beveiliging, ontwikkelomgevingen, beheerprogramma van virtuele serverparken door lastverdeling, enz.
Wat geldt voor de applicaties geldt eveneens voor de infrastructuur, in de mate waarin bedrijven het meest op het hybride model zullen terugvallen en eigen datacenters zullen blijven ontwerpen en beheren. Met andere woorden, de concepten en technieken waarop de werking van de *cloud* berust (bijvoorbeeld virtuele oplossingen en de dynamische herverdeling van de resources) zullen ook in de particuliere datacenters worden toegepast. Ook hier betreft het een waardevolle en economisch te benutten beroepservaring.

Ten slotte is op niveau van de **directe gebruikers** of "eindgebruikers" een aantal competenties vereist om het gebruik van de *cloud* te contracteren (besluitvorming), te controleren, de rechten ervan te beheren, op te leiden en de economische impact van het gebruik van de *cloud* te beoordelen.

4 Kansen en risico's van *cloud*computing

*4.1 Kansen van cloud*computing

De *cloud* biedt tal van kansen en voordelen die voortvloeien uit de kenmerken die wij hierboven hebben toegelicht:

- Een beperking van de kapitaalinvestering verbonden aan de uitbouw van een IT-infrastructuur en/of de verwerving van softwarelicenties;
- Het bedrijf hoeft zich niet te bekommeren om zijn IT-systeem maar kan zich toeleggen op zijn klanten, op de efficiëntie van zijn personeel (gebruikers van de *cloud*) en hun behoeften, dus op zijn kernactiviteit;
- De kosten worden operationeel en zijn verbonden aan de prestaties en aan de effectieve bedrijfsactiviteit (geen activiteit = geen kosten; grote bedrijfsactiviteiten die winsten voortbrengen = proportionele kosten);
- Het bedrijf geniet schaalvoordelen verbonden aan de deling van de resources met talrijke andere gebruikers (beperking van de eenheidskosten);
- Het bedrijf geniet stabielere of "uitgevlakte" prestaties die over een groot aantal gebruikers zijn verdeeld die niet allen tegelijkertijd werken.
- De gebruikers begrijpen beter de direct aan hun activiteit verbonden kost (de lasten kunnen op basis van objectieve criteria in het bedrijf worden verdeeld);
- Het bedrijf kan makkelijker zijn reële kosten doorfactureren aan zijn klanten, en kan deze eenvoudiger rechtvaardigen;
- Met een betere kostenbeheersing (die meer operationeel worden) gaan een vermindering van de algemene kosten en een betere controle van de operationele winsten gepaard (omzet - operationele kosten en algemene kosten);
- Het vooruit geplande beheer van de behoeften wordt er aanzienlijk gemakkelijker op: men hoeft zich niet meer te bekommeren over hoe op eventuele belastingpieken te anticiperen en deze op te vangen;
- Wanneer het erop aankomt een applicatie te testen te beslissen om deze al dan niet te gebruiken, kan het bedrijf sneller en flexibeler optreden. Een nieuwe klantendienst kan hierdoor sneller en met een minimaal risico worden uitgerold;
- Het bedrijf is verlost van de dwingende noodzaak zijn infrastructuren, platforms en applicaties periodiek te "upgraden". Het bedrijf hoeft niet langer aanzienlijke "eenrichtingskosten" te dragen: het bedrijf betaalt enkel voor wat het verbruikt en wanneer de vraag niet langer bestaat kan men opnieuw op de vorige situatie overschakelen;
- Het gevoel van veiligheid boet er niet bij in; integendeel het gaat er eerder op vooruit, vooral in het geval van kmo's en individuele gebruikers die geen dagelijkse back-up maken van hun gegevens: voor wie al eens werd geconfronteerd met diefstal van zijn pc of crashen van zijn harde schijf, hoeven de voordelen van de *cloud* geen betoog: e-mails, contacten, documenten en foto's gaan niet langer verloren. Met een nieuwe pc vindt men ze zo terug op de *cloud*.

Deze kansen of voordelen bestaan zowel in de publieke als in de private sector. Voor bijna alle providers en voor een groot deel van de IT'ers vertegenwoordigt *cloud*computing aanzienlijke voordelen, met bovendien - voor de eersten - de kans om een nieuwe economische activiteit te ontwikkelen.

In dit kader worden de waarschuwingen van beveiligingsdeskundigen, de bezwaren van juristen over de gegevensbescherming en de behoefte aan rechtszekerheid met betrekking tot de verwerking en opslag van gegevens vaak gezien als misplaatst. Toch moeten de risico's alsook het rechtskader van de *cloud* en de regels die eruit voortvloeien, worden onderzocht, niet om de overschakeling op de *cloud* te hinderen, maar om de gehele bedrijfstak te omkaderen en betrouwbaarder te maken.

*4.2 Risico's van cloud*computing

4.2.1 Classificatie van de risico's

Het is nuttig de risico's van *cloud*computing op basis van het servicemodel (IaaS, PaaS of SaaS) of het implementatiemodel (publiek, privaat, hybride) te klasseren. Deze classificatie laat toe zich toe te spitsen op de risico's die voor elke situatie echt relevant zijn.

4.2.1.1 Classificatie volgens het servicemodel

De afnemer die op een *cloud*provider een beroep doet en tegelijkertijd eigenaar blijft van de IT-activa gehost door de *cloud*, doet gedeeltelijk afstand van de controle en zichtbaarheid op de personen, processen en technieken gebruikt voor het beheer van deze activa. Bij de identificatie en beoordeling van de risico's moet het zichtbaarheidsniveau in aanmerking worden genomen. Elk servicemodel van de *cloud* heeft namelijk zijn eigen zichtbaarheid die varieert afhankelijk van het aantal lagen van het servicemodel dat door de *cloud* wordt beheerd. Het IaaS-model biedt een groot zichtbaarheidsniveau aan de afnemer omdat het alleen de infrastructuur vervangt, terwijl het SaaS-model een zwakkere zichtbaarheid biedt omdat het behalve de infrastructuur ook de systeemsoftware, de gegevens en de applicaties vervangt. Voor het IaaS-model beheert de afnemer van de *cloud*diensten zelf de risico's verbonden aan het beheer van de systeemsoftware, de gegevens en de applicaties, terwijl voor het SaaS-model hij dit beheer uitbesteedt op basis van SLA-overeenkomsten (SLA – *Service Level Agreements*) met zijn provider.

De risico's verbonden aan het gebruik van de *cloud* zijn cumulatief afhankelijk van het servicemodel waaraan ze verbonden zijn: het IaaS-model houdt een aantal specifieke risico's in verbonden aan het beheer van de infrastructuur; het PaaS-model houdt dezelfde risico's in met daarbij de aan dit model eigen specifieke risico's eigen aan het beheer van de systeemsoftware; ten slotte houdt het SaaS-model daarbij nog de specifieke risico's in verbonden aan het beheer van de gegevens en de applicaties.

4.2.1.2 Classificatie volgens het implementatiemodel

Sommige risico's zijn specifiek verbonden aan het implementatiemodel van de *cloud*: privaat, publiek of hybride. De beslissende factor is het vertrouwensniveau tussen de

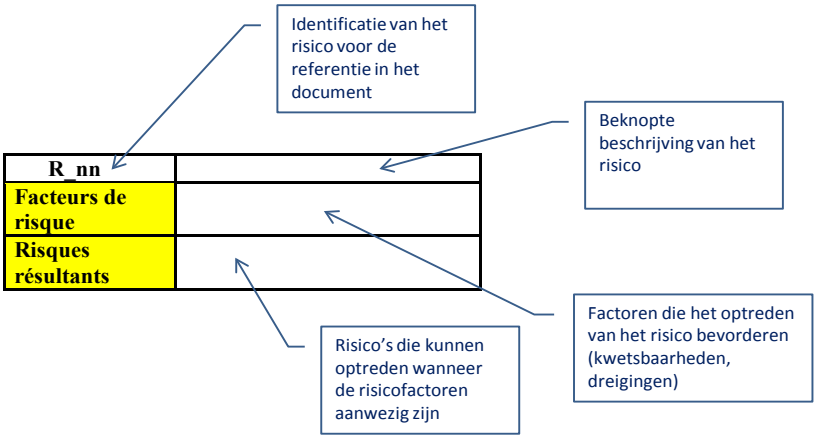
deelnemers (de *cloud*provider en de afnemer van de *cloud*diensten; de afnemers onderling). Meerbepaald wordt een publieke *cloud* gebruikt door afnemers die niets met elkaar gemeen hebben en door geen enkele vertrouwensband verbonden zijn, terwijl dat voor de afnemers van een private *cloud* wel het geval kan zijn. De risico's verbonden aan het gebruik van de *cloud* zijn in beide gevallen verschillend.

4.2.1.3 Generieke risico's

Sommige risico's verbonden aan het gebruik van de *cloud* zijn generiek, d.w.z. dat ze noch van het servicemodel noch van het implementatiemodel afhankelijk zijn.

4.2.2 Fiches risicobeschrijving

De risicobeschrijvingen worden voorgesteld in de vorm van fiches. Een fiche is als volgt opgebouwd:



Afbeelding 3 - Fiche risicobeschrijving

4.2.2.1 Risico's ingedeeld volgens servicemodel

4.2.2.1.1 IaaS

Specifieke risico's van het IaaS-model:

R_01	**Grensoverschrijdende overdracht (EU/EER)**
Risicofactoren	De *cloud*providers zijn vaak multinationals en de gegevens kunnen opgeslagen zijn in landen waar de wetgeving verschilt van die waaronder de afnemer ressorteert, vooral wat de bescherming betreft van persoonsgegevens. De autoriteiten van het land waar de gegevens zijn opgeslagen, kunnen toegang eisen tot de gegevens, soms zonder garantie dat die toegang gegrond is.
Eruit voortvloeiende risico's	• Onrechtmatige bekendmaking van gegevens • Strijdig met de wetten

R_02	**Multi-*tenancy***
Risicofactoren	Om de voordelen van de *cloud* te kunnen genieten, deelt een klant de resources (opslagruimte, hardware, netwerk, enz.) met andere klanten. De resources van elke klant moeten afgescheiden worden om te voorkomen dat gegevens van één klant door de andere gekend worden.. Isolatiefouten kunnen optreden, bijvoorbeeld wanneer opslagruimte wordt vrijgemaakt door een afnemer en aan een andere afnemer wordt toegewezen zonder dat de inhoud wordt gewist.
Eruit voortvloeiende risico's	• Onrechtmatige bekendmaking van gegevens

R_03	**Controle van de beveiligingsmaatregelen**
Risicofactoren	De *cloud*provider moet zijn apparatuur beveiligen en de nodige beveiligingsstrategie en -processen toepassen om minstens tegemoet te komen aan het door zijn klant vereiste beveiligingsniveau. Deze is niet altijd in de mogelijkheid om te controleren of de *cloud*provider zijn verplichtingen nakomt.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

R_04	**Gedelocaliseerde infrastructuur**
Risicofactoren	De delocalisatie (*offshoring*) van de infrastructuur verhoogt het risico op aanvallen. Het toezicht op de beveiliging door de *cloud*provider en de controle door de afnemer van de *cloud*diensten kunnen in afgelegen landen moeilijk blijken te zijn.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

R_05	**Onderhoud van de virtuele machines**
Risicofactoren	De providers van de IaaS-service bieden hun klanten de mogelijkheid om naargelang hun behoeften virtuele machines te creeren. Telkens deze virtuele machines correcties moeten ondergaan (*patches*) in het kader van een IaaS-service is dit meestal ten laste van de afnemer van de *cloud*diensten. Virtuele machines die niet worden gebruikt, kunnen worden vergeten en werkend worden achtergelaten wat het risico vergroot van aanvallen.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

R_06	Authenticatie
Risicofactoren	De authenticatie moet onderling tussen de *cloud*provider en de afnemer van de *cloud*diensten gebeuren. Terwijl de nadruk vaak wordt gelegd op de authenticatie van de klant ten opzichte van de *cloud*provider kan de authenticatie in de andere richting verwaarloosd worden. Dit houdt een risico in van identiteitsfraude of van een *man-in-the-middle-attack* (onderscheppen van informatie tussen twee communicerende partijen zonder dat die daar weet van hebben).
Eruit voortvloeiende risico's	• Onrechtmatige bekendmaking van gegevens

4.2.2.1.2 PaaS

Specifieke risico's van het PaaS-model bovenop de risico's eigen aan het IaaS-model:

R_07	Gebruik van de SOA
Risicofactoren	De SOA-architectuur (*Service Oriented Architecture*), vaak aanwezig in het PaaS-aanbod, kan bepaalde kwetsbaarheden vertonen, hetzij in de aangeboden diensten zelf, hetzij via hun interacties. De SOA-bibliotheken worden beheerd door de *cloud*provider, en de klant heeft geen directe controle op het beheer van deze elementen, wat kan leiden tot gekende maar niet gecorrigeerde vulnerabilities.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

R_08	Einde van de overeenkomst
Risicofactoren	Aan het einde van de overeenkomst tussen de *cloud*provider en de klant, moeten de applicaties die in de PaaS-omgeving werden ontwikkeld, door de *cloud*provider uit de *cloud* worden gewist. Indien gegevens aan deze wisprocedure ontsnappen en binnen de *cloud* blijven bestaan, kunnen ze door een derde worden opgehaald en kwetsbaarheden van de applicatie onthullen.
Eruit voortvloeiende risico's	• Gegevensverlies • Onrechtmatige bekendmaking van gegevens

4.2.2.1.3 SaaS

Specifieke risico's van het SaaS-model bovenop de gecombineerde risico's van de IaaS- en PaaS-modellen:

R_09	Eigendom van de gegevens
Risicofactoren	De *cloud*provider levert de applicaties, de klant levert de gegevens. Indien het eigendom van de gegevens niet duidelijk wordt bepaald, kan de *cloud*provider aan het einde van de overeenkomst de toegang tot de gegevens weigeren en/of extra kosten aanrekenen voor de teruggave ervan.
Eruit voortvloeiende risico's	• Gegevensverlies • Financieel risico

R_10	Einde van de overeenkomst
Risicofactoren	Aan het einde van de overeenkomst tussen een *cloud*provider en zijn afnemer moeten de gegevens die in de SaaS-omgeving werden opgeslagen, door de provider van de *cloud* worden gewist. Indien gegevens aan deze wisprocedure ontsnappen en binnen de *cloud* blijven bestaan, kan een derde partij die in handen krijgen.
Eruit voortvloeiende risico's	• Onrechtmatige bekendmaking van gegevens

R_11	Ontwikkelcyclus van de applicaties
Risicofactoren	De ontwikkelcyclus van de applicaties (SDLC – *System Development Life Cycle*) staat onder controle van de *cloud*provider. De afnemer heeft hierop weinig controle, in het bijzonder op de beveiligingsvereisten die hierbij in aanmerking werden genomen. Dit gebrek aan controle kan leiden tot een beveiligingsniveau dat niet voldoet aan de behoeften van de gebruikers van de applicatie.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de applicaties op de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

R_12	Beheer van de identiteiten en van de toegang
Risicofactoren	De *cloud*providers bieden hun diensten en hun applicaties tegelijkertijd aan meerdere afnemers aan, wat een beheer van de identiteiten en van de toegang vereist (IAM – *Identity and Access Management*). Indien de *cloud*provider dit niet correct beheert, kunnen de applicaties en - via de applicaties - de gegevens die ze verwerken, door andere afnemers van dezelfde *cloud*diensten worden gelezen of gewijzigd.
Eruit voortvloeiende risico's	• Onrechtmatige bekendmaking van gegevens • Gegevensverlies

R_13	Verandering van provider
Risicofactoren	Normaliter wordt er neits voorzien om de portabiliteit van de *cloud*dienst en de betroffen gegevens van één *cloud*provider naar een andere te vergemakkelijken. Dit is vooral van belang wanneer een provider een gebrekkige dienst levert of failliet gaat, of wanneer hij (om een faillissement te vermijden) zijn contractvoorwaarden herziet. Op dezelfde wijze stoot de beslissing van een afnemer van *cloud*diensten om deze op te zeggen en zijn gegevens te rappatrieren op moeilijkheden.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de applicaties op de *cloud* • Blokkering te wijten aan de onbeschikbaarheid van de gegevens op de *cloud* • Gegevensverlies

R_14	Overeenstemming met het inkoopbeleid
Risicofactoren	Wanneer bedrijven voor een *cloud*dienst kiezen, kan het kunnen ze hierdoo hun inkoopbeleid voor zowel hardware als software over het hoofd zien. Dit kan leiden tot tegenstrijdigheden tussen de *cloud*applicaties en de intern beheerde toepassingen.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de gebrekkige werking van de applicaties op de *cloud*

R_15	Kwetsbaarheid van de webbrowsers
Risicofactoren	De door SaaS-providers aangeboden applicaties zijn meestal toegankelijk via een browser en een beveiligde verbinding. Deze browsers vormen dan ook een gebruikelijk doelwit van aanvallen. Indien de browser beschadigd is geraakt, is de applicatie dat ook en de beveiligde verbinding kan het probleem niet oplossen.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de applicaties op de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

4.2.2.2 Risico's ingedeeld volgens implementatiemodel

4.2.2.2.1 Publieke cloud

R_16	Deling met talrijke afnemers
Risicofactoren	Elke publieke *cloud* wordt tussen veel afnemers verdeeld die inzake beveiliging geen gemeenschappelijk belang noch dezelfde eisen delen. Hierdoor zijn er meer mogelijkheden van beveiligingsinbreuken.

Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de applicaties op de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

R_17	**Randschade**
Risicofactoren	Een aanval op één klant van een publieke *cloud* kan een impact hebben op alle andere afnemers van dezelfde *cloud*. Dit is vooral het geval in het geval van DDoS-aanvallen (*Distributed Denial of Service*) alsook bij de benutting van kwetsbaarheden van door de *cloud*provider beheerde software die soms niet onmiddellijk worden gecorrigeerd.
Eruit voortvloeiende risico's	• Blokkering te wijten aan de onbeschikbaarheid van de applicaties op de *cloud* • Gegevensverlies • Onrechtmatige bekendmaking van gegevens

4.2.2.2.2 Private cloud

R_18	**Nodige investeringen**
Risicofactoren	Een bedrijf kan een private *cloud* beschouwen als een middel om kosten te vermijden die verbonden zijn aan de aankoop, het onderhoud en de besturing van de eigen IT-installatie. Soms is het moeilijk om de bedrijfsbeheerder te doen inzien dat de implementatie van een private *cloud ook kosten met zich meebrengt*. Zo wordt soms op het budget beknibbeld wat tot onvoldoende capaciteit kan leiden.
Eruit voortvloeiende risico's	• Financieel risico; onvoorziene kosten. • Blokkering te wijten aan de onbeschikbaarheid van de applicaties op de *cloud*

4.2.2.2.3 Hybride cloud

De risico's verbonden aan de hybride *cloud*, zijn een combinatie van de risico's verbonden aan de private en publieke *clouds*. Daarnaast is het volgende risico eigen aan een hybride *cloud*:

R_19	**Onderlinge afhankelijkheid**
Risicofactoren	Bij het combineren van verschillende *cloud*types kan het voorkomen dat een bepaald *cloud*type tot een ander *cloud*type toegang moet kunnen hebben. Wanneer de beveiligingsniveaus onderling verschillen, kan dit leiden tot situaties waarbij systemen met een kritisch beveiligingsniveau toegang moeten verlenen aan systemen met een lager niveau van beveiliging. De nodige specifieke beveiligingsmaatregelen worden niet altijd genomen.
Eruit voortvloeiende risico's	• Gegevensverlies • Onrechtmatige bekendmaking van gegevens

4.2.2.3 Generieke risico's

Het volgende risico is noch afhankelijk van het servicemodel noch van het implementatiemodel.

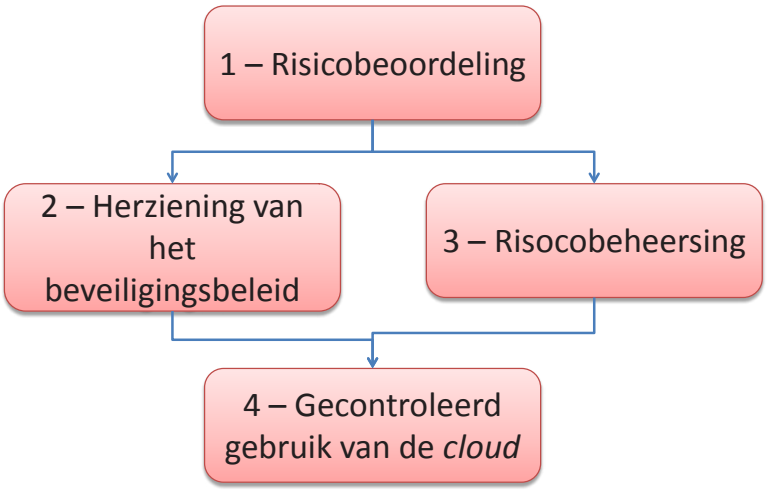
R_20	**Kost**
Risicofactoren	De *cloud*provider kan de op de *cloud* gehoste systemen van een afnemer blokkeren indien deze laatste zijn rekening niet tijdig betaalt.
Eruit voortvloeiende risico's	• Financieel risico • Blokkering te wijten aan de onbeschikbaarheid van de applicaties op de *cloud*

4.3 Risicobeheer

Zodra de risico's geïdentificeerd zijn (zie §4.2), moeten deze worden beheerd en dienen de gepaste beveiligingsmaatregelen te bepaald om deze tot een voor het bedrijf aanvaardbaar niveau te beperken en dit op een zo voordelig mogelijke wijze.
De hier voorgestelde aanpak bevat vier fasen:

1. Risicobeoordeling – De geïdentificeerde risico's, verbonden aan de implementatie van de *cloud*, moeten worden beoordeeld om te zien welke ervan moeten worden beperkt en prioritair worden gedekt;
2. Herziening van het beveiligingsbeleid – Om de implementatie van de *cloud* in het bedrijf voor te bereiden, moet het beveiligingsbeleid worden herzien (en in sommige gevallen worden uitgestippeld). Deze fase zorgt ervoor dat de beveiligingsregels effectief worden toegepast;
3. Risicobeheersing – In deze fase worden de nodige beveiligingsmaatregelen bepaald om de prioritaire risico's op gepaste wijze te dekken; bij de keuze van de *cloud*provider worden hem deze maatregelen opgelegd
4. Gecontroleerd gebruik van de *cloud* – Bij het gebruik van de *cloud*diensten houdt het bedrijf toezicht op de prestaties, vooral op niveau van de beveiliging.

De verschillende fasen zijn hierna weergegeven:



Afbeelding4 - risicobeheer

4.3.1 Risicobeoordeling

Er bestaan twee methodes om de risico's tot een aanvaardbaar niveau te beperken:

- Brongerichte aanpak - Er wordt getracht de waarschijnlijkheid te beperken van een dreiging voor het IT-systeem en de gegevens;
- Doelgerichte aanpak - Strengere beveiligingsmaatregelen worden genomen om de gegevens tegen de kwetsbaarheden van het IT-systeem te beschermen.

Zoals u ziet, bestaat het doel er niet in het risico uit te sluiten (een risico kan nooit volledig worden uitgesloten), het doel bestaat erin het risico te beperken tot een residueel niveau dat het bedrijf aanvaardbaar acht. Het is de bedrijfsdirectie die kan beslissen of een residueel risiconiveau al dan niet aanvaardbaar is, en niet de IT-dienst. Om echter met kennis van zaken beslissingen te kunnen nemen, rekent de directie op het advies van haar IT'ers.
Om te kunnen besluiten of een risico aanvaardbaar is, moet het worden beoordeeld. Zelfs al is het onmogelijk om een risico met volledige nauwkeurigheid te beoordelen -een risico is van nature onbekend- bestaan er gestructureerde methodes die een praktische risicobeoordeling en -vergelijkingen toelaten. Een voorbeeld van een zeer eenvoudig uit te voeren methode is het beoordelen van de risico's op basis van twee factoren: enerzijds de waarschijnlijkheid dat een dreiging optreedt, en anderzijds de kwetsbaarheid voor deze dreiging, de schade die ze kan veroorzaken.. De risico's worden hier op een tweedimensionale schaal voorgesteld zoals hierna weergegeven:

Risico / Kwetsbaarheid	Lage waarschijnlijkheid (bv. 1 keer per jaar)	Gemiddelde (bv. 1 keer per maand)	Hoge waarschijnlijkheid (bv. 1 keer per dag)
Grote kwetsbaarheid (een weinig uitgewerkte techniek kan de beveiliging bedreigen)			
Normale kwetsbaarheid (een bijzondere expertise is nodig om de beveiliging te bedreigen)			
Kleine kwetsbaarheid (extreme inspanningen zijn nodig om de beveiliging te bedreigen)			

Tabel 1 – Risicobeoordelingsschaal

Elk geïdentificeerd risico wordt op deze schaal voorgesteld in functie van een schatting van de waarschijnlijkheid dat het de dreiging optreedt (horizontale as) en van de kwetsbaarheid van de IT-systemen die de dreiging kan benutten (verticale as).

4.3.2 Herziening van het beveiligingsbeleid

Vóór elke implementatie van een nieuw IT-systeem moet het beveiligingsbeleid van het bedrijf worden herzien (en zelfs worden uitgestippeld indien niet bestaand). Dit principe geldt zowel voor de *cloud* als voor elk andere nieuwe IT-oplossing. De herziening kan betrekking hebben op:

- Classificatie van de gegevens – Met het oog op een aangepast beschermingsniveau van de gegevens moeten de gegevens worden ingedeeld om het bij hun verwerking gewenste beschermingsniveau aan te duiden. Sommige gegevens kunnen een speciaal beschermingsniveau vereisen wanneer hun verlies of bekendmaking een gevaar inhoudt voor het bedrijf;
- Overeenstemming met de wettelijke eisen – Het bedrijf is onderworpen aan de wetgeving over de bescherming van de persoonsgegevens. het beveiligingsbeleid van het bedrijf moet de verplichtingen op dit gebied respecteren. Sommige sectoren, zoals de gezondheidszorg of de financiële instellingen, zijn aan specifieke wettelijke eisen onderworpen die ook in hun beveiligingsbeleid moeten worden opgenomen;
- Continuïteit van de bedrijfsactiviteiten – Indien het bedrijf een preventief beleid toepast om in geval van een ramp zijn activiteiten te kunnen blijven uitoefenen, wordt een *Business Continuity Plan* opgesteld;
- Inkoopbeleid van hardware en software – In voorkomend geval moet het bedrijf ervoor zorgen dat er geen incompatibiliteit bestaat tussen de applicaties aangeboden op de *cloud* en de toepassingen die het bedrijf intern blijft beheren.

Deze diverse herzieningen vóór de implementatie van de *cloud* kunnen een aantal wijzigingen met zich meebrengen:

- Classificatie van de gegevens – het bedrijf kan beslissen om een klasse te creëren voor bijzonder gevoelige gegevens die het nooit op een *cloud* zal overdragen omdat het risico van verlies of bekendmaking hiervan als te groot wordt beoordeeld. Dit kan het geval zijn voor specificaties van industriële procedés of handelsstrategieën waarvan de bekendmaking aan derden het voortbestaan van het bedrijf in gevaar zou kunnen brengen;
- Overeenstemming met de wettelijke vereisten – het bedrijf kan beslissen om een klasse te creëren voor persoonsgegevens die nooit op een *cloud* zullen worden overgedragen indien het gevaar bij verlies of bekendmaking als te groot wordt beoordeeld. In een ziekenhuis bijvoorbeeld kunnen de medische gegevens van de patiënten het voorwerp zijn van een dergelijke classificatie;
- Continuïteit van de bedrijfsactiviteiten – Hoewel de implementatie van de *cloud* geen impact heeft op het Business Continuity Plan en, meestal, evenmin op het continuïteitsbeleid, is het raadzaam om dit beleid te herzien, rekening houdend met de nieuwe risico's verbonden aan het gebruik van de *cloud*. Indien het bedrijf geen continuïteitsbeleid heeft, is de implementatie van de *cloud* de gelegenheid om er een uit te stippelen;
- Inkoopbeleid – Het inkoopbeleid moet eventueel worden herzien indien na de implementatie van de *cloud* applicaties nog intern worden gebruikt.

4.3.3 Risicobeheersing

Zodra de risico's op een beoordelingsschaal worden weergegeven (zie voorbeeld onder punt 4.3.1), kan bepaald worden welke risico's moeten worden verminderd en met welke maatregelen.
In het voorbeeld van onze beoordelingsschaal: een risico dat na beoordeling in een groene cel wordt weergegeven, is een klein risico en hoeft niet te worden verminderd; een risico in een gele cel is aanzienlijk en moet indien mogelijk worden verminderd; een risico in een rode cel in onaanvaardbaar en moet absoluut worden verminderd:

- Ofwel wordt de waarschijnlijkheid verminderd door het nemen van preventieve maatregelen. hier wordt bijvoorbeeld een onderscheid gemaakt tussen zeer gevoelige gegevens (die nooit op een *cloud* worden opgeslagen), en de andere gegevens (die wel op een *cloud* kunnen worden opgeslagen) en dit om de waarschijnlijkheid te beperken dat gevoelige gegevens buiten het bedrijf worden bekendgemaakt;
- Ofwel wordt de kwetsbaarheid verminderd door het nemen van meestal technische maatregelen. Zo kan men bijvoorbeeld van de *cloud*provider eisen dat alle gegevens — zowel op de netwerken als op de opslageenheden met een zware versleuteling worden beveiligd.

Wanneer de "rode" risico's verwijderd zijn en de "gele" risico's wanneer mogelijk verminderd, heeft men een geheel van beveiligingsmaatregelen dat de geïdentificeerde risico's op aangepaste wijze dekt en het door het bedrijf nagestreefde beveiligingsniveau bereikt .
De onderstaande lijst geeft een aantal voorbeelden van te overwegen beveiligingsmaatregelen (en te kiezen na de fase van de risicobeheersing):

- Contractuele maatregelen – Om bepaalde risico's te verminderen, kan het bedrijf de *cloud*provider contractuele bepalingen voorschrijven:
    - Eisen dat de overeenkomst met de *cloud*provider garandeert dat de klant de enige eigenaar blijft van de gegevens en de applicaties die naar de *cloud* werden gemigreerd;
    - In de SLA met de *cloud*provider de verplichting toevoegen van een beheerproces van de kwetsbaarheden van de hypervisors[13];
    - In de SLA met de *cloud*provider de verplichting toevoegen van een beheerproces van de veranderingen, dat op zijn minst uit een risicoanalyse bestaat;
    - Erop toezien dat contractuele bepalingen opgenomen zijn die de klant toelaten van *cloud*provider te veranderen, en dit zonder

[13] Een **hypervisor** (of virtual machine monitor- VMM) is een softwarecomponent of apparaat waarmee een hostserver een of meer virtuele machines beheert (elk van deze machines wordt bijvoorbeeld door een klant van de cloud gebruikt).

verlies van gegevens of toepassingen, en dit binnen een redelijke termijn;
    - Indien nodig geografische beperkingen toevoegen voor de locatie van de gegevens op de *cloud*;
- Door de provider genomen beveiligingsmaatregelen – Het bedrijf kan van de *cloud*provider bepaalde informatie eisen:
    - Beschrijving van de regels die bepalen over wie, van het personeel van de *cloud*provider (of van zijn verwerkers), toegangsrecht heeft tot de gegevens van de klant;
    - Beschrijving van de door de *cloud*provider uitgevoerde netwerkbeveiligingen (firewall, antivirus, bescherming tegen Distributed Denial of Service-aanvallen, enz.); beschrijving van het beheerproces van deze beveiligingen;
    - Beschrijving van het beheerproces van de toegangsrechten binnen de organisatie van de *cloud*provider;
    - Beschrijving van de toegepaste versleutelingsmaatregelen: algoritmen, lengte van de sleutels, beheer van de sleutels;
    - Beschrijving van de technische maatregelen voor het wissen van vrijgegeven gegevens en de vernietiging van de opslagmedia;
    - Beschrijving van het door de *cloud*provider toegepaste Business Continuity Plan; het bewijs dat regelmatig simulaties worden uitgevoerd;
    - Het bewijs dat de *cloud*provider regelmatig audits laat uitvoeren door erkende auditors;
- Keuze van een bijzondere beheermodus van de *cloud* – Het bedrijf kan zich beperken tot een private *cloud* indien het "*multi-tenant*" karakter van publieke *clouds* risico's inhoudt die als onaanvaardbaar worden beoordeeld;
- Door de klant van de *cloud*diensten genomen maatregelen:
    - Organisatie van een sensibiliseringscampagne rond beveiliging van het gebruik van de *cloud;*
    - Toegang tot de *cloud* beperken tot beveiligde webbrowsers (gebruik van *sandboxes*) of beveiligde virtuele terminals;
    - Herziening van het continuity planning -*Business Continuity Plan*, *Disaster Recovery Plan*- om een langdurige onbeschikbaarheid van de *cloud* te vermijden.

4.3.4 Gecontroleerd gebruik van de *cloud*

Beveiliging is een continu proces, d.w.z. dat beveiliging zich niet beperkt tot de implementatie van een dienst zoals de *cloud* maar ook gedurende de werking ervan moet worden uitgeoefend.De afnemer van de *cloud*diensten moet regelmatig controleren of zijn *cloud*provider zijn contractuele verplichtingen nakomt en, indien nodig, het bewijs hiervan krijgen; hetzelfde geldt voor de door de provider genomen beveiligingsmaatregelen.
Anderzijds moet de klant verifiëren dat het IT-auditprogramma waaraan het is onderworpen het gebruik van de *cloud* in aanmerking neemt en dat zijn interne auditors opgeleid zijn tot dergelijke controles.

5 De *cloud*markt

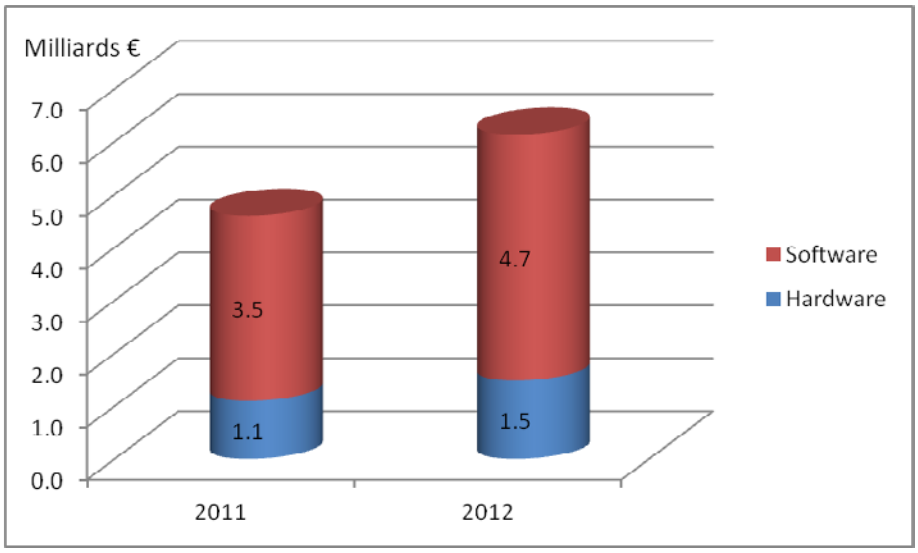
5.1 Stand van zaken in Europa en in België

5.1.1 Stand van zaken van de *cloud*markt in Europa

Uit een studie uitgevoerd in juni 2012 door IDC[14] in opdracht van de Europese Commissie (DG Informatiemaatschappij), blijkt dat de Europese publieke *cloud*markt in 2011 en 2012 een omzet optekende van respectievelijk 4,6 miljard euro en 6,2 miljard euro, wat overeenstemt met respectievelijk 1,6 % en 2,2 % van de totale IT-uitgaven exclusief diensten.

De hardwarediensten vertegenwoordigden een omzet van 1,1 miljard euro in 2011 en 1,5 miljard euro in 2012, ten opzichte van respectievelijk 3,5 miljard euro en 4,7 miljard euro voor de softwarediensten.

Deze cijfers sluiten aan bij de schattingen van de Franse markt uitgevoerd begin 2012 door Markess en die wezen op een totale omzet van 2,8 miljard euro. In dit cijfer zijn eveneens de private en gemeenschappelijke *clouds* inbegrepen.



*Afbeelding 5 - Stand van zaken van de cloud*markt *in Europa*

Voor de *cloud* in België zijn geen cijfers beschikbaar. Wij zijn vertrokken van de hypothese dat het aandeel van België 2,7 % bedraagt (verhouding Belgisch bbp ten opzichte van het Europees bbp).

[14] Quantitative Estimates of the Demand for cloud Computing in Europe and the Likely Barriers to Up-take - IDC - juni 2012

De onderstaande tabel vertegenwoordigt de IT-uitgaven in Europa in 2009[15]. Op die basis zou het Belgische aandeel 2,6 % van de Europese IT-markt vertegenwoordigen.

	IT Expenditure (bn$) - 2009
Germany	181
UK	153
France	136
Italy	104
Spain	73
Netherlands	49
Poland	26
Sweden	25
Belgium	24
Austria	21
Denmark	16
Finland	15
Greece	15
Czech Republic	15
Portugal	13
Ireland	12
Hungary	11
Romania	9
Slovakia	6
Bulgaria	3
Slovenia	2
Others	15
Total	**924**
Belgium %	**2.6%**

Afbeelding 6 - IT-uitgaven in Europa

Uitgaande van een conservatieve hypothese van 2,5 %, zou de omzet van de Belgische *cloud*activiteiten in 2012 ongeveer 153 miljoen euro bedragen. Dit cijfer werd tijdens de vergadering van 27 februari 2013 met de betrokken actoren besproken en hieruit is gebleken dat de sector geen geconsolideerde visie van de voortgebrachte omzet lijkt te hebben.

[15] World Information Technology and Services Alliance – Digital Planet 2009

5.1.2 Remmingen voor de ontwikkeling van de *cloud*

Potentiële afnemers van *cloud*diensten worden met een aantal remmingen geconfronteerd die de ontwikkeling ervan vertraagt. De hierna vermelde conclusies vloeien voort uit de voornoemde studie van de IDC alsook uit de studie uitgevoerd door de Expert Group van de DG Information Society and Media[16]. Over het geheel genomen, zijn de hierna vermelde remmingen algemeen erkend en zijn het voorwerp van heel wat publicaties op internet:

- Onzekerheid of, althans, een gebrek aan eenduidigheid wat de naleving betreft van de wetgeving over de bescherming en het vertrouwelijke karakter van persoonsgegevens (dat geldt in bijzonder voor de Amerikaanse Patriot Act die aan de CIA of FBI toegang zou geven tot de gegevens die door in de VS gevestigde bedrijven op de *cloud* worden beheerd of opgeslagen, en dit zonder dat die bedrijven de eigenaar van de gegevens hiervan kunnen verwittigen, wat in strijd is met de Europese of lokale wetten);
- Onzekerheid of, althans een gebrek aan eenduidigheid, over de wetgeving die van toepassing is op gegevens die per definitie waar dan ook ter wereld kunnen worden opgeslagen;
- Sommige lokale wetten bevorderen het gebruik van de *cloud* niet, zoals fiscale stimuli ter bevordering van kapitaalinvesteringen in verhouding tot operationele uitgaven;
- Twijfel over het feit of verwijderde gegevens wel effectief definitief van het systeem zijn gewist;
- De afwezigheid van beginselen, op zijn minst geharmoniseerd op Europees niveau, over de aansprakelijkheid van de *cloud*provider voor het verlies, de vernietiging of de diefstal van gegevens (en de vergoeding van de eruit voortvloeiende schade);
- Het gebrek aan beschikbare informatie bij de providers over de haalbaarheid en de kost om gegevens van de ene provider op de andere over te dragen;
- Het risico dat de aan de provider toevertrouwde gegevens afhankelijk worden van een leveranciersgebonden architectuur of standaarden, wat het veel moeilijker maakt om de gegevens naar een andere provider te migreren (*vendor lock-in*);
- Het gebrek aan vertrouwen over het vermogen van de provider de dienst 7/24 en met het vereiste prestatieniveau te leveren, en de vrees van de impact hiervan op de zaken in geval van onbeschikbaarheid van de dienst;
- De afwezigheid, de onnauwkeurigheid of het niet-dwingende karakter van de voorgestelde SLA's;
- In sommige regio's het gebrek aan bandbreedte van de telecominfrastructuur;
- In sommige regio's de te hoge kost van een internetverbinding;
- De afwezigheid van de garantie dat de kosten voor het gebruik van de *cloud*diensten aanzienlijk lager is dan de kost voor het gebruik van het interne IT-systeem;
- De afwezigheid van de garantie dat de bedongen voorwaarden en prijzen voor het gebruik van de *cloud*diensten duurzaam zijn: betreft het geen

[16] The Future of cloud Computing – Europese Commissie / DG Informatiemaatschappij en Media - 2010

"lanceringsprijzen"? Kan men zich verwachten, zoals dat thans het geval is voor de banken, aan eenzijdige wijzigingen van de voorwaarden?
- Het gebrek aan aangepaste software (in het bijzonder aangeboden in verschillende talen);
- Het gebrek aan een lokale helpdesk;
- De afwezigheid van enige controle op versiewijzigingen van de ter beschikking gestelde software en dus het risico van ongewenste migratiekosten;
- En zo voort..

5.2 *Evolutie van de Belgische en Europese cloud*markt

5.2.1 Mogelijke scenario's

De evolutie van de *cloud*markt zal afhankelijk zijn van de opheffing of vermindering van de eerder in dit document beschreven technische, functionele, economische en juridische hinderpalen. Bovendien blijkt uit de studies dat de juridische overheersend zijn: de zekerheid dat de verwijderde gegevens effectief van de systemen zijn gewist, de bescherming van het vertrouwelijke karakter van de gegevens alsook de op de gegevens toepasselijke wetgeving.

Hierna volgen de mogelijke scenario's:

- Het pessimistische scenario
  Een vertraging van de implementatie van de *cloud* na 2014, te wijten het uitblijven van een efficiënt rechtskader van de *cloud*markt, en aan diverse incidenten over de beveiliging, het vertrouwelijk karakter en de beschikbaarheid van de gegevens;
- Het lineaire scenario
  Een lineair verloop van de implementatie van de *cloud* in afwezigheid van interventie door de overheden, zonder ernstige incidenten en met een aanzienlijke verbetering van de bandbreedte van de telecominfrastructuren;
- Het optimistische / interventiescenario
  Een versnelling van de implementatie van de *cloud* in 2014/2015 nadat de overheden de nodige maatregelen hebben genomen.

Voor de drie scenario's wordt echter aangenomen dat:

- Europa geleidelijk aan en zonder kleerscheuren uit de crisis geraakt;
- Alle macro-economische indicatoren langzaam stijgen;
- De wereldwijde politieke situatie geen ingrijpende gebeurtenissen doormaakt die een impact hebben op de Europese beleidsstructuur of economie.

5.2.2 Het pessimistische scenario

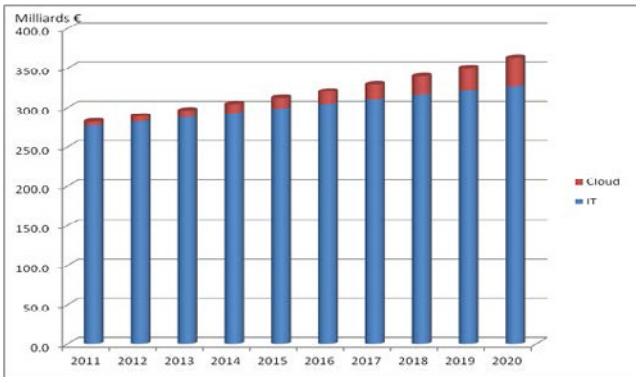
Dit scenario vloeit voort uit het feit dat de veronderstelde incidenten de overheden ertoe doen besluiten om definitief van de implementatie van de *cloud* af te zien en de bedrijven de *cloud* slechts implementeren voor beperkte applicaties die weinig gevoelige gegevens verwerken. In dergelijk geval zal het gratis gebruik van de *cloud*

(Gmail, Google apps, enz.) de ontwikkeling remmen van betalende oplossingen met toegevoegde waarde.

De huidige groei zou in 2014 terugvallen van 33 % tot 22 %.

Tegen 2020 zou dit scenario leiden tot een begroting van de uitgaven voor de *cloud* van 35,2 miljard euro, of 10,7 % van de totale IT-uitgaven, ten opzichte van 2,2 % in 2012 waarbij een linearie evolutie van de totale IT-uitgaven wordt aangenomen, met een gemiddelde jaarlijkse groei van 1,9 %.

Voor België zou dit in 2020 880 miljoen euro vertegenwoordigen.



*Afbeelding 7 - Evolutie van de cloud*markt *in Europa - Pessimistisch scenario*

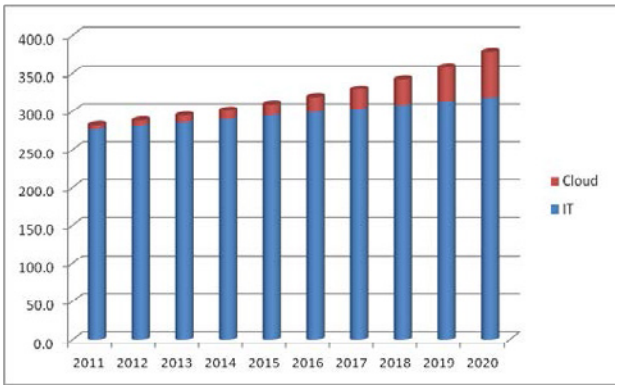
5.2.3 Het lineaire scenario

Dit scenario vloeit voort uit de afwezigheid van ernstige incidenten. De overheidsbesturen blijven wantrouwig door de afwezigheid van een reglementair en rechtskader en ontwikkelen gemeenschappelijke of "soevereine" oplossingen (wat in Frankrijk en Groot-Brittannië al het geval is). De implementatie van de *cloud* door de bedrijven zal zich tot meer applicaties uitbreiden voor zover die geen persoonsgegevens verwerken.

De huidige groei van 33 % zou gehandhaafd blijven.

Tegen 2020 zou dit scenario leiden tot een begroting van de uitgaven voor de publieke *cloud* van 59,9 miljard, of 18,7 % van de totale IT-uitgaven, ten opzichte van 2,2 % in 2012, waarbij de gematigde vervanging van interne informatica door *cloud*diensten de gemiddelde jaarlijkse groei van de totale IT-uitgaven tot 1,5% zou worden beperkt.

Voor België zou dit in 2020 1,5 miljard euro vertegenwoordigen.



*Afbeelding 8 - Evolutie van de cloud*markt *in Europa - Lineair scenario*

5.2.4 Het optimistische / interventiescenario

Hier gaat het strikt genomen om een daadkrachtig scenario waarbij de Europese en lokale overheden krachtige juridische en reglementaire maatregelen nemen om de impact van de overeenstemmende remmingen uit de weg te ruimen.

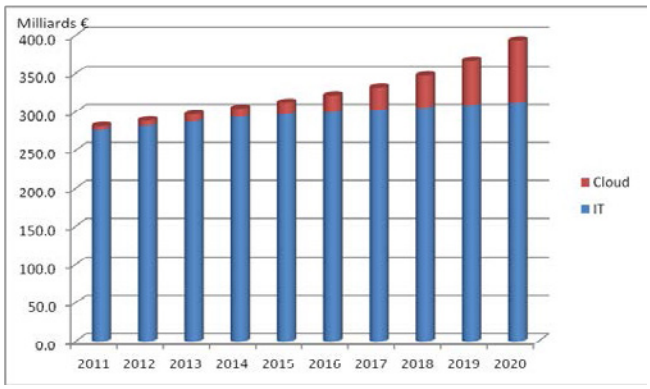
Deze maatregelen zouden hoofdzakelijk bestaan uit:

- De opstelling van eenduidige regels over de aansprakelijkheid van de *cloud*providers op het gebied van beveiliging en bescherming van het persoonlijk karakter van de gegevens, ongeacht hun locatie;
- De opstelling van eenduidige regels over de op de gegevens toepasselijke wetgeving, ongeacht hun locatie;
- De harmonisatie van de regels over de bescherming van persoonsgegevens;
- De invoering van een reglement dat de overdraagbaarheid van gegevens tussen de providers moet garanderen, alsook de garantie dat de door de gebruiker verwijderde gegevens volledig en definitief zijn gewist;
- De verduidelijking van de rechten van de gebruikers van *cloud*diensten, onder meer de klachtenbehandeling en de toegang tot de gegevens (inzage, wijziging, verwijdering).

De toepassing van deze maatregelen door de providers zou idealiter door een bevoegde overheidsinstantie regelmatig gecontroleerd moeten worden en aanleiding geven tot lokale of Europese certificeringen; bijvoorbeeld:

- Een beveiligingscertificering waaruit blijkt dat alle maatregelen ter beveiliging en bescherming van het vertrouwelijk karakter van de gegevens alsook ter bescherming van de persoonsgegevens, werden genomen en regelmatig door interne audits worden gecontroleerd.
- Een certificering Overheidsdiensten waaruit blijkt dat de *cloud*diensten voldoen aan de reglementaire voorschriften van de overheidsbesturen, met eventueel beperkingen betreffende de locatie van de gegevens (beperkt tot nationaal of EU-niveau).

Dit scenario veronderstelt eveneens een aanzienlijke verbetering van de bandbreedte van de telecominfrastructuren en een aanzienlijke daling van de prijzen van de internetproviders.
In dergelijke omstandigheden zou de omzetgroei van de *cloud*diensten in 2014/2015, na invoering van voornoemde maatregelen, van 33 % tot 40 % moeten stijgen. Daarentegen zouden de traditionele IT-uitgaven na 2014, van 1,9 % tot 1 % moeten dalen, rekening houdend met de massale overschakeling van sommige interne diensten naar de *cloud*diensten. In 2020 zou het aandeel van de *cloud*diensten 26 % van de totale IT-uitgaven vertegenwoordigen, of 2 miljard euro voor België.



*Afbeelding 9 - Evolutie van de cloud*markt *in Europa - Optimistisch scenario*

5.2.5 De kans van een directe overheidsinterventie?

Is een soevereine *cloud* zoals die thans in een lidstaat wordt geïmplementeerd, noodzakelijk, wenselijk en/of haalbaar?

Het komt erop aan om, door middel van de oproep tot de indiening van royaal gesubsidieerde projecten de oprichting te bevorderen van consortiums met het oog op de oprichting van bedrijven in de vorm van publiek-private partnerschappen (waarbij de staat aandeelhouder is en controlebevoegdheid uitoefent).

Het doel bestaat erin het volledige ecosysteem lokaal te behouden (in casu in de betrokken lidstaat): de aandeelhouders, de besluitvorming, de infrastructuur, het applicatieplatform en vooral de gegevens. Het kan ook nuttig zijn de contractvoorwaarden te controleren, onder meer de prijzen[17].

Zonder de belofte van subsidies zouden de voornoemde consortiums of bedrijven er vermoedelijk niet komen. Dit zou weleens, behalve het noodzakelijkerwijs politiek karakter van de verrichting en de juridische problemen van concurrentieverstoring waartoe dit in een opkomende of bestaande markt kan leiden, aanleiding kunnen geven tot de kunstmatige oprichting van opportunistische maar op termijn kwetsbare bedrijven die ten opzichte van de zwaargewichten van de markt – Amazon, Google,

[17] De aanwezigheid van de staat kan dienen om de prijzen te controleren (wat echter niet gemakkelijk is in de sectoren waar de staat aanwezig is, zoals de elektriciteits- en gassectoren). Dat is trouwens het argument dat IBM (Frankrijk) heeft aangevoerd om zich te verzetten tegen de aanwezigheid van de staat bij de levering van de *cloud*diensten (http://archives.lesechos.fr/archives/2012/lesechos.fr/01/31/0201873061845.htm.)

Microsoft, IBM, enz. – slechts een marginale rol kunnen spelen en door deze zwaargewichten voor een spotprijs zouden kunnen worden overgenomen zodra hun subsidies zijn opgebruikt en de staat hen niet langer kan financieren.

Is het wel nodig om op die manier nieuwe bedrijven op te richten, terwijl de grote multinationale *cloud*deskundigen samenwerkingsakkoorden sluiten met lokale partners om deze "nationale" aanbiedingen van *cloud*computing overeenkomstig de lokale reglementering te ontwikkelen? In Frankrijk bijvoorbeeld heeft SFR een partnerschap gesloten met HP voor de ontwikkeling van *cloud*diensten gericht naar de kmo's. Samen met EMC en VMWare, heeft ATOS Canopy opgericht, een provider van *cloud*oplossingen *en -diensten*. Dezelfde aanbieder van IT-diensten heeft eveneens een samenwerkingsakkoord met Microsoft gesloten voor de implementatie van de *cloud*oplossingen van het softwarehuis. Na de beëindiging van deze akkoorden, kan de soevereiniteit alsook de locatie van de gegevens eveneens worden gegarandeerd: in casu worden de gegevens opgeslagen in de datacenters van de nationale actoren gevestigd op het grondgebied van de betrokken lidstaat.

6 Het rechtskader van *cloud*computing

Op het moment van de redactie van dit deel van het verslag (maart 2013), bestaan geen specifieke reglementaire bepalingen over *Cloud*computing. Het fenomeen van *cloud*computing, evenals dat van de sociale netwerken, zoekmotoren, en van *cloud*diensten voor het "grote publiek" (e-maildiensten zoals Gmail, Hotmail, gegevensoverdrachtdienst zoals Dropbox), is vrij recent en hoewel er een recente rechtspraak over bestaat, steunt deze meer op de inbreuk van regels over het auteursrecht (overname van persartikelen in zoekmotoren en news; poging tot de sluiting van websites voor de deling van bestanden waarop auteursrecht rust) dan op de specifieke aansprakelijkheid van de *cloud*actoren.

Een nieuw Europees rechtskader is in volle ontwikkeling en zal, indien gedurende de periode 2013-2015 goedgekeurd, in de erop volgende jaren volop effect sorteren.

6.1 Stand van zaken in België

Thans bevat het Belgische recht geen specifieke reglementering over *Cloud*computing. Er moet dus worden verwezen naar het verbintenissenrecht, naar de specifieke regels over gegevensbescherming en naar het stelsel van de aansprakelijkheid van serviceproviders van gegevensopslag.

6.1.1 Bescherming van persoonsgegevens

Het domein van de bescherming van persoonsgegevens bevat de meeste specifieke kenmerken en zal binnenkort het voorwerp zijn van een Europese hervorming.

De bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens is sinds 1981 opgenomen in een conventie van de Raad van Europa[18].

Daarnaast bepaalt de Belgische wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, de rechten en verplichtingen van de verantwoordelijke voor de gegevensverwerking alsook die van de personen waarop de gegevens betrekking hebben:

- Transparantieplicht ten laste van de verantwoordelijke voor de verwerking van persoonsgegevens;
- Regels voor het gebruik van persoonsgegevens;
- Nieuwe rechten (inzage, wijziging, verzet) voor de betrokken personen.

[18] Het Verdrag 108 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens.

Vervolgens heeft het Europees recht de fakkel overgenomen met een aantal richtlijnen die in de nationale wetgevingen werden omgezet.

- Richtlijn 95/46/EG die het algemeen stelsel bepaalt van de bescherming van persoonsgegevens en hierdoor de belangrijkste Europese norm ter zake is in de gehele Europese Unie.
- Richtlijn 97/66/EG die meer bepaald betrekking heeft op de telecommunicatiesector. Deze richtlijn werd sindsdien opgeheven/vervangen door de richtlijn 2002/58/EG, de zogenaamde "richtlijn betreffende privacy en elektronische communicatie" die de beginselen van de richtlijn 95/46/EG op het gebied van elektronische communicatie ten uitvoer legt;
- Richtlijn 2006/24/EG die de voorwaarden bepaald voor gegevensverwerking in de lidstaten.

In België zijn door de omzettingen die de wet van 1992 hebben aangepast, de volgende normen van toepassing:

Wet van **8 december 1992** - Bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (WPL)
Omzetting van richtlijn 95/46/EG: - Wet van 11 december 1998 - Koninklijk besluit van 13 februari 2001 - Wet van 26 februari 2003
Omzetting van richtlijn 2002/58/EG: - Wet van 13 juni 2005 betreffende de elektronische communicatie
Specifiek geval: - Bescherming van de persoonlijke levenssfeer van de werknemers (KB van 12 juni 2012 waarbij algemeen verbindend wordt verklaard de collectieve arbeidsovereenkomst nr. 81 van 26 april 2002)

Tabel 2 – Belgische normen (gegevensbescherming)

Richtlijn 95/46/CE was op nationaal niveau niet direct van toepassing. Ze moest dus door elke lidstaat in nationaal recht worden omgezet wat ruimte gaf voor uiteenlopende interpretaties. Zo is eenzelfde situatie in België, Frankrijk, Groot-Brittannië of Duitsland niet aan dezelfde regels onderworpen, wat voor multinationale bedrijven problemen schept.

Bovendien was er in 1995 nog geen sprake van "*cloud*computing". Mede hierdoor werd niet voorzien in een globalisering van de markt, noch in de eruit voortvloeiende mobiliteit van de gegevens.
Vandaar de noodzaak om het bestaande wettelijk kader aan te passen, te harmoniseren en te versterken. Daarom heeft de Europese Commissie op 25 januari 2012 een voorstel voor een verordening gepubliceerd die, zodra aangenomen, de richtlijn 95/46/EG moet vervangen. Dze biedt het voordeel direct van toepassing te zijn in de 27 (weldra 28) lidstaten (en in sommige EVA-staten: Noorwegen, IJsland en Liechtenstein die deel

uitmaken van de EER). Er zullen dus geen verschillen meer bestaan tussen de wetgevingen van de staten waar dit stelsel van toepassing is.

Deze nieuwe elementen zijn in sectie 6.2 in detail toegelicht

Op basis van het huidige recht, welke beginselen zijn van toepassing op *Cloud*computing (voor persoonsgegevens)?

De klant van *cloud*computing die gegevens aan een externe provider (verwerker) toevertrouwt is en blijft de controleur van zijn gegevens, d.w.z. in Belgisch recht de "Verantwoordelijke voor de verwerking" (WPL art. 1 §4).

De *cloud*provider wordt beschouwd als een loutere "verwerker" van de hem toevertrouwde gegevens; het is de klant die verantwoordelijk is voor de gegevensbescherming.

Dit ontheft de verwerker van de gegevens echter niet van zijn aansprakelijkheid:

- De WPL definieert de verwerker als de persoon (natuurlijke of rechtspersoon), de feitelijke vereniging of het openbaar bestuur die persoonsgegevens verwerkt ten behoeve van de verantwoordelijke voor de verwerking (WPL art. 1 §5);
- In het kader van de gegevensbescherming is deze *cloud*provider geen derde en is hij dan ook direct onderworpen aan de bepalingen van de wet (WPL art. 1 §6);
- De verantwoordelijke voor de verwerking (klant van de *cloud*) zal een verwerker moeten kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking (WPL art. 16 §1)[19]. De contractuele relatie tussen de klant en de *cloud*provider moet het voorwerp zijn van een schriftelijke overeenkomst die de aansprakelijkheid moet vermelden van de verwerker en waarin wordt overeengekomen dat de *cloud*provider gebonden is door dezelfde verplichtingen (als zijn klant - verantwoordelijke voor de verwerking) wat betreft de toegang tot en de bescherming van de gegevens (WPL art. 16 §1, 2° tot 5°).
  In het geval van *cloud*computing, waar veel overeenkomsten door de provider vooraf opgestelde lidmaatschapscontracten zijn, is de verantwoordelijkheid voor de opstelling van een dergelijke overeenkomst weliswaar tussen de partijen verdeeld, maar kan men aannemen dat de *cloud*provider -waarvan het de kernactiviteit betreft-, grotendeels verantwoordelijk is voor de opstelling van het contract.
- In elk geval, ongeacht enige overeenkomst:
  - Mag de *cloud*provider geen enkele verwerking uitvoeren zonder hiervoor opdracht te hebben gekregen van de klant (verantwoordelijke voor de verwerking), behoudens op grond van een verplichting door of krachtens een wet, een decreet of een ordonnantie (WPL art. 16 §3);
  - Is de *cloud*provider als verwerker verplicht de gepaste technische en organisatorische maatregelen te treffen voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen

[19] Gewijzigd door de wet van 11/12/1998 – inwerkingtreding 01/09/2001

toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens (WPL art. 16 §4).

Uit deze bepalingen blijkt dus dat de aansprakelijkheid van de *cloud*provider aanzienlijk is indien:

- Hij verzuimd zou hebben zijn klant te vragen of persoonsgegevens het voorwerp waren van de verwerking;
- Hij de onderhandeling van een schriftelijke overeenkomst verzuimd of bemoeilijkt zou hebben waarin zijn aansprakelijkheid en het detail van de genomen technische maatregelen ter bescherming van de gegevens zijn opgenomen;
- Hij zonder de toestemming van de klant verrichtingen die volgens de WPL als een verwerking worden beschouwd (WPL art. 1 §2) zou hebben uitgevoerd (de overdracht van gegevens naar een derde land is een vorm van verwerking: vanuit technisch oogpunt is dit een "verstrekking door middel van doorzending", een "registratie" en een "bewaring");
- Hij verzuimd zou hebben (ongeacht deze maatregelen al dan niet in de overeenkomst zijn gedetailleerd) de gepaste technische en organisatorische maatregelen te treffen om de gegevens te beschermen tegen vernietiging, verlies, wijziging, toegang of iedere andere niet toegelaten verwerking.

6.1.2 Het stelsel van de gegevensdoorgifte

De gegevens - al dan niet persoonsgegevens - moeten binnen de Europese Unie (en de eraan verbonden Europese Economische Ruimte) vrij kunnen worden overgedragen.
Wat een probleem kan stellen, en wat wij hier "gegevensdoorgifte" noemen (of grensoverschrijdende doorgifte van gegevens) is een overdracht van persoonsgegevens vanuit een lidstaat van de Europese Unie aan een derde land, d.w.z. een land dat geen lid is van de Europese Unie en ook geen lid is van de Europese Economische Ruimte [20].

Doorgifte van gegevens aan een derde land is toegestaan indien dit land een passend beschermingsniveau biedt. Daarentegen mag de doorgifte aan een derde land dat niet over een dergelijk passend beschermingsniveau beschikt, niet worden uitgevoerd, uitgezonderd restrictief opgesomde derogaties.

Welke derde landen bieden een passend beschermingsniveau?

De Europese Commissie publiceert de lijst op haar website[21]. Hiertoe steunt de Commissie op de algemene en sectorale wetgeving alsook op de beroepsregels van het betrokken land. Het betreft Zwitserland, Canada (voor verwerkingen onderworpen aan de Canadese "Personal Information Protection and Electronic Documentation Act"), Argentinië, de Verenigde Staten (indien de ontvanger van de gegevens in de Verenigde

[20] Commissie voor de bescherming van de persoonlijke levenssfeer - veelgestelde vragen - http://www.privacycommission.be/nl/faq-page/373#t373n3746
[21] http://ec.europa.eu/justice/data-protection/index_nl.htm

Staten de "Safe Harbor" beginselen heeft onderschreven), Guernsey, het Eiland Man, de Faeröereilanden, Jersey en Israël.

De *Cloud*provider die infrastructuur in deze landen gebruiktkan er dus - hoofdzakelijk indien zijn vestigingen tussen Europa en de Verenigde Staten of Canada zijn verdeeld - de gegevens van zijn klanten doorgeven.

Meer in het bijzonder wat de Verenigde Staten betreft, moet de *cloud*provider (indien hij gegevens doorgeeft aan een dochterbedrijf van dezelfde groep of aan een verwerker) erop toezien dat zijn groep of zijn verwerker effectief de "Safe Harbor" beginselen onderschrijft.

> "Safe Harbor" ("veilige haven") is de naam van een akkoord gesloten in november 2000 tussen de EU en de VS over de regeling van de doorgifte van persoonsgegevens van Europese burgers overeenkomstig de Europese richtlijnen. Zo kan een Amerikaans bedrijf certificeren dat het de wetgeving van de Europese Economische Ruimte naleeft en de toestemming krijgen om persoonsgegevens uit de EER aan de Verenigde Staten door te geven. Het akkoord schrijft de volgende verplichtingen voor:
>
> - Kennisgeving - Individuen in de EER moeten in kennis worden gesteld dat hun gegevens worden verzameld en van de wijze waarop ze zullen worden verwerkt.
> - Keuze - Individuen moeten de mogelijkheid hebben te weigeren dat hun persoonsgegevens aan derden worden doorgegeven of worden gebruikt voor andere doeleinden dan die waarmee het individu oorspronkelijk had ingestemd.
> - Doorgifte aan derden - De doorgifte van gegevens aan derden is alleen maar toegestaan indien de derde hetzelfde nalevingsniveau van de beginselen van bescherming van persoonsgegevens garandeert.
> - Beveiliging - Het bedrijf zal de nodige maatregelen nemen om de verzamelde gegevens te beschermen tegen verwijdering, onrechtmatig gebruik, bekendmaking of wijziging ervan.
> - Integriteit van de gegevens - Het bedrijf verbindt zich ertoe de verzamelde gegevens uitsluitend te gebruiken voor de doeleinden voor welke de gebruiker zijn akkoord heeft gegeven.
> - Toegang - Individuen moeten toegang hebben tot hun persoonsgegevens en die desgewenst kunnen corrigeren of verwijderen.
> - Toepassing - Het bedrijf zal al het nodige doen om ervoor te zorgen dat deze regels effectief worden toegepast en zal toezien op hun naleving.
>
> Een Amerikaans bedrijf kan op een derde een beroep doen om de naleving van zijn "certificering" te controleren, maar kan ook verklaren de beginselen van het akkoord te onderschrijven, en zelf toezien op zijn opleiding (en deze van zijn personeel) en op de naleving van de Safe Harbor-verplichtingen. Dit moet jaarlijks gebeuren.

De doorgiften van gegevens die in het kader van de "Safe Harbor" beginselen zijn toegestaan, kunnen worden uitgevoerd zoals een gegevensoverdracht tussen twee *cloud*centers in België of in een andere lidstaat van de Europese Unie. Hierbij moeten echter altijd de algemene beginselen van de wet worden nageleefd (onder meer de wettigheid, de verenigbaarheid van de gegevensoverdracht aan derden met de oorspronkelijke verwerking, kennisgeving aan de betrokkene).

Wat indien het land van bestemming niet voorkomt op de lijst van de Europese Commissie?

Indien het land waarnaar men gegevens wenst door te geven niet voorkomt op de lijst van de landen die een passend beschermingsniveau bieden, kan de *Cloud*provider (= de verantwoordelijke voor de verwerking, in dit geval de doorgifte) via contractuele weg een passende bescherming bieden. Zo kan deze bescherming worden bepaald aan de hand van een overeenkomst die bindend is voor de overdrager van de gegevens en voor de ontvanger van de gegevens en voldoende garanties bevat betreffende de bescherming van de gegevens. Om echter in België te kunnen worden toegepast, moet deze overeenkomst of modelovereenkomst na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, door een koninklijk besluit worden goedgekeurd.

Er bestaan modelovereenkomsten, ter beschikking gesteld door de Europese Commissie[22], die automatisch worden geacht voldoende garanties te bieden met betrekking tot gegevensbescherming (deze hoeven dus niet door een koninklijk besluit worden goedgekeurd indien ze als zodanig zonder wijzigingen worden gebruikt). Het voltaat moet een kopie van deze overeenkomsten aan de Commissie voor de bescherming van de persoonlijke levenssfeer worden gestuurd zodat zij kan nagaan of ze overeenstemmen met de modelovereenkomsten van de Europese Commissie.

Multinationale bedrijven die binnen hun groep gegevens wensen door te geven waarbij sommige leden van deze groep buiten de Europese Economische Ruimte zijn gevestigd in een land dat niet is erkend als een land dat "een passend beschermingsniveau biedt", kunnen toch voldoende garanties bieden voor gegevensbescherming door de aanneming van bindende bedrijfsvoorschriften of BCR's (Binding Corporate Rules[23]). Deze regels moeten door de verschillende nationale autoriteiten voor gegevensbescherming worden goedgekeurd (in België wordt deze goedkeuring gegeven met een koninklijk besluit na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer). Meer hierover is te vinden op de website van de Europese Commissie in een rubriek over de BCR's en de diverse hulpmiddelen uitgewerkt door de werkgroep "Artikel 29" om het de bedrijven gemakkelijker te maken[24].

Om geacht te worden als voldoende garantie biedend op het gebied van gegevensbescherming, moeten de bindende bedrijfsvoorschriften door de bevoegde nationale gegevensbeschermingsautoriteiten worden goedgekeurd. In dit opzicht heeft de werkgroep "Artikel 29" een samenwerkingsprocedure tussen de verschillende nationale gegevensbeschermingsautoriteiten opgesteld. Zo kan het multinationaal bedrijf zijn aanvraag bij één enkele nationale autoriteit indienen die vervolgens met de andere betrokken Europese autoriteiten contact opneemt om het ontwerp van bindende

[22] De modelovereenkomst werd goedgekeurd bij beschikking van de Commissie van 5 februari 2010 (document C (2010) 593). Het document bestaat alleen in het Engels: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:en:PDF

[23] BCR's zijn regels uitgewerkt door multinationale bedrijven (zoals een gedragscode) die bindend zijn voor alle entiteiten en werknemers van het bedrijf en die betrekking hebben op de internationale doorgifte van persoonsgegevens binnen de groep. http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

[24] http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm

bedrijfsregels samen te onderzoeken. Op die manier kunnen de verschillende autoriteiten een coherente beslissing nemen over het ontwerp van bindende bedrijfsregels[25].

Uitzonderingen
Als er geen overeenkomst is afgesloten, is de gegevensdoorgifte aan derde landen in bepaalde "uitzonderlijke gevallen" toch toegestaan. Dat is onder meer het geval wanneer de betrokken personen uitdrukkelijk hun toestemming geven voor de doorgifte van hun gegevens aan een bepaald land, of wanneer de doorgifte noodzakelijk is voor de tenuitvoerlegging van een overeenkomst met de betrokken persoon, of wanneer de gegevens afkomstig zijn uit een openbaar register ter informatie van het publiek (bijvoorbeeld telefoongids, handelsregister). Deze uitzonderingen moeten restrictief worden geïnterpreteerd en kunnen geen normaal kader vormen voor de doorgifte van gegevens, in het bijzonder wanneer het massale en repetitieve doorgiften betreft. Deze uitzonderingen mogen dus alleen als noodoplossing worden toegepast en hierbij moet snel een contractuele oplossing worden gevonden om de garanties van gegevensbescherming te formaliseren.

6.1.3 Wat is de "toepasselijke wet" op gegevensverwerking?

De vaststelling van de toepasselijke wet is belangrijk opdat de klant van een *cloud*provider (verantwoordelijke voor de verwerking of "controleur") zijn verplichtingen binnen een vastgesteld kader kan beoordelen. Let echter wel dat in geval van een klacht of een geschil deze wet van de bevoegde rechtbank moet worden onderscheiden die niet noodzakelijkerwijs dezelfde is: zo kan het gebeuren dat een buitenlandse rechter uitspraak moet doen in een zaak waarbij de Belgische wet van toepassing is. De toepasselijke wet kan verschillen naar gelang het gegevensverwerking of andere voorschriften zoals beveiliging betreft.

Voor de bescherming van persoonsgegevens, is de toepasselijke wet (zoals bepaald in de richtlijn 95/46) verbonden aan de verantwoordelijke voor de verwerking en niet aan de locatie waar de gegevens worden verwerkt of zijn opgeslagen, wat in het kader van *cloudcomputing* goed uitkomt omdat deze locatie niet altijd kan worden vastgesteld[26]. Het maakt dus geen verschil uit wanneer een in België gevestigde klant zijn gegevens in België, in de EU of buiten de EU verwerkt en opslaat: in elk van deze gevallen zal de Belgische wet van toepassing zijn.
Het volstaat dus dat de "controleur" (verantwoordelijke voor de verwerking) een "vestiging" heeft op het grondgebied van de EU of er "installaties" of "middelen" gebruikt (artikel 4.1 c van de richtlijn). De situatie wordt moeilijker wanneer de *cloud*provider ook de verantwoordelijke voor de verwerking is (hij levert online bijvoorbeeld een agenda waarmee particulieren hun afspraken kunnen beheren, een sociaal netwerk of een ruimte voor gegevensopslag) en hij geen vestiging heeft in de EU. Men moet er dan attent op zijn dat deze provider in de EU installaties of middelen gebruikt. Zoals de werkgroep

[25] Werkdocument van 14/4/2005 (EN) inzake een samenwerkingsprocedure met het oog op het uitbrengen van gemeenschappelijk advies betreffende de bescherming geboden door de "bindende bedrijfsvoorschriften" (WP107)
[26] Werkgroep Artikel 29 - gegevensbescherming, advies 8/2010 inzake toepasselijk recht http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

"Artikel 29" erop wijst, moet de term "middelen" dan worden geïnterpreteerd. Een loutere doorvoer van de verzamelde gegevens (doorgifte via het netwerk) of tewerkstelling van personeel (werknemer die de gegevens verzamelt) of sommige vormen van reclame (online-aanbod via een buitenlandse website) zouden niet voldoen, terwijl een vestiging in de EU, auto's met opnameapparatuur of specifieke apparatuur voor de opslag of verwerking dat wel zouden zijn.

Voor het vertrouwelijk karakter en de beveiliging van de verwerking, ligt de situatie anders (artikel 17(3)van de richtlijn omgezet in artikel 16 van de WPL): de toepasselijke wet is die van de lidstaat waar de processor (*cloud*provider of "verwerker") gevestigd is. Zelfs binnen de EU zijn in de verschillende lidstaten zeer uiteenlopende beveiligingseisen van toepassing. Sommige lidstaten hebben zich beperkt tot de overname van de algemene bepalingen van de richtlijn (de verantwoordelijke voor de verwerking moet de gepaste technische en organisatorische maatregelen treffen... een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen... toezien op de naleving van deze maatregelen), terwijl andere lidstaten, zoals België, schriftelijke contractuele bepalingen eisen die de aansprakelijkheid van de *cloud*provider bepalen en hem dezelfde verplichtingen opleggen als de verantwoordelijke voor de verwerking.

De Belgische wetgeving schrijft dus betere garanties voor die in een schriftelijke overeenkomst moeten worden opgenomen (deze overeenkomst wordt dan de "wet van de partijen"), onder meer wanneer een andere minder dwingende wet van toepassing is (wet van een andere lidstaat wanneer de *cloud*provider zijn activiteiten in de EU uitoefent, of wet van een derde land wanneer hij buiten de EU gevestigd is). Deze bepalingen hebben altijd betrekking op de beveiliging van persoonsgegeven, terwijl klanten andere gegevens met een vertrouwelijk karakter op de *cloud* kunnen plaatsen (bijvoorbeeld documentatie over de strategische doelstellingen van een bedrijf of over fabricagegeheimen). Daarom moet de klanten worden aanbevolen om in elk geval (en niet alleen voor de verwerking van persoonsgegevens) ervoor te zorgen dat ze de best mogelijke contractuele beveiliging hebben. Dat is een van de redenen van de aanbeveling van modelbepalingen (zie sectie 9).

6.1.4 De aansprakelijkheid van de *cloud*provider die gegevens host

Hosting door een *cloud*provider kan op velerlei soorten gegevens betrekking hebben (documenten, bestanden, muziekopnames, foto's, video's) die niet noodzakelijkerwijs als persoonsgegevens kunnen worden aangemerkt, maar die ook, en bovendien:

- "onwettig" kunnen zijn "***door de schending*** van de rechten van derden", d.w.z. waaraan diverse rechten verbonden kunnen zijn, hoofdzakelijk intellectuele rechten (in het bijzonder auteursrechten) die louter door de kopiëring, bewaring, bekendmaking of verspreiding van deze gegevens kunnen worden geschonden;
- "onwettig" kunnen zijn "***van nature***", d.w.z. waarvan de bewaring, verwerking of verspreiding bij wet verboden is (wij denken hier vooral aan beelden of films met een seksuele inhoud, die minderjarigen, misdaad of pedofiele daden/pedopornografie in beeld brengen);
- "onwettig" kunnen zijn "***door bestemming***", d.w.z. gebruikt voor doeleinden om een onwettige activiteit te organiseren of documenteren: terrorisme, spionage,

drugshandel, proxenetisme, mensenhandel, heling of verkoop van gestolen kunstwerken, wapenhandel, enz.

Deze aansprakelijkheid werd ingevoerd door de wetten van 11 maart 2003 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij[27]. Krachtens deze wet wordt hosting (host-diensten) gedefinieerd als "de levering van een dienst van de informatiemaatschappij - d.w.z. elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van de dienst wordt verricht - bestaande uit de opslag van de door een afnemer van de dienst verstrekte informatie.

Hoewel noch de richtlijn, noch de wet uitdrukkelijk betrekking hebben op *cloud*computing, kan de volgende vergelijking worden getrokken:

Dienstverlener van een dienst van de informatiemaatschappij	= *Cloud*-provider = Verstrekker van de *cloud*
Afnemer van de dienst	= *Cloud*-customer = Afnemer van de *cloud*

Artikel 20 van de wet die de bepalingen van de richtlijn omzet, bepaalt dat de dienstverlener van hosting (de *cloud*provider) niet aansprakelijk kan zijn voor de op verzoek van de afnemer van de dienst opgeslagen informatie (zijn klant van *cloud*diensten), mits bepaalde voorwaarden:

- Hij mag niet daadwerkelijk kennis hebben van de onwettige activiteit of informatie, of van omstandigheden waaruit het onwettige karakter van de activiteit of de informatie blijkt. Deze onwetendheid kan echter moeilijk worden staande gehouden, bijvoorbeeld wanneer de *cloud*provider een applicatiedienst heeft ontwikkeld (SaaS) die specifiek bestemd is voor de deling en uitwisseling van films of muziekopnames. Ook wanneer de dienstverlener van hosting op enige wijze actief heeft deelgenomen aan de verspreiding van de informatie, kan hij zich niet vrijstellen van aansprakelijkheid;
  Zodra hij daadwerkelijk kennis heeft van voornoemde activiteit of informatie, moet hij prompt handelen ende informatie verwijderen of de toegang ertoe onmogelijk maken;
  Hij moet de procureur des Konings onverwijld op de hoogte stellen. Dat maakt van de *Cloud*provider geen "politie" want hij heeft geen algemene verplichting van "actief toezicht" noch van "preventie van inbreuken"[28]. Hij moet echter wel "onverwijld" handelen, van. zodra hij kennis krijgt van de feiten[29].

[27] Deze Belgische wet zet de richtlijn 2000/31/CE om van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt doorgaans de "richtlijn inzake elektronische handel" genoemd.
[28] In een zaak doorverwezen door de Belgische rechtbanken, heeft het Europees Hof van Justitie geoordeeld dat de hostproviders geen algemene toezichtverplichting kan worden opgelegd (door hun bijvoorbeeld te verplichten tot een preventieve of systematische controle van alle door de klanten opgeslagen gegevens): zaak Sabam c/ Tiscali-Scarlet, Rb. Brussel (staking), 29 juni 2007, beschikbaar op http//www.droit-

Zonder dat hij tot systematisch toezicht kan worden verplicht, vloeit uit de voornoemde bepalingen voort dat de *cloud*provider een algemeen idee moet hebben van de gegevens die hem worden toevertrouwd en, althans in de dienstovereenkomst, formeel de verzekering moet krijgen van de klant dat de overgedragen, bewaarde en/of verspreide gegevens geen enkel onwettig karakter hebben (hetzij van nature, door bestemming of door de inbreuk op de rechten van derden).

6.1.5 Het bijzondere geval van elektronische communicatie

*Cloud*applicaties maken een snelle ontwikkeling door en uit sommige studies blijkt dat sociale netwerken een steeds groter aandeel van de elektronische communicatie innemen[30].

In dit kader isde *cloud*provider gebonden door de bepalingen die voortvloeien uit de omzetting van de richtlijn betreffende "privacy en elektronische communicatie"[31]. Deze richtlijn werd in 2002 goedgekeurd samen met een nieuwe wettelijke maatregel tot regulering van de sector van de elektronische communicatie. Ze bevat bepalingen over een aantal vrij gevoelige thema's zoals de bewaring van de verbindingsgegevens door de lidstaten voor politiële toezichtdoeleinden (achterhouden van gegevens), het verzenden van ongevraagde e-mails (spam), het gebruik van cookies en de opname van persoonsgegevens in openbare abonneelijsten.

6.2 Europees kader (huidige situatie en projecten)

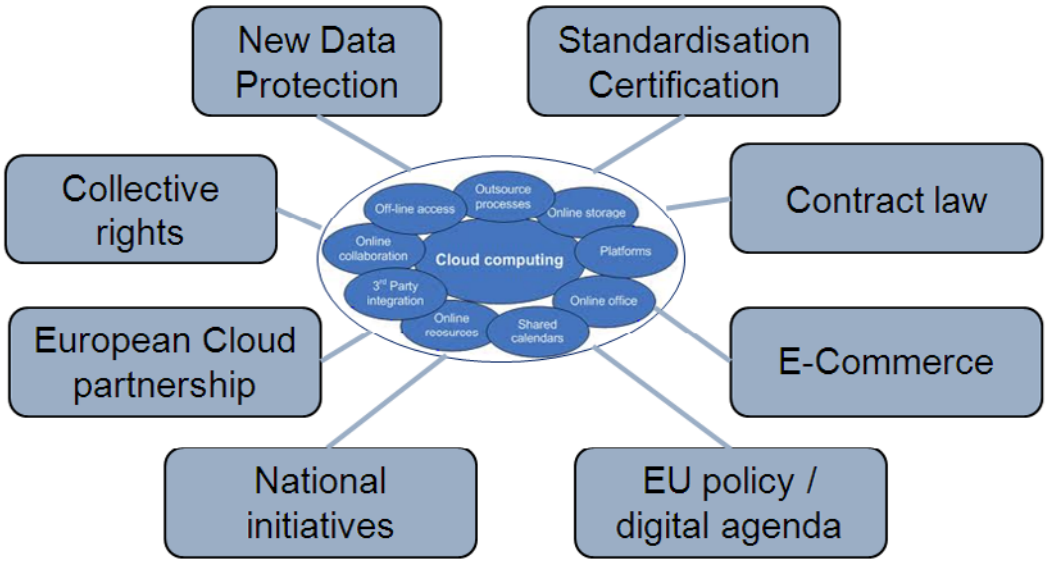
Cloudcomputing is een fenomeen dat in talrijke domeinen van de Europese politiek aan bod zal komen. Dit gaat van de bescherming van de consument over voorschriften met betrekking tot contracten, elektronische handel, standaardisering en certificering van bedrijven tot diverse aspecten van de bescherming van de persoonlijke levenssfeer.

technologie.be + HJEU 24 november 2011 C-70/10 en zaak Sabam / Netlog, HJEU, 16 februari 2012, C-360/10.

[29] §3 van artikel 20 van de wet bepaalt dat "*Wanneer de dienstverlener daadwerkelijk kennis krijgt van een onwettige activiteit of informatie, meldt hij dit onverwijld aan de procureur des Konings, die de nodige maatregelen neemt overeenkomstig artikel 39bis van het Wetboek van strafvordering*" (betreffende het beslag op immateriële gegevens).

[30] Zie « Les réseaux sociaux ont détrôné l'e-mail aux Etats-Unis » http://www.lemonde.fr/technologies/article/2011/02/08/les-reseaux-sociaux-ont-detrone-les-mails-aux-etats-unis_1476656_651865.html

[31] Richtlijn 2002/58/EG van 12 juli 2002, betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) - Publicatieblad L 201 van 31 juli 2002.



Afbeelding 10 – De cloud en de lopende evoluties

De bescherming van de persoonlijke levenssfeer lijkt het meest voor de hand liggend en het meest problematisch. Dit blijkt uit een groot aantal studies en politieke standpunten. Daarom behandelen we dit aspect als eerste.

6.2.1 Gegevensbescherming

Toepasselijk recht

In de Europese Unie worden vragen met betrekking tot de verwerking van persoonlijke gegevens met behulp van informatietechnologie geregeld door richtlijn 95/46/EG betreffende de gegevensbescherming[32]. Richtlijn 2002/58/EG betreffende de bescherming van de elektronische communicatie[33] gewijzigd door richtlijn 2009/136/EG[34] is van toepassing op de verwerking van persoonlijke gegevens als men communicatiediensten aan het publiek aanbiedt en dus in alle gevallen waarin deze diensten geleverd worden via de *cloud*.

Artikel 4 van richtlijn 95/46/EG schrijft voor dat de nationale wetgeving ter omzetting van de richtlijn geldig is voor de gegevensverwerking indien de desbetreffende verantwoordelijke gevestigd is op het grondgebied van één of meerdere lidstaten van de Unie of als de gebruikte uitrusting zich op het grondgebied van de Unie bevindt.

32 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonlijke gegevens en betreffende het vrije verkeer van die gegevens, OJ L 281 van 23/11/1995 p. 31

33 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37

34 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337 of 18.12. 2009 p. 0011 - 0036

De verantwoordelijke voor de verwerking en de 'verwerkers' van de gegevens: rol, rechten en verantwoordelijkheden

Alvorens de vragen met betrekking tot de verantwoordelijkheden en de verplichtingen van de verschillende actoren op het vlak van *cloud*computing te behandelen, moet eerst een definitie gegeven worden voor de concepten 'verantwoordelijke voor de verwerking' (in het Engels 'data controller') en 'verwerkers' (in het Engels 'data processor', de leverancier van de benodigde technologische hulpmiddelen). Aangezien de klant van de *cloud* de belangrijke beslissingen met betrekking tot de gegevensverwerking neemt (zijn doelstelling of het delegeren van de gegevensverwerking aan de verwerker), wordt hij beschouwd als verantwoordelijke voor de verwerking. De *cloud*provider is de organisatie die de *clou*dservices ter beschikking stelt (middelen en platform), en hierbij handelt in naam van de klant van de *cloud*, hierdoor handelt hij als onderaannemer.

In haar Opinie over *Cloud* Computing[35], gevalideerd op 1 juli 2012, argumenteert de werkgroep 'Artikel 29' over de gegevensbescherming (Art. 29 WP) dat veel klanten van *cloud*computing services van mening zijn dat er weinig mogelijkheden zijn om over de contractvoorwaarden te onderhandelen wegens de gestandaardiseerde aanbiedingen. De klant heeft echter in ieder geval het recht om zijn *cloud*provider te kiezen. Het is raadzaam hierbij te opteren voor een provider die de eisen op het vlak van gegevensbescherming strikt naleeft. Zoals bevestigd door de werkgroep 'Artikel 29', vooraf gevalideerd in Opinie 1/2010 over de concepten 'verantwoordelijke voor de gegevensverwerking' en 'verwerker'[36], 'mag het bestaan van een beschermende wet niet beschouwd worden als een excuus of afdoende bescherming die de verantwoordelijke voor de verwerking toelaat om het even welke contractuele voorwaarden te aanvaarden die een onevenwicht weerspiegelen tussen de macht van een kleine verantwoordelijke voor gegevensverwerking ten opzichte van een grote leverancier van diensten'.

Eén van de belangrijke verplichtingen voor *cloud*providers is een vertrouwelijke behandeling. De verwerkers moeten hierbij het *clou*dtype (bv. publiek, privaat, gemeenschappelijk of hybride) en het soort service dat het contract voorschrijft in overweging nemen. Ze zijn ook verplicht de EU-normen in hun veiligheidsmaatregelen te implementeren. Bovendien moeten de onderaannemers de verantwoordelijke voor de verwerking bijstaan bij de naleving van de rechten van de klanten.
Alle relevante verplichtingen op het vlak van *cloud*computing zijn eveneens van toepassing voor de onderaannemers van de *cloud*leverancier ('sub-processors' van de gegevens); de contracten tussen de *cloud*provider en onderaannemers moeten gebaseerd zijn op de oorspronkelijke contractvoorwaarden tussen de klant van de *cloud* en de *cloud*provider.

35 Article 29 Data Protection Working Party, WP196 – Opinion 05/2012 on Cloud Computing, adopted July 1st 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/index_en.htm#h2-1.
36 Opinion 1/2010 on the concepts of "controller" and "processor"- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Verwachte evolutie: een nieuw algemeen reglement

Om een aantal garanties op het niveau van de onderaannemers in te bouwen, heeft de Commissie nieuwe bepalingen opgenomen in haar voorstel van 2012 voor een Algemeen reglement op de gegevensbescherming[37].

Waarom een reglement? Om te vermijden dat een nieuwe richtlijn omgezet wordt met verschillende aanpassingen of toevoegingen in de afzonderlijke lidstaten. Het reglement zal het eerste bindende internationale instrument zijn met als doel de bescherming van persoonlijke gegevens tegen misbruik van de geautomatiseerde verwerking van persoonlijke gegevens.

Het voorgestelde reglement versterkt de rechten van de personen die betrokken zijn bij de verwerking van hun persoonlijke gegevens en legt nieuwe verplichtingen op aan de voor deze verwerking verantwoordelijke bedrijven.

Het ontwerp toont aan dat de Europese Commissie niet van plan is zich te beperken tot een eenvoudige aanpassing van het bestaande rechtskader, maar het rechtskader wil harmoniseren, de rechten van de betrokkenen wil versterken en de naleving van de reglementering effectiever wil maken wat onderstaande punten betreft:

1. Harmoniseren en actualiseren

Het huidige rechtskader uit 1995 was niet rechtstreeks van toepassing op nationaal niveau. Hierdoor heeft iedere lidstaat de regelgeving omgezet in een nationale wetgeving waarbij geprofiteerd werd van de toegestane vrijheden. Het gevolg is dat er aanzienlijke wettelijke verschillen zijn tussen de lidstaten. Een identieke situatie zal niet noodzakelijk op dezelfde manier geregeld worden in bijvoorbeeld Italië, Duitsland, het Verenigd Koninkrijk of België. Een bedrijf met vestigingen in elk van deze vier landen moet zijn activiteiten dan ook afstemmen op verschillende wetteksten, terwijl dit bedrijf vaak veel persoonlijke gegevens via en tussen de verschillende vestigingen verzamelt en uitwisselt.

Het tweede nadeel vloeit voort uit het feit dat deze richtlijn opgesteld werd voor het ontstaan van sociale netwerken en *cloud*computing. Deze elementen zijn niet de enige determinerende factoren in de evolutie van de verwerking van persoonlijke gegevens. Ze zijn wel een aanwijzing voor de enorme groei en de globalisering van de verwerking van persoonlijke gegevens tijdens het voorbije decennium.

2. De bescherming van de betrokken personen versterken

De bescherming van de 'betrokken personen' wordt in het ontwerpreglement versterkt door:

- Een extraterritoriale toepassing: terwijl de huidige richtlijn bijna fysieke aanknopingscriteria tussen de betrokken persoon en een deelnemende staat voorziet voor de toepassing van de Europese regelgeving, voorziet het ontwerpreglement een extraterritoriale toepassing van het Europese recht.

37 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 25.1.2012

Hierdoor verdwijnen de eisen voor een 'vestiging' van de verantwoordelijke of zijn onderaannemer op het grondgebied van de Unie, of de aanwezigheid van 'al dan niet geautomatiseerde middelen' op het grondgebied van de Unie. Het nieuwe reglement zal dus gelden voor iedere operator die verwerkingsactiviteiten uitvoert in de Unie, zelfs bij het ontbreken van een vestiging of middelen op het grondgebied van de Unie.

- Een verduidelijking van het recht om te worden vergeten, dit wil zeggen het effectief doen verwijderen van gegevens als hun bewaring niet langer wenselijk is. Dit recht is bijzonder nuttig in het kader van het gebruik van sociale netwerken.

- Een nieuw recht op 'portabiliteit' van gegevens, waardoor een klant van de *cloud* mag eisen dat zijn gegevens bewaard worden in een formaat (bijvoorbeeld een open standaard) dat toelaat de gegevens over te dragen naar een andere *cloud*provider.

- Een verduidelijking van een aantal begrippen zoals 'betrokken persoon' (van wie de gegevens verwerkt worden). Dit is iedere persoon die rechtstreeks of onrechtstreeks geïdentificeerd kan worden door de verantwoordelijke voor de verwerking of door ieder ander natuurlijk persoon of rechtspersoon (dit kan dus ook een persoon zijn van wie een foto genomen werd, eventueel zonder zijn medeweten, om vervolgens verwerkt te worden in de *cloud*, op een sociaal netwerk te publiceren enz.), en de vrijelijk gegeven 'toestemming' die de aanwijzing vormt van een specifieke, weloverwogen en expliciete wens, (wat zowel betrekking kan hebben op minderjarigen, voor wie de toestemming van een ouder nodig is, als op andere personen van wie de vrijheid beperkt is – bijvoorbeeld door een arbeidsovereenkomst).

3. Verplichtingen en sancties uitbreiden

De nieuwe verplichtingen die voortvloeien uit het ontwerpreglement hebben betrekking op de aanduiding van een 'geschoold bediende verantwoordelijk voor de persoonlijke gegevens' in bedrijven met meer dan 250 werknemers, met de verplichting om in bepaalde gevallen een rapport op te stellen over de impact van de geplande verwerking op de bescherming van de gegevens, de documentatie van de genomen beleids- en beschermingsmaatregelen en de uitgevoerde activiteiten, de bekendmaking van problemen (bijvoorbeeld gegevensverlies) aan de bevoegde nationale gegevensbeschermingsautoriteit en in sommige gevallen aan de betrokken persoon. Ten slotte worden ook de sancties in geval van een overtreding uitgebreid. Deze kunnen oplopen tot 5 % van het jaarlijkse omzetcijfer van de verantwoordelijke voor de verwerking.

Bepalingen betreffende de *cloud*provider

In artikel 26(2) van het reglementeringsvoorstel zal de interventie van een verwerker geregeld worden door een contract of ieder ander wettelijk bindend document, waardoor de verwerker en de verantwoordelijke voor de verwerking aan elkaar gebonden zijn, en waarin in het bijzonder gepreciseerd wordt dat de verwerker (bijvoorbeeld de

*cloud*provider) uitsluitend kan onderaanbesteden aan een derde met de voorafgaande toestemming van de verantwoordelijke voor de verwerking.

Zoals hierboven uitgelegd, hangt de geldigheid van de verwerking van persoonlijke gegevens in de *cloud* af van de conformiteit aan de EU-voorschriften met betrekking tot de bescherming van gegevens. Deze voorschriften omvatten transparantie bij de gegevensverwerking ten opzichte van betroffen persoon, het principe van de beperking van de verwerking tot het beoogde doeleinde, en de verplichting om de gegevens te corrigeren indien nodig en deze te schrappen als de bewaring niet langer noodzakelijk is. Bovendien moeten passende technische en organisatorische maatregelen geïmplementeerd worden om bescherming en beveiliging van de gegevens te garanderen. Naast de belangrijkste veiligheidseisen op het vlak van beschikbaarheid, vertrouwelijkheid en integriteit moeten bijkomende criteria zoals transparantie, bescherming, de mogelijkheid om in te grijpen, de verantwoordelijkheid voor eventuele schade en overdraagbaarheid in overweging genomen worden. Volgens artikel 17(3) van richtlijn 95/46/EG moet het contract dat formeel ondertekend wordt met de *cloud*provider bepalingen bevatten met betrekking tot deze veiligheidsmaatregelen.

In het algemeen moet het contract de volgende elementen bevatten, zoals vastgelegd door de werkgroep 'Artikel 29':

1) Een gedetailleerde beschrijving van de vragen of verwachtingen van de klant van de *cloud* ten opzichte van zijn provider, in het bijzonder over het service level agreement (SLA, die objectief en meetbaar moet zijn) en de geldige sancties (bedragen die betaald moeten worden om schade te compenseren en mogelijkheid om actie te ondernemen tegenover de provider in geval van non-conformiteit).
2) De veiligheidsmaatregelen bepalen waarnaar de *cloud*provider zich moet richten.
3) De aard van de services en de periode waarbinnen de *cloud*provider de services levert, de omvang, wijze en doelstelling van de verwerking van de persoonlijke gegevens en het type van persoonlijke gegevens die verwerkt worden.
4) De voorwaarden voor de teruggave van de persoonlijke gegevens en hun vernietiging (op de site van de *cloud*provider) nadat de service beëindigd werd.
5) Een bindende vertrouwelijkheidsclausule voor de *cloud*provider en al zijn medewerkers die toegang tot de gegevens hebben.
6) De verplichting voor de *cloud*provider om zijn klant te helpen bij de uitoefening door de betrokken personen van hun recht van inzage, verbetering of schrapping van hun gegevens.
7) Een formele bepaling die voorschrijft dat de *cloud*provider de gegevens niet mag meedelen aan derden, zelfs niet voor beveiligingsredenen, behalve indien het contract deze mogelijkheid voorziet.
8) De verantwoordelijkheden van de *cloud*provider voor kennisgeving aan zijn klant in geval van schade aan de toevertrouwde gegevens of elk incident dat gevolgen kan hebben voor de gegevens die de klant toevertrouwd heeft.
9) Verplichting voor de *cloud*provider om de klant een lijst te overhandigen met de fysieke plaatsen waar zijn gegevens verwerkt kunnen worden.

10) Recht van de klant van de *cloud* (verantwoordelijke voor de verwerking) op informatie waarmee hij de naleving van het contract kan controleren, en verplichting voor de *cloud*provider om de klant hierin bij te staan.
11) Verplichting voor de *cloud*provider om de klant te informeren over belangrijke wijzigingen over de service, zoals het voorzien van bijkomende functionaliteiten.
12) Beschrijving van activiteiten in het kader van logging en auditing van de verwerking die door de *cloud*provider of zijn onderaannemers uitgevoerd werden.
13) Kennisgeving aan de klant van de *cloud* over aanvragen voor toegang tot de gegevens die de *cloud*provider wettelijk gezien moet beantwoorden, afkomstig van de bevoegde gerechtelijke of politionele autoriteiten, behalve indien deze kennisgeving verboden is door de wet, bijvoorbeeld om de vertrouwelijkheid van een gerechtelijk onderzoek niet te schenden.
14) Algemene verplichting van de *cloud*provider om te garanderen dat zijn interne organisatie en zijn procedures voor de verwerking van de gegevens voldoen aan de geldende nationale en internationale normen.

Waarschuwing in geval van schending van de gegevens

In het algemene ontwerpreglement over gegevensbescherming wordt voorgesteld om een clausule op te nemen die voorschrijft dat de gegevensbeschermingsautoriteiten en de klanten ingelicht moeten worden in geval van een inbreuk in verband met persoonsgegevens. De bepalingen van het ontwerp voorzien dat de gegevensbeschermingsautoriteiten 'indien mogelijk' geïnformeerd moeten worden binnen een termijn van 24 uur; de betroffen personen moeten binnen een 'passende' termijn geïnformeerd worden. Het ontwerpreglement breidt de eis met betrekking tot de kennisgeving over een inbreuk in verband met gegevens van providers van telecommunicatie- en internetdiensten in de EU uit naar alle sectoren, wat een belangrijke stap voorwaarts is rekening houdend met de toename van de algemene risico's op het vlak van informaticacriminaliteit en gegevensverlies.

Gegevensoverdracht buiten de EER

Artikel 25 en 26 van richtlijn 95/46/EG bevat principebepalingen met betrekking tot de overdracht van persoonlijke gegevens naar derde landen en afwijkingen van deze principes. Het concept van een geschikt niveau van gegevensbescherming maakt de verwerking van gegevens buiten de EER mogelijk als een dergelijke bescherming gegarandeerd is. Anders moeten de verantwoordelijke voor de verwerking en/of de *cloud*provider beantwoorden aan specifieke voorwaarden. Aangezien het zelden mogelijk is om de gegevens in een *cloud*omgeving te situeren, wordt de toepassing van een vast rechtskader vrij ingewikkeld.

Ten eerste zijn de overwegingen met betrekking tot een geschikt beschermingsniveau onderworpen aan geografische beperkingen en kunnen dus niet alle overdrachten binnen de *cloud* dekken. Dit geldt ook voor de criteria volgens het Safe Harbor-programma. De werkgroep 'Artikel 29' is immers van mening dat het loutere bestaan van het Safe Harbor-certificaat (dat meestal voortvloeit uit een gewone verklaring) niet volstaat en dat de importeur van de gegevens concreet moet aantonen dat de principes met betrekking tot de bescherming van de persoonlijke levenssfeer gerespecteerd werden. Bovendien moet

gecontroleerd worden of de contracten die opgesteld worden door de *cloud*provider voldoen aan de geldige nationale voorschriften. Tot slot kan het nodig zijn om bijkomende voorzorgsmaatregelen te implementeren rekening houdend met de specifieke aard van de *cloud* (zo worden sommige specifieke veiligheidsrisico's zoals de onvolledige schrapping van gegevens mogelijk onvoldoende behandeld door de bestaande Safe Harbor-principes met betrekking tot gegevensbeveiliging).

De contractuele standaardclausules (SCC) zoals ze door de Europese Commissie goedgekeurd werden om een internationaal kader voor gegevensoverdracht[38] te scheppen, moeten in deze context eveneens vermeld worden. Als de *cloud*provider als verwerker[39] optreedt, kunnen de modelclausules in zijn contract met de verantwoordelijke voor de verwerking gebruikt worden om passende beschermingsmaatregelen aan te bieden.

Een ander instrument zijn de bindende bedrijfsvoorschriften (binding corporate rules of BCR) met richtlijnen voor bedrijven die gegevens transfereren binnen hun groep. Met dergelijke BCR kunnen persoonlijke gegevens getransfereerd worden naar het bedrijf van de groep dat instaat voor een verwerking, waarbij ze bij de *cloud*provider bewaard blijven en waarbij men tegelijk profiteert van het passende beschermingsniveau voor alle bedrijven binnen de groep.

Slotopmerkingen en aanbevelingen

In haar 'Sopot Memorandum' uit 2012 over *cloud*computing is de International Working Group over gegevensbescherming in de telecommunicatiesector onder andere van mening dat deze technologie per definitie 'grenzeloos en grensoverschrijdend' is en dat 'gegevensverwerking een wereldwijde aangelegenheid is'[40]. Daarom moeten organisaties die zich willen positioneren op de markt van *cloud*computing services zich bewust zijn van de relevante risico's op het vlak van gegevensbescherming en in het bijzonder de verplichtingen met betrekking tot veiligheid en internationale transfers naleven.

De naleving van de voorschriften met betrekking tot gegevensbescherming door klanten en providers van de *cloud* moet in de eerste plaats gebaseerd zijn op het huidige rechtskader, dit wil zeggen richtlijn 95/46/EG. Dit werd bevestigd tijdens de vergadering van 16 januari 2013 met de vertegenwoordigers van de Europese Commissie van DG CONNECT en het team dat verantwoordelijk is voor deze studie[41].

38 Decision 2010/87/EU of the European Commission of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39/5, 12.2.2010
39 De Nederlandse tekst van de richtlijn vertaalt het Engelse begrip 'processor' met 'verwerker'.
40 International Working Group on Data Protection in Telecommunications, Working Paper on Cloud Computing – Privacy and Data Protection issues – "Sopot Memorandum, 675.44.8, Sopot, 24.3.2012
41 Meeting with the European Commission, DG CONNECT/E2 Software & Services, Cloud, Brussels, 16.01.2013

Deze vergadering had tot doel de bespreking van een aantal aspecten van *cloud*computing zoals vermeld in de Digitale agenda voor Europa[42]. Er werd benadrukt dat men zich vooral verder moet concentreren op de huidige wettelijke mogelijkheden aangezien nieuwe voorschriften met betrekking tot gegevensbescherming (zoals het voorstel voor een nieuw reglement) pas na veel jaren in de realiteit vertaald kunnen worden.
Er werd echter een opmerking gemaakt over de concepten van 'verantwoordelijke voor de verwerking' en 'verwerker' (onderaannemer) aangezien het ontwerpreglement hierover enige onduidelijkheid heeft laten bestaan en men heeft voorgesteld hier met verklarende richtlijnen te werken. Op basis van de aanbevelingen van DG JUSTICE werd er beslist mogelijke verklaringen eerder op te nemen in de implementatieaktes of delegatie na de goedkeuring van het reglement. Een dergelijke oplossing lijkt doeltreffender rekening houdend met het veranderlijke karakter van *cloud*computing. Te gedetailleerde bepalingen zouden in de toekomst nieuwe aanpassingen noodzakelijk kunnen maken.

Wat de toekomstige ontwikkelingen van de regelgeving op het vlak van *cloud*computing betreft, heeft de werkgroep Artikel 29 enkele aanbevelingen voorzien, die we hierna beschrijven:

- Een beter evenwicht tussen de verantwoordelijke voor de verwerking en de *cloud*provider wat de verantwoordelijkheden betreft: artikel 26 van het ontwerpreglement verplicht de provider hulp te bieden aan de verantwoordelijke wat de naleving van de veiligheidsvoorschriften en de andere verplichtingen betreft. Bovendien introduceert artikel 30 van het ontwerp een wettelijke verplichting voor de *cloud*provider om passende technische en organisatorische maatregelen te nemen. Het ontwerp voorziet ook dat een verwerker (*cloud*provider) op dezelfde wijze verantwoordelijk wordt en onderworpen wordt aan dezelfde controleregels in het geval deze verwerker de instructies van de verantwoordelijke van de verwerking niet naleeft. De werkgroep 'Artikel 29' is dan ook van mening dat het ontwerpreglement een goede basis vormt om ter verhelpen aan het onevenwicht dat *cloud*computing vaak kenmerkt. De klant (vooral als het een kmo betreft) kan immers moeilijkheden ondervinden om de door de wet op de gegevensbescherming opgelgde volledige controle uit te oefenen, als gevolg van de de manier waarop de *cloud*provider zijn service levert. Rekening houdend met de asymmetrische juridische situatie van de betroffen personen (de individuele personen waarvan de gegevens verwerkt worden) en de klanten van de *cloud* (kleine bedrijven) tegenover de reuzen van de *cloud*computing, wordt aangeraden dat de organisaties die de klanten beschermen of de sociale partners vertegenwoordigen een actievere rol krijgen en de bevoegdheid krijgen om te onderhandelen over meer evenwichtige voorwaarden met de grote providers.

42 Communication from the Commission of 3 March 2010 - Europe 2020 A strategy for smart, sustainable and inclusive growth, COM(2010) 2020 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

- De werkgroep 'Artikel 29' is van mening dat nieuwe bepalingen over de toegang tot de gegevens door de Staatsveiligheid of de justitionele en politionele autoriteiten toegevoegd moeten worden aan het ontwerpreglement. De werkgroep vindt dat de verantwoordelijken voor de verwerking die werkzaam zijn in de Unie nooit persoonlijke gegevens bekend mogen maken aan justitionele en administratieve autoriteiten van een derde land, behalve indien dit toegelaten is in het kader van een internationaal akkoord of een verdrag over wederzijdse bijstand, of goedgekeurd is door de toezichthoudende autoriteit (van de betrokken lidstaat). Het reglement van de Raad (EG) nr. 2271/96[43] kan volgens de werkgroep 'Artikel 29' als wettelijke basis dienen. De werkgroep maakt zich zorgen over dit tekort in het ontwerpreglement dat voorgesteld wordt door de Commissie, want dit creëert een juridische onzekerheid als de gegevens verwerkt worden in centra die over de hele wereld verspreid liggen. Om die reden suggereert de werkgroep om in het reglement de verplichting op te nemen om de procedure te volgen die voorzien wordt door de verdragen over wederzijdse juridische bijstand (MLAT: Mutual Legal Assistance Treaty) in de gevallen waarin deze openbaarmaking niet toegelaten is door de wet van de Unie of haar lidstaten.
  Deze aanbeveling is rechtstreeks gekoppeld aan de bezorgdheid met betrekking tot de Amerikaanse 'Patriot Act' die de Amerikaanse overheid ongebreideld toegang geeft tot de gegevens op *cloud*servers van Amerikaanse providers (of die ten minste een vestiging in de Verenigde Staten hebben, wat hen zou verplichten om aan de vraag voor toegang van de Amerikaanse autoriteiten te voldoen). Volgens de belangrijkste overwegingen van de studie van het Europees Parlement over de strijd tegen informaticacriminaliteit en de bescherming van de persoonlijke levenssfeer op de *cloud*[44] werden de aspecten 'privacy' en gegevensbescherming compleet verwaarloosd, zowel in de 'Patriot Act' als in de Foreign Intelligence Surveillance Amendment Act (FISAA) van 2008, ondanks hun belangrijke impact op de soevereiniteit van de EU wat haar gegevens betreft en de bescherming van de rechten van de burgers.
  De experten van de Commissie die aanwezig waren tijdens de ontmoeting met voor deze studie verantwoordlijke team hadden echter een andere mening. Zij verwijzen naar de wetgeving van sommige lidstaten die volgens hen gelijkaardige bepalingen hieromtrent bevat die mogelijk nog toleranter of lakser zijn. Zo kunnen de Franse autoriteiten die bevoegd zijn voor strafzaken toegang tot de gegevens verkrijgen zonder de betrokken persoon te informeren. De Britse autoriteiten die verantwoordelijk zijn voor rechtshandhaving kunnen zich op gelijkaardige rechten zoals voorzien in de Patriot Act beroepen. Bovendien werd het nieuwe voorstel voor een richtlijn die de bescherming bij de gegevensverwerking uitbreidt tot de Europese autoriteiten die verantwoordelijk zijn voor juridische opdrachten[45]

43 Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, OJ L 309 , 29/11/1996 P. 0001 - 0006
44 Study on Fighting Cybercrime and Protecting Privacy in the Cloud, requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; study conducted uUnder coordination of the Justice and Home Affairs Section of the Centre for European
Policy Studies (CEPS) and the Centre d'Etudes sur les Conflits (C&C), 2012
45 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention,

aangehaald als illustratie van een coherente en transparante Europese aanpak op het vlak van gegevensbescherming, zowel op het gebied van repressieof preventie van criminaliteit als voor wat betreft internationale samenwerking.

- Bijzondere voorzorgen te nemen door de openbare sector: De werkgroep 'Artikel 29' is van mening dat het raadzaam is een bijzonder veiligheidsmechanisme toe te voegen over de noodzaak dat een openbaar organisme in de eerste plaats evalueert of de communicatie, de verwerking en de opslag van de gegevens buiten het nationale territorium onaanvaardbare risico's op het vlak van veiligheid en bescherming van de persoonlijke levenssfeer kan vormen voor de burgers, de nationale veiligheid en de economie – vooral wat kwetsbare gegevens (bijv. tellingen) of strategische diensten (bijv. medische verzorgingen) betreft. Volgens deze visie moet dit punt in overweging genomen worden telkens vertrouwelijke gegevens verwerkt worden in de *cloud*. Vanuit dit oogpunt kunnen de nationale regeringen en de instellingen van de Europese Unie overwegen om de studie verder te zetten over een 'Europese regerings*cloud*' die een supranationale, virtuele ruimte zou vormen met uniforme en geharmoniseerde regels.

6.2.2 Bescherming van de consument en contractueel recht

<u>Akkoorden over grensoverschrijdende vergunningen en vergunningen voor privékopieën</u>

Zoals uitgelegd in de Europese strategie over Cloud Computing[46] moeten de consumenten de informatie op een wettelijke manier kunnen gebruiken (gekocht – beschermd door het auteursrecht) in één of meerdere lidstaten van de EU zonder de toegang te verliezen tot de diensten waarvoor ze betaald hebben in om het even welke andere lidstaat. De innovatie die hierdoor ontstaat kan nieuwe inkomstenbronnen doen ontstaan. Het voorstel van de Commissie voor een richtlijn over het collectief beheer van de auteursrechten[47] zal, als het aangenomen wordt, veel voorwaarden bevatten met betrekking tot grensoverschrijdende vergunningen betreffende de inhoud van de *cloud* op het vlak van muziek. De Europese Commissie onderzoekt momenteel andere maatregelen met betrekking tot het Groenboek[48], zoals de vereenvoudiging van licenties voor de onlinedistributie van audiovisuele werken, in het bijzonder transnationaal. Met een *cloud*computing service kan ook informatie in de *cloud* bewaard worden. De consument kan deze ook gebruiken als digitaal opslagmedium voor zijn eigen informatie en als synchronisatiemiddel om vanop verschillende toestellen toegang te verkrijgen tot zijn informatie. Hiermee moet rekening gehouden worden bij de behandeling van een eventuele inning van belastingen voor privékopieën van werken.

---

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

46 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final, 27.9.2012

47 Voorstel voor een RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende het collectieve beheer van auteursrechten en naburige rechten en de multiterritoriale licentieverlening van rechten inzake muziekwerken voor onlinegebruik op de interne markt, COM(2012) 372 definitief, 11.7.2012

48 GROENBOEK over de onlinedistributie van audiovisuele werken in de Europese Unie – Naar een digitale eengemaakte markt: mogelijkheden en uitdagingen, COM(2011) 427

De analyse van de experten met betrekking tot de mogelijke wettelijke acties op het vlak van heffingen op privékopieën in de EU wordt momenteel uitgevoerd onder leiding van de voormalig Europees commissaris van Justitie en Interne Aangelegenheden, de heer Antonio Vitorino[49]. Op basis van de conclusies zal de Commissie de afbakening van de uitzondering van privékopieën en de relevantie van heffingen evalueren, in het bijzonder in welke mate de *cloud*computing services die de rechtstreekse vergoeding van rechthebbenden mogelijk maken, uitgesloten zijn van het stelsel van heffingen voor privékopieën.

Degelijke en rechtvaardige contractvoorwaarden

Gezien het complexe rechtskader met betrekking tot *cloud*computing gebruiken de *cloud*providers meestal complexe service level agreements (SLAs). Deze 'te nemen of te laten' contracten schikken de providers uitstekend. Dit is echter niet het geval voor de gebruikers van de service, aangezien er heel weinig mogelijkheden zijn om te onderhandelen over wijzigingen of verbeteringen van het contract. Degelijke en rechtvaardige standaardcontractvoorwaarden opstellen, zal dus nodig zijn om meer bescherming aan de eindgebruikers van de *cloud* te bieden.

Zoals bevestigd tijdens de vergadering met de vertegenwoordigers van DG CONNECT bestaan dergelijke voorwaarden momenteel nog niet maar men is hier op het terrein mee bezig. De voorwaarden die ontwikkeld werden door het Amerikaanse National Institute for Standards and Technology (NIST) worden momenteel bestudeerd. Een dialoog met de betrokken partijen wordt gevoerd om referentiegevallen/situaties uit de praktijk voor te stellen op basis van de resultaten van deze besprekingen. De groep van de providers is heel divers. Het is dus belangrijk om de belangen van alle leden te vertegenwoordigen. Het overleg bevindt zich momenteel in een beginfase en de samenwerking met de andere diensten van de Europese Commissie zoals het DG JUSTICE is belangrijk. Voor de consumenten en kleine ondernemingen voorziet het voorstel van de Commissie betreffende een gemeenschappelijk Europees kooprecht[50] duidelijke antwoorden op veel onzekerheden die vaak gecreëerd worden door uiteenlopende nationale bepalingen.

Het is evident dat de creatie van best practices met betrekking tot de modelcontractvoorwaarden de *cloud*providers ten goede zou komen aangezien dit het vertrouwen van potentiële klanten zou versterken. Eens de richtsnoeren gevalideerd werden op Europees niveau en erkend zijn door de toezichthoudende autoriteiten van de lidstaten, zullen deze dienen als praktische gedragsregels op het terrein. Hiervoor wordt de aandacht gevestigd op de doelstellingen van de Commissie voor 2013, zoals

49 See Commission Communication "A Single Market for Intellectual Property Rights" COM(2011) 287 – Action 8 – which launched this mediation process in order to "explor[e] possible approaches with a view to harmonising the methodology used to impose levies [....]" and stated that a "concerted effort on all sides to resolve outstanding issues should lay the ground for comprehensive legislative action at EU level". The eCommerce Communication, COM(2011) 942 final, envisages a legislative initiative on private copying in 2013. The question on how the private copying exception applies to illegal content was equally addressed by the European Court of Justice as referred by the Austrian courts in Kino.to and the Dutch courts in ACI Adam B.V. v Stichting de Thuiskopie.

50 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende een gemeenschappelijk Europees kooprecht, COM(2011) 635 definitief, 11.10.2011

opgesomd in haar strategie met betrekking tot *cloud*-computing, op het niveau van de contractuele standaardvoorwaarden:

- Samen met de belanghebbenden typeclausules op serviceniveau uitwerken die geldig zijn voor de contracten tussen dienstverleners op het vlak van *cloud*toepassingen en professionele gebruikers, rekening houdend met de verworven kennis op dit vlak;
- In overeenstemming met de communicatie met betrekking tot het Gemeenschappelijk Europees Kooprecht[51] worden voorstellen opgesteld voor typeclausules en -contractvoorwaarden aan de particulieren en kleine ondernemingen voor de aspecten die betrekking hebben op het voorstel in kwestie; streven naar een normalisatie van de belangrijkste clausules en voorwaarden voor contracten, om de beste praktijken te ontwikkelen op het vlak van contractuele voorwaarden voor *cloud* services over de levering van 'digitale informatie';
- Samen met vertegenwoordigers van de sector werd een groep experten voor samengesteld. Deze kreeg de opdracht om tegen eind 2013, degelijke en rechtvaardige typeclausules en -contractvoorwaarden op te stellen voor particulieren en kleine ondernemingen op basis van een facultatief instrument van hetzelfde type, voor de aspecten die niet onder het Gemeenschappelijk Europees Kooprecht vallen,;
- Europa betrekken bij de wereldwijde groeidynamiek op het vlak van *cloud*-services door de standaardcontractvoorwaarden die van toepassing zijn op de overdracht van persoonlijke gegevens naar derde landen te heronderzoeken en deze eventueel aan te passen aan *cloud*toepassingen en door de nationale gegevensbeschermingsautoriteiten uit te nodigen om specifieke bindende bedrijfsvoorschriften voor *cloud*providers[52] goed te keuren;
- Samen met de betrokken sector werken aan de goedkeuring van een gedragscode voor de *cloud*providers om een uniforme toepassing van de voorschriften over gegevensbescherming te stimuleren. Deze gedragscode kan ter goedkeuring overhandigd worden aan de werkgroep 'Artikel 29' om de rechtszekerheid en de coherentie tussen de gedragscode en het Europese recht te garanderen.

6.2.3 Elektronische handel

Het bestaande wettelijke communautaire instrument dat gebruikt kan worden op het terrein is de richtlijn over de elektronische handel[53]. Eén van de belangrijkste aspecten van de

51 Mededeling van de Commissie 'Een Europese consumentenagenda – Vertrouwen en groei stimuleren', COM(2012) 225 definitief
52 De relevante adviezen van de werkgroep 'Artikel 29' (zie WP 195 en WP 153) zullen als basis dienen voor dit project van de Commissie. De bindende bedrijfsvoorschriften (BCR) vormen één van de middelen om de wettelijke internationale transfer van gegevens mogelijk te maken: ze bevatten bepalingen over de manier waarop de verschillende entiteiten van een bedrijf, om het even waar ter wereld ze gevestigd zijn, persoonlijke gegevens verwerken.
53 Richtlijn 2000/31/EG van het Europees Parlement en van de Raad van 8 juni 2000, betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel') OJ L 178/1, 17.7.2000

richtlijn betreft de intermediaire verantwoordelijkheid. Dit omvat de verantwoordelijkheid van de *cloud*provider voor de gegevens die hij 'ontvangt'. De doelstelling van dit stelsel bestaat erin te garanderen dat tussenpersonen niet aansprakelijk gesteld kunnen worden (bijvoorbeeld bij activiteiten in het kader van 'Safe Harbor') in gevallen waar ze niet verantwoordelijk zijn voor de desbetreffende informatie. De richtlijn maakt een onderscheid tussen 'mere conduit', 'caching' en 'hosting'. De dienstverlener die optreedt als louter doorgeefluik waarbij informatie doorgegeven wordt via een netwerk is niet aansprakelijk voor zover hij niet aan de oorsprong van de gegevens ligt / de gegevens niet ontvangt of wijzigt. Wat 'caching' betreft, zal de serviceprovider die de automatische, tussentijdse en tijdelijke opslag van informatie ondersteunt, uitsluitend om de doorgifte van de informatie doeltreffender te maken, niet aansprakelijk zijn voor de aard van de informatie op voorwaarde dat aan bepaalde voorwaarden voldaan werd. Wat de opslag betreft, is de serviceprovider ook niet aansprakelijk voor de informatie die bewaard wordt in het kader van zijn dienstverlening op voorwaarde dat aan bepaalde voorwaarden voldaan wordt (bijv. geen kennis van illegale informatie en prompte actie om illegale informatie te verwijderen als die ontdekt wordt).

Een ander problematisch domein met betrekking tot de richtlijn over elektronische handel zijn de meldings- en actieprocedures. De meldings- en actieprocedures verwijzen naar de opheffing of blokkering van de toegang tot de illegale informatie door een onlinebedrijf, nadat deze de vraag hiervoor gekregen heeft. Om te vermijden dat de onlinetussenpersoon aansprakelijk gesteld wordt, verplicht de richtlijn over elektronische handel de onlinetussenpersoon om actie te ondernemen zodra hij kennis neemt van de illegale handel. Actie ondernemen is mogelijk in de vorm van een demontage (de betwiste informatie schrappen) of een blokkering (de toegang tot de betwiste inhoud blokkeren).

De Commissie is van plan om de bezorgdheden van de verschillende betrokken partijen te analyseren. Deze gaan over het feit dat de wettelijke online informatie al lang bestaat en dat er een gebrek aan respect is voor de rechten van de auteurs of leveranciers van informatie. De analyse moet een antwoord geven op verschillende vragen: hoe moet een tussenpersoon precies ingelicht worden? Moet deze waarschuwing of kennisgeving elektronisch gegeven worden? Moet de kennisgeving een gedetailleerd internetadres bevatten? Moet een aanbieder van 'verdachte' informatie de mogelijkheid krijgen om gehoord te worden en uit te leggen waarom hij denkt dat de informatie niet illegaal is? Binnen welke periode moet een tussenpersoon reageren als de informatie effectief illegaal is? Is meer transparantie of publiciteit nodig op het vlak van meldings- of actieprocedures die individueel door personen of bedrijven ondernomen worden?

Een aantal van deze vragen hebben betrekking op de vaststelling van de geldige wetgeving (bv.: Waar bevindt zich de vestiging, het bedrijf?) of de toepassing van meldingsprocedures met betrekking tot de (vermeend) illegale informatie of de activiteiten van deze opkomende diensten (inclusief cloudcomputing). Deze vragen werden behandeld in de Mededeling over de digitale eenheidsmarkt voor elektronische handel en onlinediensten, in de aanpak van de Commissie betreffende de meldings- en actieprocedures[54].

54 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees en Economisch Sociaal Comite en het Comité van de regio's: 'Een coherent kader voor een groter vertrouwen in

6.2.4 Standaarden en certificering

Zoals vermeld in de Europese strategie over *cloud*computing[55] zullen een ruimer gebruik van de normen (standaarden), de certificering van de *cloud*services om aan te tonen dat ze voldoen aan deze normen en de validering van deze certificering door de regelgevende autoriteiten als bewijs van de naleving van de wettelijke verplichtingen bijdragen tot de verdere ontwikkeling van de *cloud*sector. De Europese Commissie heeft dus de intentie om Europese normen met betrekking tot *cloud*computing te introduceren en een lijst van betrouwbare *cloud*providers op te stellen.

Normen of standaarden

De normalisatie van de *cloud* zal ook de belanghebbenden buiten de informaticasector beïnvloeden, in het bijzonder de kmo's, de gebruikers uit de openbare sector en de consumenten. Vooral de kmo's zijn zelden in staat om de eisen van de providers op het vlak van de implementatie van standaarden, compatibiliteit van hun *cloud*services of het gemak waarmee de gegevens van één provider naar een andere verplaatst kunnen worden te evalueren. Daarom is een onafhankelijke en geloofwaardige certificering noodzakelijk.

Er werden al maatregelen genomen om *cloud*computing te standaardiseren. Het Amerikaanse National Institute for Standards and Technology (NIST) heeft een reeks documenten gepubliceerd, waarvan een reeks definities die grotendeels aanvaard zijn. Het Europees Instituut voor Telecommunicatienormen (ETSI) heeft een denktank opgericht over de noden en de conformiteit wat de normen voor compatibiliteit betreft. De eerste coördinatievergadering van het ETSI met betrekking tot de *cloud*normen heeft plaatsgevonden op 4-5 december 2012 in Cannes. Er werden drie onderwerpen behandeld:

- Normen met betrekking tot SLA;
- Normen met betrekking tot veiligheid;
- Normen met betrekking tot compatibiliteit, overdraagbaarheid van gegevens en reversibiliteit.

Zoals uitgelegd aan de studiegroep door de vertegenwoordigers van DG CONNECT werden de te behandelen onderwerpen vastgelegd, de resultaten hiervan zullen waarschijnlijk beschikbaar zijn voor de zomer van 2013. Het hoofddoel is niet nieuwe normen vastleggen maar de bestaande technische specificaties te bestuderen aangezien ETSI op dit vlak al veel werk verricht heeft. daar de oplijsting van de normen zich nog maar in de beginfase bevindt, werd er nog geen enkele beslissing genomen.
De Commissie zal echter haar werk voortzetten in samenwerking met ETSI, ENISA en andere competente organisaties om bij te dragen tot de ontwikkeling van Europese standaardiseringsprogramma's op het vlak van *cloud*computing (waaronder gegevensbescherming).

de digitale eengemaakte markt voor elektronische handel en onlinediensten', COM(2011) 942 definitief, 11.1.2012, p. 15
55 http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

Certificering

De certificering van de *cloud*providers is even belangrijk als het garanderen van de veiligheid. Deze beide aspecten zijn essentieel voor de ontwikkeling van *cloud*computing. De Europese Commissie plant echter geen invoering van specifieke certificeringen, wat haar voorzichtige benadering van deze materie illustreert (deels te verklaren door het risico van hoge kosten voor een dergelijke certificering). De Commissie is van mening dat deze beslissing door de *cloud*providers zelf genomen moet worden.

De Commissie onderzoekt echter het nut en de voordelen van een systeem van een Europees vertrouwenslabel – zie Actie 17 van de Digitale Agenda van Europa (Digital Agenda). Hier wordt samengewerkt met ENISA. Er bestaan verschillende symbolen of kwaliteitslabels zoals het "kleine httpsgele hangslot" wat veiligheid betreft of de labels aangaande toegankelijkheid van websites zoals gecreëerd door W3C. Men vindt dit onderwerp belangrijk want de invoering van garanties of functionaliteiten die door het label gesuggereerd en vertegenwoordigd worden, versterkt het vertrouwen in de dienstverlening van de actoren. Er zijn echter ook enkele negatieve aspecten aan certificering verbonden zoals de kosten die er mee gepaard gaan en de moeilijkheid om de verschillende vertrouwenslabels te herkennen. De Commissie heeft over dit onderwerp nog geen standpunt ingenomen maar zal dit binnenkort doen. Dit zal een belangrijke impact hebben op het algemene beleid in de sector van de *cloud*computing. Er moeten een aantal fundamentele problemen behandeld worden; één van de mogelijke oplossingen is deze taak aan een EU-agentschap toevertrouwen.

6.2.5 Het Europese Cloudpartnerschap

Het Europese Cloudpartnerschap (European Cloud Partnership of ECP) werd opgericht in het kader van de European Cloud Strategy en heeft als doel industrie en openbare sector samen te brengen teneinde een digitale eenheidsmarkt op te richten voor cloudcomputing in Europa.

De agenda van de ECP omvat:

1) Het werk van een recent gevormd directiecomité; dit bestaat uit vertegenwoordigers van de publieke sector en van de industrie. De bedoeling ervan is het geven van advies, samenwerking en stimulering voor de vorming van een markt voor *cloud*computing. Er wordt geen formeel standpunt ingenomen over de vraag of deze groep al dan niet uitgebreid wordt zal worden.

2) Voorbereidende activiteiten voor een overheidsopdracht: een aanbesteding voor de definitie van een *cloud*computing omgeving van hoge kwaliteit en voldoende aan de noden van de openbare sector werd gepubliceerd (procedure afgesloten op 15 januari 2013). De bedoeling hiervan is enerzijds de creatie van een forum voor de uitwisseling van ideeën en ervaringen tussen de lidstaten teneinde de beste *cloud*oplossingen voor de publieke sector te vinden. Daarnaast wil men de nationale ervaringen naar een Europees niveau brengen. Van dan af zullen de eerste samenwerkingen tussen lidstaten gestart kunnen worden; vervolgens kan

de privésector in de lidstaten er bij betrokken worden door middel van aanbestedingen.

Daar men deze omgeving kan verwijten dat ze nog heel vaag is, worden sommige blijven sommige lidstaten dromen van soevereine *cloud*services, hetzij om hun eigen dienstensecto te bevoordelen, hetzij om zich beter te beschermen tegen informatielekken (bijvoorbeeld in het typische geval van landen met een sterke traditie wat het bankgeheim betreft).

In haar strategische mededeling[56] heeft de Commissie duidelijk gesteld dat ze niet de leiding wil nemen in de creatie van een Europese super*cloud* voor de de openbare sector. Zij sluit niet uit dat een staat een privé*cloud* kan creëren voor de verwerking van gevoelige gegevens, maar dit moet een uitzondering blijven, waarbij mededinging op basis van een bestek omvattende de kwaliteitseisen geformuleerd door de openbare sector de regel blijft.mededinging.

De louter nationale initiatieven[57] worden in bedekte termen bekritiseerd want 'als men de openbare sector op deze manier fragmenteert, heeft de creatie specificaties (of bestekken) weinig impact, is de mate van integratie van de services laag en krijgen de burgers niet de beste waarde voor hun geld [58]'. De weg die men momenteel wil volgen, is dus die van mutualisatie ('pooling public requirements') in het kader van éénmalige of sectorale samenwerking (gezondheid, sociale hulpverlening, e-government services, open gegevens), tussen landen of ondernemers van diensten. Boveno de complexiteit om deze multipolaire akkoorden om 'samen te investeren' af te ronden (Welk budget? Wie neemt de leiding? Zal dit leiden tot partnerschappen die open staan voor nieuwe leden in het kader van een Europa met meerdere snelheden?)[59], is de eerste fase – die toekomt aan de ECP – deze gezamenlijke specificaties vastleggen.

6.2.6 Lopende studies met betrekking tot Cloudcomputing

Zoals aangekondigd tijdens de vergadering met de vertegenwoordigers van de Commissie spelen twee lopende studies over *cloud*computing een rol:

1) De studie over de initiatieven van de lidstaten met betrekking tot de implementatie van cloudcomputing (uitgevoerd door E-data). Zeven lidstaten zijn hier bij betrokken. Het einde van deze studie is voorzien voor juli 2013.
2) De studie (uitgevoerd door IDC) met als bedoeling een meer algemeen beeld te bekomen van wat nog te implementeren is op het gebied van cloudcomputing.

56 COM (2012) 529 « Unleashing the potential of Cloud Computing in Europe" – 27/9/2012 – p.6
57 Andromède in Frankrijk, G-Cloud in het Verenigd Koninkrijk, Trusted Cloud in Duitsland …
58 COM (2012) 529 – p. 13
59 Met de strategie '*Pooling open source software*' die door de Commissie uitgewerkt werd in 2002 hebben we kunnen vaststellen dat – ondanks de oprichting van OSOR.eu platformen (2008) en recenter Joinup.eu (2012), en ondanks de Ministeriële Verklaring van Manchester (2005) en Malmö (2009), de initiatieven ofwel communautair ofwel nationaal blijven en niet tot een intergouvernementele of interregionale mutualisatie geleid hebben.

7 Aanbevelingen

7.1.1 Aansluiten op de Europese benadering

De vooruitgang van de projecten volgen (niet proberen vooruit te lopen):

- Het algemene ontwerpreglement over gegevensbescherming (het project is nog niet definitief vastgelegd). Hier moeten in het bijzonder de inspanningen van sommige lobbyisten gevolgd worden. Deze gebruiken verschillende hefbomen, in het bijzonder bepaalde Europarlementsleden, om de inhoud ervan te wijzigen of te versoepelen)[60] ;
- De rechten van de consument die kopieën van aan beperkingen krachtens het auteursrecht onderworpen werken aan de cloud wil toevertrouwen;
- De evolutie van de richtlijn over de elektronische handel;
- De technische standaarden die door ETSI of ENISA aanbevolen of opgelegd zullen worden;
- De deelname aan het 'Europese Cloudpartnerschap'.

In al deze domeinen komt het er op aan te vermijden op een overhaaste of geïsoleerde manier wetten te creëren, maar moet er een technologisch en juridisch bewakingsmechanisme komen teneinde te anticiperen op komende hervormingen en om relevante adviezen te kunnen formuleren.
Deze kennisverwerving moet de publieke autoriteiten toelaten een actievere en meer zichtbare rol in het ECP te spelen.

Als alternatief wordt aanbevolen te werken aan de bevordering van goede praktijken als voorbereiding van de inwerkingtreding van de hervormingen.

Het voordeel van deze 'goede praktijken' is dat zij vastgelegd kunnen worden in werkdocumenten, waarvan de opeenvolgende versies de actualiteit kunnen volgen (versie 1.0 – 2013; versie 1.2 – 2014 enz.) en die de belanghebbenden toelaten hun conformiteit met een welbepaald niveau van deze 'goede praktijken' kenbaar te maken, zonder dat hier strikte en dure certificeringsprocedures opgestart moeten worden.

Wat de noden van de openbare sector betreft, een sterk geregionaliseerd land zoals België zou zich niet moeten concentreren op een op de constructie van een 'soevereine *cloud'*. Dit zou neerkomen op het opnieuw invoeren van economische grenzen (nationaal of regionaal). Integendeel, men moet aandacht hebben voor de mogelijkheden tot open samenwerking (nieuwe banden) met de buurlanden. Vooral de mutualisatie van sommige aanbestedingen (wanneer het bestek van de 'publieke *cloud'* zal vastgelegd zijn in het

60 Zie over dit onderwerp de aanklacht door schrijver Glynn Moody over de voorstellen tot wetswijzigingen ingediend door Europarlementsleden, die woord voor woord de wensen van sommige buitenlandse bedrijven reproduceren: 'EU Data Protection: Proposed Amendments Written by US Lobbyists' in : *http://blogs.computerworlduk.com/open-enterprise/2013/02/eu-data-protection-proposed-amendments-written-by-us-lobbyists/index.htm*.

kader van het Europese partnerschap) en het delen van resources in open modus (hoofdzakelijk softwaretoepassingen speciaal ontwikkeld door of voor de openbare sector, in verschillende lidstaten, in 'open source' modus en volgens open standaarden en vrij van rechten) zijn twee benaderingen waaraan de voorkeur gegeven moet worden, in samenwerking met de Federale Overheidsdienst voor Informatie- en Communicatietechnologie (FEDICT).

7.1.2 De dialoog met en tussen de economische actoren versterken

De eerste stappen om een 'Belgian Cloud' groep te vormen werden inmiddels gezet. De meeste leden van deze groep zijn momenteel actief in 'BELTUG', een vzw die de grootste representatieve organisatie voor ICT-managers wil zijn, met bijzondere aandacht voor netwerken tussen bedrijven, mobiele communicatie, groepen die streven naar de verbetering van de software (Software Improvement Group) voor de eenvormig gemaakte communicatie en de *cloud*.

Het uitbouwen en economisch aantrekkelijker maken van de cloudcomputing in België zullen er niet komen als gevolg van een unilateraal overheidsvoorschrift maar als door onderzoek naar de beste praktijken en verbetering van de veiligheid, samen met de betrokken actoren. Hier moet een dialoog opgestart worden -al dan niet binnen Beltug- tussen de overheid en de professionals van deze sector, met als doel een hogere aantrekkelijkheid van de sector en een verhoogd marktvertrouwen.

Een specifieke organisatie van het beroep van cloud-provider zou nuttig zijn, zodat de providers een referentierol kunnen spelen voor een goed beheer van ICT, zowel voor de bedrijven en als voor de overheidsdiensten. Hierdoor kan deze gesprekspartner worden in het kader zowel nationale als Europese initiatieven. De regionale en taalstructuur van België kan hierbij echter een belemmering vormen. Dit aspect vraag verdient nader bestudeerd worden.

7.1.3 Contracten

Rekening houdend met de reeds vastgelegde goede praktijken, zoals beschikking 2002/16/CE van de Commissie van 27 december 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar in derde landen gevestigde verwerkers krachtens richtlijn 95/46/EG[61], rekening houdend met de BCR (Binding Corporate Rules[62]) die beschouwd worden als voldoende garantie voor de bescherming van gegevens dankzij bindende bedrijfsvoorschriften, en rekening houdend met de vaststellingen in dit rapport en de bij dit rapport opgenomenn checklist (zie sectie 8), zou het nuttig zijn om, in overleg met de vertegenwoordigers van de sector, één of meerdere typecontracten die overeenkomen met de belangrijkste servicemodellen op te stellen. Deze contracten zouden de aanbevelingen van de werkgroep 'Artikel 29' kunnen overnemen (zie de lijst van contractuele clausules onder 6.2.1) en op deze wijze

61 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:FR:PDF
62 Een BCR is een regel die opgesteld werd door een multinational (bijv. een interne gedragscode), die bindend is voor alle entiteiten en medewerkers, en die betrekking heeft op de internationale transfers van persoonlijke gegevens die binnen de groep uitgevoerd worden.
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

vooruitlopen op (en rekening houden met) de strekking van het algemene ontwerpreglement voor gegevensbescherming. Aldus kunnen ze dienen als kwaliteitsstandaard en referentie, waarbij het vertrouwen van de bedrijven en de overheid versterkt worden.

In de mate waarin de investeringen beperkt blijven en het bovenstaande overgenomen en goedgekeurd kan worden door onze Europese partners, kan de – vrijwillige – instemming met deze contractuele specificaties beloond worden door de toekenning van een '**Fair Cloud**' label (te ontwerpen) en door de publicatie door de regelgevende overheid van een lijst van de aanbieders die deze specificaties opvolgen. De publiciteit die dit label krijgt, zal het vertrouwen en de aantrekkelijkheid van de markt versterken.

7.1.4 Informatie voor het publiek

Publicatie van een praktische gids

Sommige landen[63] hebben kleine praktische gidsen gepubliceerd voor bedrijven en burgers. Een dergelijk document mag niet lang zijn (maximaal 20 pagina's) en moet gemakkelijk lezen.

De gids moet het volgende bevatten:

- een overzicht van de cloud: begrippen, toepassings- en servicemodellen;
- een definitie van de rollen en bijbehorende verantwoordelijkheden;
- praktische aanbevelingen over de keuze van een provider (hoe een provider kiezen en evalueren, contractvoorwaarden);
- welke interne regels moet de klant volgen en welke basisopleiding hij moet gevolgd hebben om de controle en leiding te behouden;
- een checklist (zie verder);
- praktische illustraties die gebaseerd zijn op de dagelijkse realiteit;
- een lijst 'wie doet wat?' voor de kandidaat-gebruiker met contactpunten bij de vertegenwoordigers van het beroep en de overheid, vooral indien deze een begeleidende, controlerende of verzoenende rol kan garanderen.

Het is raadzaam een voorbeeld te nemen aan wat er al bestaat en een dergelijke gids te publiceren, in ten minste de drie landstalen en het Engels zodat deze gids kan dienen als 'visitekaartje' voor de *cloud* in België, en dit voor bedrijven, overheidsinstellingen en potentiële klanten in België en in het buitenland.

63 Zie: UK – (Information Commissioner's Office) Guidance on the Use of Cloud Computing – 2 October 2012; Ireland – NSAI Standards, SWiFT 10:2012 Adopting the Cloud – decision support for cloud computing; Slovenia – Information Commissioner and Cloud security alliance, Slovenia chapter – Personal data protection and cloud computing (15 juni 2012)

Hoe kan de gids met praktische voorbeelden geïllustreerd worden?

Voorbeeld:
Een school overweegt haar onderwijsmethodes te moderniseren door 'informaticaklassen' op te richten waarbij iedereen een eigen werkplaats heeft.

Normaal zou dit de aankoop van een pc per leerling impliceren (en de betaling van licenties, beheer van de veiligheid, antivirussoftware, internettoegang, downloaden en uploaden op initiatief van de leerlingen, onderhoud dergelijke voor iedere pc).

Door echter te kiezen voor de toegang tot een gespecialiseerde *cloud*oplossing (SaaS) vermijdt de school al deze problemen en de werkposten (bijvoorbeeld tablets) worden uitsluitend binnen het voorziene kader gebruikt.
Met deze oplossing krijgen de leerlingen overal toegang tot hun opdrachten (school, thuis) en kunnen hun prestaties optimaal opgevolgd worden (resultaten).

De school die de dienst aanbiedt is de klant van de *cloud*. De school is ook de 'verantwoordelijke voor de verwerking' die de voorziening van een gegevensbeschermingssysteem moet vragen (namen, toegang tot de beoordelingen van leerkrachten).

De *cloud*provider is de 'verwerker' van de gegevens (de onderaannemer volgens de wet), maar als professional moet hij de school adviseren en een toepassing aanbieden die beantwoordt aan de verwachte veiligheidsnormen (toegangscontrole, identiteitscontrole, coder) en ervoor zorgen dat het service level agreement de opslagplaatsen, de beschikbaarheid van de service, de procedures met betrekking tot aanpassing en verwijdering van de gegevens enz. preciseert en de vermelding bevat dat de gegevens niet voor commerciële doeleinden gebruikt mogen worden.

De leerling is de 'betrokkene'. Hij/zij heeft recht op informatie over de gegevens die op hem/haar betrekking hebben en heeft het recht om de wijziging van de gegevens in geval van fouten te vragen.

Publicatie van een checklist

Het idee om een 'checklist' over cloudcomputing te publiceren werd bijzonder goed onthaald op de vergadering van 27 februari 2013 met de cloudoperatoren.

De checklist kan onderwerpen bevatten met betrekking tot:

- De klant (die zichzelf moet kennen, weten of hij gegevens met een persoonlijk karakter behandelt, zijn behoeften en eisen op het vlak van verkeer, continuïteit, support enz. kennen);
- De cloudprovider;
- De contractuele verhouding tussen de klant en de provider.

Een voorbeeld van checklist vindt u in sectie 8.

7.1.5 Veiligheid

Het doorslaggevende karakter van de cloudinfrastructuur moet de overheid ertoe aanzetten om:

1) Op het terrein een praktische en realistische risico-evaluatie te houden van de elementen die een bedreiging voor de *cloud* vormen (zoals ze in deel 4 van dit rapport beschreven worden) en deze te rangschikken naar prioriteit en dit meerbepaald voor de IaaS en PaaS-services die op ons grondgebied geïmplementeerd zijn.
   Om te vermijden dat de aandacht te veel versnipperd wordt, moet men zich eerst concentreren op de services waarvan de onbeschikbaarheid een impact kan hebben op talloze andere organisaties:
   - Deze grote infrastructuren of platformen identificeren op basis van hun belang voor het behoud van de economische activiteit en deze fysieke en logische afhankelijkheid in kaart brengen;
   - Analyseren wat kritisch is voor de goede werking van deze infrastructuren, niet alleen op gebied van hun fysieke bescherming maar ook voor hun energievoorziening, hun afkoeling, hun toegang tot de communicatienetwerken.
   -

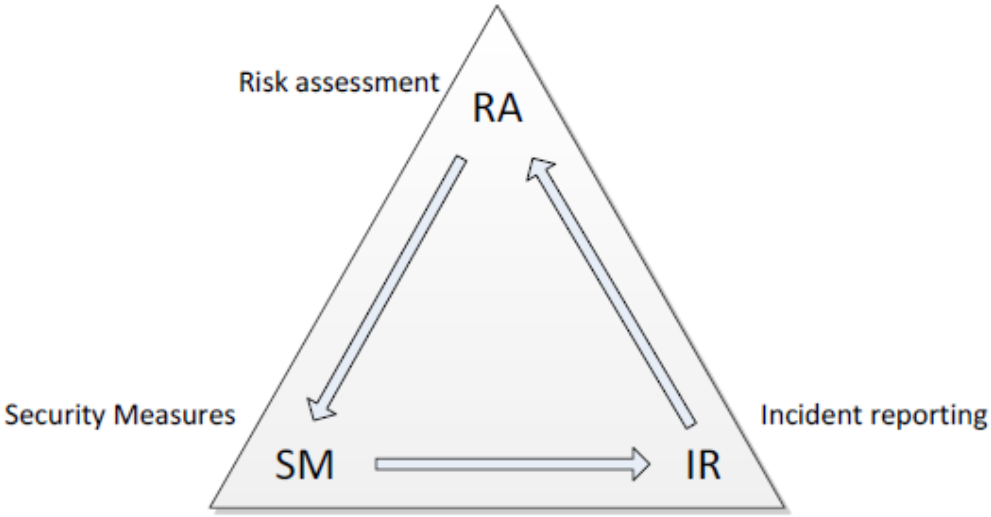
2) De aanbevolen veiligheidsmaatregelen te identificeren en te laten toepassen (waarbij gecontroleerd moet worden of ze effectief toegepast worden) om incidenten te voorkomen of op zijn minst hun impact te beperken. In het bijzonder vermijden dat er, in welke schakel dan ook van de productieketting, zwakke plekken (single points of failure) zijn en dat er voldoende redundantie is om uitvallen van een element uit het systeem door andere te compenseren.
   Ongeacht of dit nu wel of niet in het kader van een certificering gebeurt, is het bijzonder aan te bevelen regelmatige audits aan te bevelen en te eisen, bij voorkeur uitgevoerd door een onafhankelijk organisme. Deze moeten toevertrouwd worden aan professionals die van dichtbij de risico-evolutie volgen. In het snel evoluerende domein van de veiligheid moet men in plaats van te kiezen voor een 'automatische' periodiciteit (bijvoorbeeld jaarlijks) de actoren van de *cloud* uitnodigen om zich te richten naar de voorschriften en een controle uit te oefenen 'zodra nodig' als blijkt dat een maatregel zich opdringt. In dit verband zou de overheid, in samenwerking met de vertegenwoordigers van de sector, een observatiegroep moeten oprichten om te onderzoeken welke maatregelen aan te bevelen -of eventueel op te leggen- en binnen welke limieten dit moet gebeuren (in functie van het belang van de service).

3) Een systematische rapportering organiseren over alle incidenten die zich voorgedaan hebben hetzij op veiligheidsvlak, hetzij op het vlak van serviceonderbreking (boven een vast te stellen limiet), teneinde de risico-evaluatie te valideren. Voor elk incident dat betrekking heeft op veiligheid moet bijzondere aandacht besteed worden aan de informatie-uitwisseling tussen de verschillende betrokken autoriteiten of regeringen; hierbij kan gebruik gemaakt worden van de hiervoor door de Europese Unie ontwikkeld instrumenten (zoals CIWIN). De rol van de overheid bestaat er in de

uitwisseling van informatie tussen alle belanghebbenden te bevorderen om de gepaste maatregelen zo snel mogelijk toe te passen (binnen een snel evoluerende technologie).
In samenwerking met de vertegenwoordigers van het beroep dient vastgelegd te worden vanaf wanneer en binnen welke limiet een incident verplicht gemeld moet worden.
Als een incident aanleiding kan geven tot vervolgingen of sancties moet ervoor gezorgd worden dat de vrijwillige melding van een incident de verantwoordelijkheid van de aangever sterk vermindert of zelfs teniet doet (om zijn minst voor wat een strafrechtelijke sanctie betreft, op dezelfde wijze als bedrijven die een kartel of concurrentievervalsing aan de Europese autoriteit signaleren aan sancties kunnen ontsnappen).

4) De bekomen informatie (zie vorige sectie) gebruiken om de bedrijven en het publiek te laten weten dat een bijzondere inspanning geleverd wordt om de veiligheid van de *cloud* te verbeteren. Hierbij de nadruk leggen op de systematische verzameling van de incidentenrapporten, de analyse van de risico's en genomen maatregelen om deze risico's te voorkomen en de gevolgen van de problemen te beperken.

In het geval deze 'beheersdriehoek' toegepast wordt door een professionele organisatie moet de regulerende instantie (overheid) haar controlerende rol opnemen. Hierbijj dienst ze op de hoogte te zijn van alle rapporten, van ieder evenement dat zich voordoet en van de opvolging van de genomen maatregelen.



Afbeelding 11 – De risico-evaluatie (RA), de invoering van maatregelen (SM) en de raportering van incidenten (IR) (bron: Rapport ENISA, december 2012)

Wat bedoelt men precies met controleorgaan? Volgens de aanbevelingen van ENISA uit 2012 zijn dit de organisaties die verantwoordelijk zijn voor de opstelling en het onderhoud van de nationale programma's voor risicobeperking

('Agencies responsible for establishing and maintaining national contingency plans')[64]. Voor zover de *cloud*services erkend zijn als kritisch, dit wil zeggen 'installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken' kan gebruik gemaakt worden van de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken (ADCC). De wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren heeft dit organisme aangeduid om de plaatsing van deze beveiligingen en het werk van de betrokken actoren te analyseren en te controleren en de in deze wet voorziene maatregelen te doen gelden.

[64] ENISA, Critical Cloud Computing – a CIIP perspective on cloud computing services – December 2012 [Online] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing, p. 23

8 Checklist

Een van de best onthaalde aanbevelingen (tijdens de vergadering met de spelers van de *cloud*) was de publicatie van een “checklist” die de klant van de *cloud* zou helpen zijn eigen behoeften te definiëren om een goed geïnformeerde keuze van zijn provider te kunnen maken.

Hieronder formuleren we een voorontwerp:

Uw positie (als **verantwoordelijke voor de verwerking** volgens de WPL) als “Klant” van de *Cloud* (Intern onderzoek)	Welke commerciële of economische voordelen verwacht u van de *cloud*? - Hebt u het voorgestelde economische model goed begrepen? - Hebt u de operationele kosten afgewogen ten opzichte van de kapitaalinvesteringen (bv. op 5 jaar)? - Hebt u nagedacht over de nodige bandbreedte en de kostprijs daarvan?	
	Welke andere voordelen verwacht u van de *cloud*? Wat is de verwachte impact op: - Uw organisatie (organigram, rollen) - Uw kennisniveau (opleidingen) - Uw processen - Uw onderhoudsmogelijkheden	
	Hoe ziet u de evolutie van uw “IT-verbruik” voor de komende vijf jaar, al naargelang deze groei intern of extern gebeurt (middelen voor de *cloud*)?	
	Bevatten uw gegevens persoonsgegevens (eender welke informatie, zelfs een eenvoudig nummer dat op unieke wijze een geïdentificeerde of identificeerbare persoon kan aanduiden en eraan gekoppeld kan worden)? Zo ja, houdt u daar dan zorgvuldig een lijst van bij?	WPL 1, §1
	Beschikt u, in uw hoedanigheid van “controleur” van deze gegevens (of “**verantwoordelijke voor de verwerking** van persoonsgegevens” volgens de WPL) en toekomstige “klant” van een *clouddienst*, over de nodige wettelijke basis om deze gegevens te verwerken?	WPL 4 & 5
	Hebt u gecontroleerd dat u geen “verboden” of beperkte gegevens hebt (ras, opinies, gezondheid enz.) of dat u in dergelijk geval onder een van de uitzonderingen voorzien in de wet valt?	WPL 6, 7 & 8

	Hebt u bepaald welke gegevens (inclusief de gegevens hierboven) waarop u controle uitoefent en waarvoor u dus verantwoordelijk bent voor de verwerking, in de *cloud* behandeld zullen worden?	
	Hebt u gecontroleerd dat geen enkele (bv. contractuele) bepaling de verwerking van deze gegevens beperkt (indien ze betrekking hebben op uw eigen klanten, op uw leden, enz.)?	
Uw provider	Hoe lang is uw provider reeds actief in het domein van de *cloud*? Kan hij een lijst met referenties overhandigen? Hebt u toegang tot zijn gepubliceerde rekeningen (of tot een economische audit die op hem betrekking heeft)?	
	Is uw provider gedekt door een verzekering die ook uw gegevens en het verlies aan omzet in geval van onbeschikbaarheid dekt? Is er desgevallend een “escrow”-regeling of equivalent die garandeert dat u uw gegevens kunt terugkrijgen?	
	Is uw provider (of de groep waarvan hij deel uitmaakt, met inbegrip van de datacenters en verwerkers) exclusief gevestigd op het grondgebied van de Europese Economische Ruimte (Europese Unie, Noorwegen, IJsland, Liechtenstein)?	
	Als uw provider vestigingen heeft of datacenters gebruikt in landen buiten de EER, zijn die landen dan opgenomen in de lijst van de Europese Commissie met “landen die een passend beschermingsniveau voor gegevens bieden”?	
	Als uw provider vestigingen heeft of datacenters gebruikt buiten de EER (voornamelijk in de Verenigde Staten van Amerika), is hij dan globaal gecertificeerd als instelling die de principes in het “Safe Harbour”-akkoord toepast?	
	Heeft uw provider u een dienstcontract voorgesteld (wat verplicht is voor persoonsgegevens), dat zijn verantwoordelijkheid definieert en de waarborgen vermeldt die hij biedt op het vlak van veiligheid en organisatie?	WPL 16 §1, 1°-4°
	Is het contract met de provider van de *cloud* schriftelijk (wat verplicht is voor persoonsgegevens)? Onder schriftelijk kunnen we ook in elektronische vorm verstaan.	WPL 16 §1, 2° & 5°
	Als er persoonsgegevens zijn, wordt dan expliciet in het contract vermeld dat de provider van de *cloud* er ten opzichte van u verantwoordelijk voor is, en aanvaardt hij dezelfde verplichtingen die u (verantwoordelijke voor de verwerking) ook moet naleven?	WPL 16 §1, 5°
	Heeft uw provider van de *cloud* zijn veiligheid laten auditeren door een onafhankelijk expert, en hebt u de conclusies van dat rapport ontvangen?	

	Voldoen de ingevoerde maatregelen na dit rapport aan (of overtreffen ze) het bestek of een kwaliteitsnorm die u als geschikt beschouwt voor uw activiteitssector?	
De bepalingen in uw contract	Binnen welke termijn verbindt de provider zich ertoe u te informeren in het geval dat hij een veiligheidsprobleem vaststelt bij de diensten of producten die hij voorstelt?	
	Hoe kunt u de aanmaak van nieuwe gebruikersaccounts beheren? Wat zijn de operationele termijnen (en de eventuele kosten) voor de creatie, opschorting, verwijdering van een account?	
	Versleuteling: Is het gegarandeerd dat de gegevens versleuteld worden in geval van een overdracht binnen de *cloud* (bijvoorbeeld tussen twee verwerkingscentra die geografisch gezien uit elkaar liggen)? Is het gegarandeerd (indien nodig, voor persoonsgegevens) dat gegevens versleuteld zijn wanneer ze “in rust” zijn op de voorgestelde *cloudserver*? Is er een beheerssysteem (generatie/behoud) voor de versleutelingscodes ingevoerd?	
	Als u de definitieve vernietiging van sommige registraties of gegevens vraagt, garandeert uw provider u dan de effectieve vernietiging (overschrijving/reset) van alle kopieën of versies die op de cloud bewaard zouden kunnen zijn? Wat is de termijn voor deze vernietiging?	
	Als u besluit een einde te maken aan de *clouddiensten*, garandeert uw provider u dan de effectieve vernietiging (overschrijving/reset) van alle kopieën of versies van de gegevens die op de cloud bewaard zouden kunnen zijn?	
	Hebt u alle gevallen geïdentificeerd waarbij uw gegevens (inclusief informatie over uw gebruikers) al dan niet zouden kunnen worden gedeeld met of overhandigd aan andere partijen (relaties, “vrienden” enz.) of gebruikt in het kader van andere diensten die de provider van de *cloud* zou kunnen aanbieden (bv. commerciële aanbiedingen, e-mailing)?	
	Voorziet de provider een manier om u te informeren wanneer iemand toegang heeft tot uw gegevens? Kunt u een lijst ontvangen die vermeldt wie tot welke gegevens toegang heeft gekregen en wanneer?	
	Garandeert de provider u dat hij op aanvraag en zonder voorwaarden een kopie van uw gegevens kan verkrijgen, in een bruikbaar formaat (conform met een open norm, vrij van rechten, wijd verspreid en goed gedocumenteerd) voor de eventuele overdracht van deze gegevens naar een andere provider?	
	In geval van een storing of een onvoorziene vernietiging (bv. een kapotte schijf), wat is dan de	

	gegarandeerde termijn voor een herstart/een herstel zonder wijzigingen vanaf een back-upkopie?	
	Kan de provider garanderen dat zijn dienst voldoende capaciteit biedt om uw dienstkwaliteit te garanderen in geval van “verbruikspieken” veroorzaakt door andere gebruikers?	
	In welke mate kunnen de handelingen van de andere gebruikers de kwaliteit van de aan u geleverde diensten verstoren?	
	Is er een engagement van de provider om u permanent de toegang tot zijn dienst of uw gegevens te verzekeren? Wat is de tolerantie (maximale tolereerbare onderbreking), rekening houdend met uw activiteit?	
	Hebt u een raming gemaakt van de materiaalkosten (randapparatuur, routers) en verbindingen (abonnementen) voor al uw gebruikers wanneer ze de clouddiensten zullen gebruiken 1) vanaf hun gebruikelijke bureau 2) buiten hun gebruikelijke bureau (thuis of op reis)?	
	Zijn de rechten en plichten van de partijen (uw provider en uzelf) in detail beschreven in een schriftelijke overeenkomst? (een serviceniveauovereenkomst of SLA: “service level agreement”)	
	Heeft uw provider zich ertoe verbonden elke wijziging door te geven (in zijn voorwaarden, zijn werking, zijn infrastructuur, zijn diensten) die een invloed zou kunnen hebben op de uitvoering van uw contract met hem?	
	Beperkt het contract de lijst met landen waarin uw gegevens mogen worden doorgegeven, opgeslagen of verwerkt (bv. enkel de landen van de Europese Unie, of de Europese Economische Ruimte)?	
	Zo niet, bieden de landen waarin uw gegevens mogen worden doorgegeven voldoende garanties volgens de Europese Commissie, dat wil zeggen, gaat het om: Canada, Zwitserland, Argentinië, Guernsey, eiland Man, Faeröer-eilanden, Jersey of Israël? (Voor de Verenigde Staten, zie hieronder)	
	Als de Verenigde Staten deel uitmaken van de landen waarin gegevens mogen worden overgedragen, hebben alle geadresseerden (*cloud*-verwerkingscentra, filialen of aannemers) formeel de principes van het “Safe Harbour”-akkoord tussen de EU en de VS onderschreven?	
	Als de provider van de *cloud* van plan is een infrastructuur te gebruiken die over andere landen verspreid is (landen buiten de EU/EER en de landen die een passend beschermingsniveau bieden), wat zijn dan de garanties inzake de bescherming van deze gegevens, en werden deze garanties – onder de vorm van een contract of een modelcontract – toegestaan door een	

	koninklijk besluit na een advies van de Commissie voor de bescherming van de persoonlijke levenssfeer?	
	Kan de provider in een document vastleggen in welke omstandigheden en waarom uw gegevens naar andere landen zouden kunnen worden overgedragen?	
	Hebt u in het algemeen de mogelijkheid om u op voorhand te verzetten tegen een gegevensoverdracht of deze te beperken tot de landen die u geschikt acht?	

9 Modelcontractbepalingen

Het is vrij moeilijk om een modelcontract op te stellen, aangezien de situaties, verwachtingen van klanten, hun eigen activiteitenmodellen en de prijs die ze bereid zijn te betalen voor deze dienst (OPEX vs. CAPEX) zo sterk kunnen verschillen. Bij gebrek aan een gestandaardiseerd "publiek" modelaanbod, d.w.z. een aanbod dat beperkt is tot zeer precieze functies, kunnen deze prijskwesties, net als vele andere punten in verband met de provider (zijn andere klanten, met inbegrip van contracten afgesloten "tot tevredenheid van beide partijen"), de details van de aangeboden diensten en functies, de groeicapaciteit van de diensten (over x jaar) slechts geregeld worden in de lijst met te controleren punten (checklist), een geïndividualiseerde SLA of in bijlagen van het contract.

De onderstaande ideeën voor bepalingen zouden echter, na een akkoord met een groep die representatief is voor het vakgebied, kunnen worden aangenomen als voorbeeld voor een "**Fair Cloud**"-label.

Benaming	Bepaling	Opmerking
Definities	De klant van de cloud is de persoon die op de provider van de cloud een beroep doet om, op afstand, op aanvraag en via een telecommunicatienetwerk, gebruik te maken van IT-middelen waarmee hij zijn activiteit kan uitoefenen en zijn gegevens kan verwerken. De provider van de cloud is de persoon die aan de klant, gratis of tegen betaling, een infrastructuur (capaciteit), een operationeel platform en/of applicaties aanbiedt waarmee de klant zijn gegevens kan uploaden, verwerken of bewaren.	Behoefte aan definities van rollen die kunnen worden gekoppeld aan de toepasbare wetgeving
Verwachtingen van de klant en serviceniveau	De aard van de diensten, de specifieke verzoeken van de klant en het verwachte serviceniveau worden op objectieve en meetbare wijze gespecificeerd in bijlage 1. Er worden boetes voorzien om de schade te compenseren in het geval dat de provider het verwachte serviceniveau niet zou halen. Deze boetes worden op objectieve en meetbare wijze vastgelegd in bijlage 2.	
Duur van de diensten	De duur van de dienst (gedekte periode) en de mogelijkheid om de diensten te verlengen of te beëindigen worden vastgelegd in bijlage 3.	
Continuïteit van de activiteiten/Serviceniveau-overeenkomst	De provider garandeert een beschikbaarheid van de dienst van __ % en een herstart bij een onderbreking na een incident binnen een maximumtermijn van __ uur, vastgelegd in de serviceniveauovereenkomst.	
Professionele verzekering	Naast de forfaitaire boetes indien het kwaliteitsniveau niet wordt nageleefd, heeft de provider een professionele verzekering afgesloten om de reële directe en indirecte	

	door de klant geleden schade te vergoeden (in geval van een onderbreking van de activiteiten, verlies aan omzet, schade aan het imago, enz.). Dit bedrag is per schadegeval geplafonneerd tot X.	
Aard van de behandelde gegevens (1)	In het geval dat het om persoonsgegevens gaat (in de zin van richtlijn 95/46 EG) verklaart de klant dat hij – in zijn hoedanigheid van "verantwoordelijke voor de verwerking" – in de wettelijke omstandigheden verkeert om ze te laden en te verwerken.	Koppeling met geldende wetgeving
Aard van de behandelde gegevens (2)	In bijlage 4 vermeldt de klant of de gegevens die hij op de cloud plaatst "persoonsgegevens" zijn en beschrijft hij kort welke de gegevens zijn en wat de bedoeling van de verwerking is. Bij gebrek aan deze formele verklaring, en als de provider zich er niet toe heeft verbonden ALLE gegevens van de klant te behandelen ALSOF het om persoonsgegevens ging, heeft de provider het recht ervan uit te gaan dat deze gegevens geen persoonsgegevens zijn.	Eenvoudige of versterkte bescherming
Aard van de behandelde gegevens (3)	In het geval dat de provider ermee instemt om persoonsgegevens op te slaan, of als hij zich ertoe heeft verbonden alle gegevens van de klant te behandelen alsof het om personeelsgegevens ging, aanvaardt de provider de verantwoordelijkheid van de Verwerker in de zin van richtlijn 95/46/EG. Bovendien, voor elke behandeling die hij uitvoert of waarvoor hij het initiatief zou nemen (opslag, overdracht, export, bewaring), stemt de provider in met de verplichtingen van de Verantwoordelijke voor de verwerking in de zin van richtlijn 95/46/EG.	Koppeling met geldende wetgeving
Vertrouwelijkheid	Ongeacht de aard van de gegevens, verbindt de provider zich ertoe de vertrouwelijkheid van de gegevens strikt na te leven. Ten opzichte van de klant is hij rechtstreeks verantwoordelijk voor de handelingen van al zijn medewerkers en van de eventuele verwerkers aan wie hij de gegevens zou toevertrouwen.	
Niet-communicatie aan derden	Tenzij het contract of de bijlagen expliciet melding maken van de mogelijkheid om diensten uit te besteden, of van een "betrouwbare derde" (Escrow), verbindt de provider zich ertoe de gegevens niet aan derden door te geven, ook niet gewoon om ze op te slaan.	
Plaats van verwerking en bewaring	De provider verklaart dat als gegevens van de klant door hem worden verwerkt (of worden overgedragen, bijgehouden of opgeslagen), dat deze gegevens gelokaliseerd zullen blijven in en hun behandeling onderworpen zal zijn aan de reglementering van: A) De volgende landen: ……* B) De lidstaten van de Europese Unie en andere landen van de Europese Economische Ruimte (EER).	Koppeling met geldende wetgeving

	C) De landen van de EU, de EER en andere landen in de lijst van de Europese Commissie met landen die een passend beschermingsniveau voor gegevens bieden. D) De landen onder C) en de Verenigde Staten van Amerika (VS), waarbij ervan wordt uitgegaan dat de provider en al zijn vestigingen, verwerkers of tussenpersonen gevestigd in dat land en die technisch gezien toegang zouden kunnen hebben tot de gegevens, zich op geldige wijze hebben onderworpen aan de regels van de "Safe Harbor"-overeenkomst tussen de EU en de VS. (*) kiezen en/of invullen wat van toepassing is	
Formaat van de gegevens	In het geval dat hij een platform en/of applicaties levert, garandeert de provider dat de gegevens worden bewaard in een open standaardformaat (op heldere en transparante wijze gedocumenteerd) dat vrij is van gebruiksrechten, in die zin dat ze vrij kunnen worden geëxploiteerd of herladen door de klant of door een andere provider die over de vereiste standaardinstallaties beschikt (bijvoorbeeld aan het einde van het contract of op vraag van de klant).	Garantie van overdraagbaarheid
Verzekering voor teruggave van de gegevens	Aan het einde van het contract of op verzoek van de klant, verbindt de provider zich ertoe alle gegevens terug te geven aan de klant, in het hierboven vermelde open, gedocumenteerde standaardformaat vrij van gebruiksrechten, en dat gratis of tegen een kostprijs die de materiële kosten voor de realisatie van de kopie en/of de overdracht aan de klant niet overschrijdt. Het einde van het contract en elk geschil tussen de klant en de provider (bijvoorbeeld na de niet-betaling van facturen) kan aanleiding geven tot de opschorting of de onderbreking van de diensten en tot een minnelijke, arbitraire of gerechtelijke schikking, maar in geen geval mag de provider de gegevens bijhouden.	Garantie van overdraagbaarheid
Back-up and Recovery	De provider biedt aan de klant de in bijlage 5 beschreven opties aan voor de - back-up - redundantie - recuperatie na een ongeval.	
ESCROW (optie)	Om de beschikbaarheid van de gegevens van de klant te verzekeren zal de provider regelmatig een kopie ervan afgeven aan een "betrouwbare derde". De klant zal de derde kennen en de toestemming hebben om zijn kopie bij hem op te vragen, gratis of tegen een kostprijs die de materiële kosten voor de realisatie van de kopie en/of de overdracht aan de klant niet overschrijdt.	
Vernietiging van de gegevens	Aan het einde van het contract en na de teruggave aan de klant van de laatste kopie van zijn gegevens garandeert de provider – tenzij de klant hier met een formele	

	instructie anders over beslist – dat de gegevens van de klant en alle kopieën effectief vernietigd zullen worden door een reset of een fysieke vernietiging van de dragers, zo snel mogelijk en na een maximumtermijn van 1 maand.	
Veiligheid	De provider verbindt zich tot veiligheidsmaatregelen, en heeft in het bijzonder de nodige maatregelen getroffen om: - Zijn installaties fysiek te beschermen tegen ongeoorloofde toegang; - Zijn installaties op logische wijze te beschermen tegen ongeoorloofde toegang; - Zijn middelen op evenwichtige wijze te verdelen tussen zijn klanten; - Zijn infrastructuren, platformen en/of applicaties op het meest recente geschikte veiligheidsniveau te brengen, binnen de door de ontwerpers aanbevolen termijn; - Een wederzijdse authenticatie in te voeren tussen zijn diensten en de gebruikers van zijn klant en aldus de identiteiten en toegang te beheren; - Een opslagmiddel in te voeren (beschreven in bijlage 5); - Een middel voor de versleuteling van de gegevens in te voeren (beschreven in bijlage 6); - De toegang tot de persoonsgegevens te kunnen traceren (beschreven in bijlage 7); - Een waarschuwingssysteem en een systeem voor de detectie van incidenten in te voeren; - De incidenten die zich voordoen te registreren en te documenteren, en ze desgevallend mee te delen volgens de procedures die werden ingevoerd door een controleautoriteit; - Over te gaan tot een specifieke en gedetailleerde evaluatie, per prioriteit, van de risico's met betrekking tot deze diensten; - De nodige maatregelen in te voeren om deze risico's te dekken, volgens hun prioriteit; - Zijn evaluatie en de getroffen maatregelen te laten auditeren door een onafhankelijke specialist.	Het is moeilijk om te verwijzen naar precieze standaarden (tal van normen, die steeds evolueren), maar men kan verwijzen naar een bijlage
Naleving van de normen	De provider erkent zijn algemene verplichting om de klant te verzekeren dat zijn interne organisatie en zijn procedures voor gegevensverwerking voldoen aan de	

	toepasbare nationale en internationale normen. In het bijzonder verklaart hij dat zijn diensten voldoen aan de normen vermeld in bijlage 8.	
Traceerbaarheid	De provider zal operaties uitvoeren voor de tracering of audit (logging and auditing) van de verwerkingen van persoonsgegevens die door hem (of door zijn verwerkers, indien van toepassing/toegelaten) werden uitgevoerd.	
Melding van incidenten	De provider verbindt zich ertoe aan zijn klant elk incident te melden in verband met: - veiligheidsproblemen (verspreiding enz.) die een rechtstreekse impact kunnen hebben op de gegevens van zijn klant; - een ernstig probleem of incident dat een impact kan hebben op het geheel van de diensten, ook al lijken de gegevens van de klant niet getroffen te zijn.	
Melding van andere evenementen	De provider verbindt zich ertoe elke interventie door derden (bijvoorbeeld een subcontractant, een verandering in de Escrow) aan zijn klant te melden indien deze derde een rol zou kunnen spelen in de verwerking of de bewaring van de gegevens van de klant. De provider zal ook elke belangrijke wijziging aan de dienst, zoals de invoering van bijkomende functies, aan de klant melden.	
Audit door de Klant	De klant heeft het recht om op zijn kosten een onafhankelijke audit aan te vragen van de veiligheidsprocedures van zijn provider, van de naleving van de aangegeven standaarden en van de eventuele incidenten die zich hebben voorgedaan. De provider verbindt zich ertoe om mee te werken met deze audit en om aan de auditeur de nodige informatie te leveren voor de uitvoering van zijn opdracht.	
Melding van toegangsaanvragen	De provider zal de klant op de hoogte brengen van alle aanvragen voor toegang tot de gegevens die hij wettelijk gezien verplicht is te beantwoorden (aanvragen door de bevoegde gerechtelijke of politieoverheden), behalve wanneer dit verboden is door de wet, bijvoorbeeld om de vertrouwelijkheid van een strafrechtelijk onderzoek niet te schaden.	
Bijstand aan de Klant	De provider zal zijn klant effectief bijstaan om de betrokken personen te helpen hun recht op inzage, rechtzetting of verwijdering van hun gegevens uit te oefenen en bij andere technische interventies die kunnen voortvloeien uit de rol van "verantwoordelijke voor de verwerking" die de klant uitoefent in de zin van richtlijn 95/46 EG.	
Export van persoonsgegevens door de Provider	In het geval dat, volgens de formele verklaring van de klant en/of het engagement van de provider, de door de provider bewaarde gegevens persoonsgegevens zijn in de zin van richtlijn 95/46/EG en op initiatief van de provider worden overgedragen naar installaties in derde landen die geen passend beschermingsniveau voor de	Hier worden de modelcontractbepalingen aangepast aan de cloud zonder dat ze opnieuw geformuleerd moeten worden

	gegevens garanderen, zal de provider gezamenlijk met de klant de verplichtingen van *exporteerder* en *importeerder* van deze gegevens op zich nemen, in de zin van de Modelcontractbepalingen (verwerkers) gepubliceerd door de Europese Commissie in haar beslissing van 5 februari 2010 (Publicatieblad 12/2/2010 L39/5) zoals vermeld in artikel 26 paragraaf 2 van richtlijn 95/46/EG.	

10 Tabel van de voornaamste actieve spelers

Op basis van de informele groep "Belgian cloud" en andere bronnen werd een tabel opgesteld van de voornaamste actieve spelers in het domein van de *cloudcomputing in België*. "In België" betekent niet noodzakelijk "Belgisch": de genoemde bedrijven hebben op zijn minst één site of vertegenwoordiger in België. De realiteit van de Benelux maakt dat sommige bekende buitenlandse ondernemingen (onder meer Amerikaanse bedrijven, zoals Amazon) ervoor hebben gekozen om in België actief te zijn vanuit Luxemburg-stad (of Amsterdam) en geen kantoren of vertegenwoordigers in België hebben.

De tabel bevat:

- De naam van de speler (in alfabetische volgorde);
- Zijn "slogan", de manier – meestal door hem gekozen of van zijn site afgeleid – waarop hij zijn activiteit samenvat bij zijn klanten;
- Zijn voornaamste diensten;
- De website;
- Het land en het type bedrijf (groot bedrijf of kmo). Gezien het gebrek aan openbare gegevens en de frequente overnames van Belgische bedrijven door buitenlandse maatschappijen, wordt deze informatie onder voorbehoud meegegeven.

Nom	Slogan"	Services	Site	Pays	Type
Altimate	Smart IT distributor	Value-added Enterprise IT solutions Close to its partners expectations Competence and expertise in IT infrastructure solutions	http://www.altimate.be/ Belongs to dcc.ie. Aquired by Arrow Electronics in 2012	?	?

Nom	Slogan"	Services	Site	Pays	Type
Amplidata	Build cost-efficient and highly available storage *clouds* with AmpliStor	Erasure coding ensures reliable data storage Reduces TCO with up to 70 % compared to traditional systems Cuts power usage by up to 90 %	www.amplidata.com	BE	Large (US & Egypt)
Adc Antwerp	Is ready to serve you!	Tier 3 Carrier Neutral datacenter Pay-as-you-grow model Disaster Recovery	http://www.antwerpdc.be	BE	PME
Arxus	Hosted Service Provider	Hosted Messaging and Collaboration platform Hosted SharePoint Services	www.arxus.eu	BE	PME
Aspex	Hosting your applications	Trouble-free updates Extremely fast deployment Easy support	www.aspex.com	US	PME (35 highly qualified staff members)
Azlan	Part of the Tech Data Group	Converged Infrastructure Data Centre and Virtualisation Unified Communications and Collaboration	www.azlan.com	UK	Part of TechData since March 2003

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Nom	Slogan"	Services	Site	Pays	Type
Belgacom	Be*Cloud*, providing you end-to-end *Cloud*solutions	We offer *cloud* choice & competences. Private, public or hybrid X-aaS, onsite or hosted in our state-of-the-art datacenter Realising, cost reduction, improved time to market, going green, pay per use	www.belgacom.be	BE	Large
Brandfractal	Social Media Monitoring en Measuring	Impact analysis Sentiment monitoring Community Building	www.brandfractal.com	BE	?
Caligo	*cloud* Enabling & Migration	Housing & Co-Location Hosted Services *cloud* Services, IaaS,SaaS,PaaS	www.caligo.be	BE	?
Channel Reflex	*cloud* Go-To-Market	Succeeding in the *cloud* partner eco-system Strategic & operational B2B channel development Individual personalized approach and 2 days *cloud* Training	www.channelreflex.com	BE	PME <10 employees
Cisco	The people are the network	Borderless Network Collaboration Datacenter & Virtualisation	www.cisco.com	US	Large
Citrix	Making *cloud* computing Enterprise-Ready	Protect sensitive data in the *cloud* Develop and test applications in the *cloud* Deliver applications and desktops on demand	www.citrix.com	US	Large

Nom	Slogan"	Services	Site	Pays	Type
Clevver	Managed BI services	Rapid Deployment Increased user adoption Reduced Cost	www.clevver.com	?	?
*Cloud*time	We change IT as you know it	Improve your customer support Learn how to reduce your IT cost Greater flexibility and scalability; better security and continuity	*cloud*time.be	*?*	*PME*
Combell	Your host in the *cloud*	More than 30.000 clients almost 1 out of 5 Belgium websites Custom *cloud* Hosting to the needs of your business	www.combell.com	BE	PME
Dinamiqs	VirtualStorm – Full private *cloud* desktops	Private & public *cloud* applications Application streaming for offline usage Data synchronization from within the private *cloud*	dinamiqs.com	NL	?
Element 61	Business Intelligence in the *cloud*	BI & data warehousing in the *cloud* *cloud*-based Performance Management Solutions Supporting leading *cloud* platforms	www.element61.be	BE	? 360 MAN Years of experience
EMC^2	Journey into the *cloud*	Architect for the future Drive workforce productivity Reduce operational cost	belgium.emc.com/index.htm?fromGlobalSiteSelect	US	Large

Nom	Slogan"	Services	Site	Pays	Type
Eurofiber	Take advantage of the freedom of an open network	The guarantee that the work on our network is carried out according to pre-agreed procedures minimalises the chances of unnecessary incidents and further increases the reliability of our network.	www.eurofiber.com	NL	?
Exclusive Networks	Value Added Distributor	Security, storage and networking technologies IAAS, PAAS, SAAS IP Address Management	www.exclusive-networks.com	FR	Large
First Served	Think beyond hardware	Smart hosting services Stretching limits of classic server hosting Enterprise grade *cloud* platforms	www.firstserved.net	BE	?
Google	Data centers scattered around the world	12 centres in the US, one in Australia (Sydney), and 3 major known centres in Europe: Eemshaven and Groningen in the Netherlands and Mons (St. Ghislain), Belgium. Services: Gmail, Google docs, Google+, search engine	www.google.com/about/datacenters/locations/st-ghislain/	US	Large
Hitachi	Data Drives our World	Virtualized Automated Sustainable	www.hitachi.com	JP	Large

Nom	Slogan”	Services	Site	Pays	Type
Housing Center	Datacenter- en Netwerkdiensten	Collocation of servers and other infrastructure hardware in fully redundant datacenters *cloud* environment spreading over three datacenters with separate Backup/Disaster Recovery location Managed Services ranging from Basic Server Management to Advanced System Management, Migration and Performance Audits	www.hostcenter.com	CH	?
HP	Take service delivery to the next level	Solutions that help you build *cloud* services Software and services that help you manage and secure your environment Services that help you transform your infrastructure	www.hp.com	US	Large
IBM	The *cloud* – Plan, Build & Deliver	Reduce cost Improve service delivery Enable business innovation	www.ibm.com	US	Large

Nom	Slogan"	Services	Site	Pays	Type
Impro Biz	Improve your business	Implementation services for Salesforce CRM Development of applications on force.com and VMforce.com platform Designed to rapidly meet changing business needs	www.improbiz.be	BE	?
InterAct	Making the Data Center work	Virtualisation & *cloud* computing Experts in Data Center Solutions Designed to rapidly meet changing business needs	www.interact-eu.net	EU ?	?
Interxion	Your carrier-neutral datacenter	High density housing Superior Connectivity Belgium's biggest *cloud* hub	www.interxion.com	UK	?
iRelate	Your expert in business relationships	Providing in depth customer insights for better informed decisions Expert in CRM with competence center in Belgium & The Netherlands, servicing both local and international companies Oracle Belux Partner of the Year – Applications 2010 and 2011	www.irelate.be	BE	?

Nom	Slogan”	Services	Site	Pays	Type
Kappa Data	Value Added Distributor in Networking & Security	Delivering all components for secure transition in the *cloud* Offering tools to maximize *cloud* performance Applying strong user authentication	www.kappadata.be	BE	?
LaCie	Made for ideas	We offer *cloud* choice : Private, public or hybrid Broad network of competent Storage Partners Specialized in SMB offerings	www.lacie.com	US	Large
LCL	The Belgian *cloud* datacenter	A Carrier Neutral Tier 3 data center LCL likes to find with you the right solution LCL, a flexible building for all your *cloud* computing needs	www.lcl.be	BE	?
Microsoft	*cloud* Power	Create, Investigate, Transform, Collaborate, Scalability Office 365 Windows Azure & Hyper-V	www.microsoft.com	US	Large
NetApp	The *Clouds* Are Within Your Reach	Delivering on the Promise of a Virtualized Data Center Perform self-service recoveries in minutes, not hours Provision resources on the fly to meet business needs	www.netapp.com	US	Large

"De voorwaarden scheppen voor een competitieve, duurzame en evenwichtige werking van de goederen- en dienstenmarkt in België."

Nom	Slogan"	Services	Site	Pays	Type
Nucleus	Specialized in *cloud*-Hosting	Hosting Solution Builder *cloud* Hosting specialist Serious Geeks	www.nucleus.be	BE	?
Oracle	Technology That Powers the *cloud*	Ensure that *cloud* computing is fully enterprise grade Deliver most complete PaaS and IaaS product offerings Develop and enable rich SaaS offering	www.oracle.com	US	Large
ProAct	We secure mission-critical information	Data and Storage centric approach for cost efficiencies Gradual transition and migration to the *cloud* Private, public and hybrid Enterprise *cloud* services	www.proact.eu	SE	?
RES Software	Making the Desktop dynamic	Reduce desktop complexity Manage and deliver secure,personalized and compliant desktops Dynamic workforce with on-demand access	www.ressoftware.com	US	?

Nom	Slogan"	Services	Site	Pays	Type
Riverbed	The IT performance company	Increasing application performance with WAN optimization solutions from Riverbed. Eliminating the need to increase bandwidth, storage or servers Delivers greater productivity and cost savings	www.riverbed.com	US	Large
Roger that.net	Enable business process automation through rich mobile interactions	Rogerthat, the world's first "multiple choice messaging platform" Revolutionises communication and process automation via smartphones and tablets We offer our customers flexible mobile reach	www.belgiumcloud.com/?page_id=4684	BE	?
SAAS45 Channel	The *cloud*-SaaS Channel business community	Dedicated online channel community Develop and share knowledge within the ICT Value chain	www.saas4channel.eu	BE	?
SaaSForce	*cloud* Services Distributor	Marketplace for resellers with real-time provisioning Private, Public, Vendor *cloud* Connections Enable Deliver Manage	www.saasforce.be	BE	?

Nom	Slogan"	Services	Site	Pays	Type
SafeNet	The Data Protection Company	Leading global provider of data protection. For over 25 years, global corporations and government agencies have turned to SafeNet to secure and protect their most valuable data assets and intellectual property.	www.safenet-inc.com	US	Large
Silver Peak	Move More. Go Farther. Spend Less	◦Provides Data Center class WAN optimization solutions. ◦Enabling high-quality, reliable throughput over any WAN connection. ◦Optimize all applications and protocols using either physical or virtualized appliances	www.silver-peak.com	US	Large
Symantec *cloud*	Bringing certainty to the exchange of business information	◦Hosted Messaging And Web Security Management ◦Hosted Endpoint Protection ◦Anti Virus & Anti Spam	www.symantec.com	US	Large
Systemat	Bring trust in the *cloud*	◦Local *cloud* integrator ◦Thousands of mid-market customers in Belgium & Luxembourg ◦Green certification ISO 14001	www.systemat.com	BE	Large

Nom	Slogan"	Services	Site	Pays	Type
Telenet	Your IT in reliable hands	◦Build your own custom virtual servers ◦Latest hardware in our high-tech data centres ◦Quick interventions for 99,9 % uptime	www.telenet.com	BE	Large
Terremark	Infrastructure as a Service	◦Enterprise *cloud* ◦Infinistructure ◦Managed Dedicated Hosting	www.terremark.be	US	Large
the CRM-Warehouse	*cloud* Integrators	◦Full automation with *cloud* Applications (CRM, HMC, CCM, ERP, CMS) ◦Fixed Fee per month per user ◦100 % *cloud*, 100 % Customised	www.crm-warehouse.be	BE ?	?
Thin *factory*	Delivering *cloud* Solutions in a Dynamic World	◦*cloud* Infrastructure ◦Marketplace for *cloud* Services ◦*cloud* Orchestration Platform	www.thinfactory.com	BE	?
uptime Group	ICT Differently	◦Your idea our business ◦Power & Passion ◦Knowledge Datacenter	www.uptime.be	BE	?
Vasco	MYDIGIPASS.COM – Join today!	◦Add Convenient Security to your Web Applications ◦Eliminate password management hassles ◦Free mobile client authenticators	www.vasco.com	US	Large

Nom	Slogan"	Services	Site	Pays	Type
VM WARE	Accelerate IT. Accelerate your Business	◦Self Service for the *cloud* ◦Scalability & Flexibility ◦Pooling & dynamic resourcing	www.vmware.com	US	?
Xaop	We keep your documents in the *cloud* in Sync & Secure	◦System integration in the *cloud* ◦(Mobile) Application development ◦Process analysis and prototyping	www.belgium*cloud*.com/?page_id=133	BE	?
Zenith	Zenith Infotech Europe	◦*cloud* oplossingen voor KMO's ◦Private *cloud* ◦Business Continuïteit	www.zenithinfotech.com	US	Large

11 Bibliografie

United Kingdom – Information Commissioner Office (ICO), Guidance on the use of cloud computing, [Online] http://www.ico.org.uk/about_us/research/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

United Kingdom (UK) Open Standards Principles: For software interoperability, data and document formats in government IT specifications [Online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78892/Open-Standards-Principles-FINAL.pdf

Interxion Europe-wide survey of current and intended cloud usage and attitudes towards cloud computing. [Online] http://www.interxion.com/cloud-insight/index.html.

Dale Vile, Freedom Dynamic ltd, A vision for the Data Centre – The Register – [Online] https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&sqi=2&ved=0CDgQFjAB&url=http%3A%2F%2Fwhitepapers.theregister.co.uk%2Fpaper%2Fdownload%2F2674%2Fa-vision-for-the-data-centre.pdf&ei=DzZdUf-TJsiQrQfTkICYDw&usg=AFQjCNGrbACIU8jp1mtMGGInnjEFQmcu9A&sig2=u4uILFYBJItPkVS7uEtbUQ&bvm=bv.44770516,d.bmk

European Parliament – DG Internal policies, Fighting cybercrime and protecting privacy in the cloud (study) December 2012 – [Online] http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

European Commission – COM (2012) 529, Unleashing the Potential of Cloud Computing in Europe [Online] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0271:FIN:EN:PDF

European Commission COM (2012) 11 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Online] http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201286

European Commission COM (2011) 942 COMMISSION COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A coherent framework for building trust in the Digital Single Market for e-commerce and online services [Online] http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/COM2011_942_en.pdf

European Commission COM (2002) 16 EC Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC. [Online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0016:EN:NOT & http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:FR:PDF

IDC, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take - SMART 2011/0045 [Online] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 05/2012 on cloud computing [Online] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

European Commission – DG INFSO Expert Group Report, The Future of Cloud Computing, Opportunities for European Cloud Computing beyond 2010. [Online] http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=6993

Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland, 26th January 2012. [Online] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38&format=HTML&aged=0&language=EN&guiLanguage=en.

Cloud Computing: Benefits, Risks and Recommendations for Information Security. [Online] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

ENISA, Critical Cloud Computing – a CIIP perspective on cloud computing services – December 2012 [Online] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing

ENISA Cloud Computing Information Assurance Framework. [Online] 2009. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.

ENISA. Security and Resilience in Governmental Clouds. [Online] 2011. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

ENISA, Cloud Computing, Benefits, risks and recommendations for information security (November 2009) [Online] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view

ENISA Procure Secure – A guide to monitoring of security service levels in cloud contracts [on line]

https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CDAQFjAA&url=http%3A%2F%2Fwww.enisa.europa.eu%2Factivities%2FResilience-and-CIIP%2Fcloud-computing%2Fprocure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts%2Fat_download%2FfullReport&ei=yi9dUbWtIcjZrQep5oCYBA&usg=AFQjCNGWddPe5UXWfuBNK1_rRxu0FyaJsQ&sig2=N_sRgVmVd-i9NpRpYnFoGw&bvm=bv.44770516,d.bmk

Information commissioner and Cloud security alliance Slovenian chapter, Personal data protection and cloud computing, (15 June 2012)

NSAI (Ireland) SWiFT 10:2012 Adopting the Cloud – decision support for cloud computing (4 avril 2012) [Online] http://www.nsai.ie/Special-Pages/News/NSAI-and-IIA-Cloud-Computing-Standard-Launched-by-.aspx

Survey and analysis of security parameters in cloud SLAs across the European public sector. [Online] 2011. http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector.

International Standard on Assurance Engagements (ISAE) 3402. [Online] http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf.

Cloud Security Alliance Cloud Controls Matrix. [Online] https://cloudsecurityalliance.org/research/ccm/.

Guidelines on information security controls for the use of cloud computing services. [Online] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43757. A guide to monitoring of security service levels in cloud contracts

NIST Definition of Cloud Computing - NIST SP 800-145. [Online] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

NIST. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. [Online] 2011. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

Government, US. Federal Risk and Authorization Management Programme - Concept of Operations (Includes a section on continuous monitoring). [Online] 2012. http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

Annual FISMA Reporting: Chief Information Officer Questions. [Online] 2009. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/cio_questions.pdf.
ENISA. Resilience Metrics and Measurements: Technical Report. [Online] 2011. http://www.enisa.europa.eu/activities/res/other-areas/metrics/reports/metrics-tech-report.

Commission decisions on the adequacy of the protection of personal data in third countries. [Online] http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

European IT decision-makers and influencers give their views on cloud computing. [Online] http://www.interxion.com/cloud-insight/index.html.

Survey and analysis of security parameters in cloud SLAs across the European public sector. [Online] http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector.

Survey and analysis of security parameters in cloud SLAs across the European public sector. [Online] http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector.

Security and Resilience in Governmental Clouds. [Online] http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

ENISA Cloud Computing Information Assurance Framework. [Online] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.

Cloud Computing: Benefits, Risks and Recommendations for Information Security. [Online] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

12 Lijst van gebruikte afkortingen

BCR	Binding Corporate Rules (regels van een onderneming, die moeten worden goedgekeurd door een nationale overheid bevoegd voor de bescherming van gegevens)
CIP	Critical Infrastructure protection
CIIP	Critical Information Infrastructure Protection (Eur Commissions Communication on …)
DDoS	Distributed Denial of Service
ECP	European Cloud Partnership
EER	Europese Economische Ruimte (EU + Noorwegen, IJsland, Liechtenstein)
ENISA	European Network and Information Security Agency
ETSI	Europees Instituut voor Telecommunicatienormen
IaaS	Infrastructure as a Service (Cloud die capaciteit aanbiedt voor communicatie, berekeningen en opslag)
WPL	(Belgische) Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer
NIST	(US) National Institute for Standards and Technology
PaaS	Platform as a Service (Cloud die een operationeel platform aanbiedt voor de hosting van diensten)
Kmo	Kleine of middelgrote onderneming (< 250 personen in Europa)
RA	Risk Assessment – De bepaling van welke infrastructuren kritiek zijn, hun belang, de incidenten die voor hen vermeden moeten worden.
SaaS	Software as a Service (Cloud die applicaties of oplossingen aanbiedt die de gebruikers online kunnen gebruiken)
SLA	Service Level Agreement (Serviceniveauovereenkomst)
SOA	Service Oriented Architecture
SPF/FOD	Service public fédéral/Federale Overheidsdienst
TCO	Total cost of ownership (globale kostprijs voor installatie, exploitatie en evolutie/release van een oplossing)
EU	Europese Unie

© Female photographer - Fotolia.com

economie
FOD Economie, K.M.O., Middenstand en Energie

Vooruitgangstraat 50
1210 Brussel
Ondernemingsnummer: 0314.595.348
http://economie.fgov.be