International In-house Counsel Journal
Nordic Edition 2011, 19

The Legal Challenges of Cloud Computing

NIELS CHR. ELLEGAARD
Attorney-at-Law, Plesner, Denmark

Cloud computing has for some time been a buzz word within the IT industry and has been seen by many stakeholders as a "revolution" that will alter the world of IT. Critics of the new IT concept maintains that this is just "old wine on new bottles" applying existing technology in a new business model. From a legal perspective, cloud computing raises several challenges which has - also taking into account the operational risks - caused reluctance from the customer side to adopt new cloud based solutions at a broader scale. This article seeks to identify the "legal" entry barriers, and concludes that these may to a large extent be overcome if the supplier and customer can agree on a customised approach to cloud computing.

1 What is cloud computing?

No general definition of cloud computing exists. However, in general, the industry has agreed on certain characteristics of a cloud service. Normally cloud computing is regarded as a general term for an IT solution which is offered as a service over the internet instead of the customer buying the solution and installing it in its own environment.

The characteristics of a cloud service is that it is normally:

- accessed via the internet
- paid on the basis of need and use
- adjusted up and down as needed, and
- delivered from a platform of pooled computer resources

Normally, cloud computing services are divided into the following categories[4]:

- "Infrastructure as a Service" (IaaS): Network, computer power or storage, processing and other fundamental computing ressources, which the user can use for running software such as operating systems and applications.
- "Platform as a Service" (PaaS): Webbased platform containing a number of basic services, and where the user can deploy its own applications.
- "Software as a Service" (SaaS): applications provided by the supplier which can be used without installation on the user's own computer. Management of applications including updates are made centrally.

[4] See definitions in Cloud Security Alliance Security guidance for Critical Areas of Focus in Cloud Computing, p. 15-16 (http://cloudsecurityalliance.org/csaguide.pdf)

 ISSN 1754-0607 print/ISSN 1754-0607 online

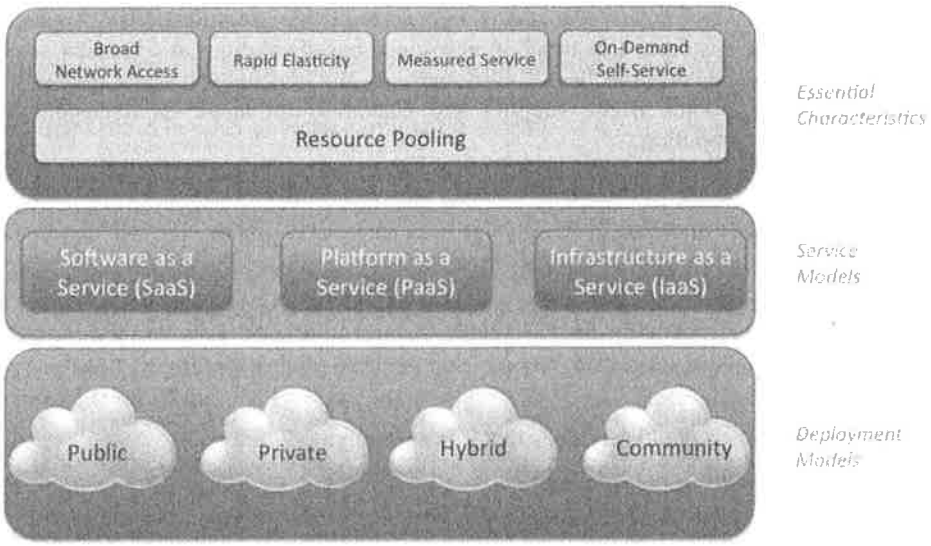
Infrastructure as a Service (IaaS) is the basic layer offering the core layer of computer power, storage, network service enabling running of any software.

Platform as a Service (PaaS) is the middle layer offering tools, application programming interfaces (API), integration and middleware enabling the customer to place applications directly on the platform established in the service provider's or a third party's infrastructure.

Software as a Service (SaaS) is the upper layer providing for applications placed by the service provider on a platform controlled by the service provider.

Visually, cloud computing can be displayed as following:

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



The main advantages of cloud computing are often summarised as follows:

- Low – or no – start-up costs
- Payment according to need/use
- Great flexibility in relation to fast up- and downscaling of resource needs
- Possibility of short term of agreements
- Possibility of "thin clients"
- Possibility of *full service* with maintenance and service levels for performance (SLA) in an overall service
- Possibility of access to supplier's economies of scale by use of server capacity
- Easier (and cheaper) access to new software versions
- Other common outsourcing advantages (security for uptime, availability, contingency arrangements, reduced costs of investment in own data centre)
- Environmental advantages – considerable CO2 reductions when server-resources are pooled in large data centres, or when servers are grouped virtually to a joint server capacity (enables a far more efficient utilisation).

In turn the main disadvantages of applying cloud computing services are often seen to be the following:

- Financial trade-off is necessary – in the long run it might be more expensive to have a cloud solution compared to an in-house solution ("Opex vs Capex")
- Lack of control on operation and development
- Vulnerability in relation to the solution being delivered and operated by (normally) one supplier (adding to "lock in" of the customer with the service provider)
- Costs of data traffic to and from the solution
- Risks in connection with security in the communication with the solution (encryption of traffic and access to the solution (the so called "triple-A problem" - Access, authority and authentication)
- Dependence on being online
- data security and return of data upon termination
- Limitations in relation to customisations to standard software
- integration with other applications and systems
- Coordination of co-operation among the cloud service provider and the customer's other IT-suppliers (e.g. application maintenance (AM) and operation)
- Lack of standards between cloud service providers can create problems upon relocation of data to a new supplier or at the interaction between different "clouds" (adding to "lock in" of the customer with the service provider))
- It may be difficult to assess which laws apply to the data stored, since use of cloud resources entails data may be placed in various locations

2 What do the services comprise legally?

2.1 The essence of the services

As opposed to traditional computing, the customer is in essence offered services as opposed to goods. This is not new when compared with IT outsourcing services such as data centre services. However, the business model is new since such services are acquired over the internet.

A cloud service may be seen as a combined service consisting of:

- access to a solution with a given functionality,
- a given availability of the solution, and
- access to or handling of data, software and/or applications by the solution.

As a point of departure, it is the customer who bears the risk that the service can be accessed and received. Thus, if the service id ready for download it is up to the user to obtain such access through his or her browser. Also - if the processing time of the solution is within agreed service levels it is also the risk of the customer, that it is able to experience such processing time at its own end.

The fact that the cloud solution is a service does not change the basic features of what the customer wants the infrastructure or software to do for it. It is still the same processing that is provided for the customer through the solution. However, in a cloud environment

the customer is no longer in control of the operation of the software or infrastructure (or only in a limited manner). The lack of control is most predominant in the SaaS-solutions whereas the customer will have a higher degree of control in a IaaS-solution, where the customer itself chooses the software and applications to be deployed on the infrastructure.

Most of the specific legal issues arising out of the use of cloud computing is related to the lack of control compared to the situation where the solution is run by the customer or user itself. For users who have already outsourced its operational environment in the form of servers and storage capacity in a standard IT outsourcing (in what could be called a private or community cloud) this is not a new situation. However, new dimensions are added to such - existing - lack of control when entering into the domain of SaaS and this is probably what most people have in mind when assessing the legal risks of cloud computing.

2.2 The software licence in a new context

Users should also be aware that cloud services also opens up a new dimension in terms of licensing. In Denmark and Europe in general software is mainly protected through copyright legislation and typically software licenses are granted for a specific purpose (which may be broadly phrased) as a perpetual, non-exclusive right to use software for a specific number of users or at servers with a certain set of processors (CPU's).

In cloud computing (Software as a Service = SaaS), the licence is a kind of a "subscription", where the customer on a month by month basis rents a right to access the software for a specific circle of users.

When assessing a software license, the principle of speciality under section 53(3) of the Danish Act on Copyright needs to be taken into account. The principle means that no rights, other than those explicitly agreed to, are covered by the license. The right of use to the software (SaaS) is provided only through the access to the solution (the licence becomes in a sense indirect). Thus, as can be seen from the various subscription agreements and terms & conditions governing the cloud services, the services are not presented legally as a license, but rather as services.[5]

Regardless of whether the use of services are described through the license terminology or the service terminology, the parties should agree as to whether the customer has or shall have rights to the software apart from the "indirect" licence. Such rights are not so relevant when dealing with standard software where the customer should expect that no rights exists other than the rights to access the software in the subscription period. However, the scope of the license is relevant if the solution includes customisations, modifications or configurations which the customer would have a need to retain if it wishes to move to a new cloud provider upon termination of the agreement. Such rights will only exist if they are specifically addressed in the license

Many software vendors have built their business on having customers to subscribe for support and maintenance over annual subscription arrangements. However, the cloud business model may change this since new updates and support of the solution in SaaS will form an automatic part of the services. Thus, the support and maintenance relation will be between the cloud provider and the software vendor unless special arrangements

---

5 See e.g. Salesforce.com defining their services as " means the products and services that are ordered by You under a free trial or an Order Form and made available by Us online via the customer login..." (https://www.salesforce.com).

are made. This feature may also affect how software vendors build their future revenue streams.

3 General legal risks

The inherent legal risks of cloud computing seen from the perspective of the user have briefly been touched upon in the list of disadvantages displayed above. Going into further detail they may be summarised as follows:

- How to ensure that the customer always has access to its data (availability)?
- How to ensure that nobody else than the customer and users authorised by the customer have access to the data (security)?
- In which country is the solution provided/where is the server placed (which laws apply and how to secure compliance with such laws)?
- How to secure against adverse consequences of lock-in (i.e. are there any effective legal remedies that will allow the customer to protect itself (through shifting to another supplier or taking home the services provided by the cloud provider, deny acceptance of changes or claim compensation that will keep the customer whole) in the event of suppliers failure to meet service levels, price increases, changes in software version etc.)?
- How to deal with consequences upon termination - with cause and without cause ("how do I get my data back")?

All the said risks can be attributed to the lack of control referred to above under section 2 and could - seen from the user's perspective - in principle be managed legally by introducing protective legal requirements in the contract between the supplier and the customer. However, in practice the situation is quite the contrary since requirements of action and liability of the supplier is to a large extent disclaimed. As will be further examined in detail below the prevailing legal regime used by cloud providers represents an entry barrier for cloud computing. On the other hand users need to understand and accept as a fundamental premise of outsourcing that an outsourcing partner such as a cloud provider needs to maintain operational freedom and reduce and cap its liability given that the price of the service would not otherwise mirror the risks of it.

4 The need to adapt the IT contract to the new business model

4.1 Elements of cloud services and match with existing standard contracts

The elements included in a cloud service makes it relevant to consider various types of agreements and provisions used in IT-contracts. Cloud services may be seen as a package combining features from the following pre-existing services and products:

- Hosting services
- General IT-outsourcing services
- Licence of software
- Service Level Agreements (SLA) on availability

This bundling of services makes it relevant to consider provisions from agreements normally used in such areas. No general standard agreement exists which could work as a benchmark for the cloud services agreements

In Denmark the standard contract K01 drafted for governmental short term IT-projects has to some extent worked as a standard within the IT-industry in Denmark.[6] Using this standard contract as an example it can easily be seen that it would require considerable adjustments to adapt such standard contract to make it fit for cloud computing purposes. A highlight of the problems are the following:

- No system as such is delivered; Instead access to a system (redefinition of subject matter is needed)
- Provisions governing process are superfluous (Often it will be difficult to view the delivery as a "project" and therefore many of the provisions governing the process are unnecessary)
- IP-rights need to be clarified (as mentioned above the point of departure in cloud computing would normally bet hat you only have an indirect license right of use as long as the subscription remains)
- Tests – what should they comprise for cloud services (Hardly any tests apply in respect of the existing cloud service offerings save for do it yourself testing)?
- Payment provisions need to be amended (payment would normally not fall due in instalments along with the progression of the "project" but rather base don consumption)
- Need for integration of hosting terms, including increased focus on data protection
- Proof of security
- Audit of operating environment (e.g. verification through audit statements such as SAS 70)
- Service levels are the offering
- Extended terms and conditions governing consequences of termination (How to get back data upon termination and how to make sure that data are subsequently deleted with the cloud provider)

Some issues are beyond the contract itself with the cloud provider. Thus, certain issues the customer needs to assess on its own or ask independent professionals to ascertain. E.g. if maintenance of the solution is not performed by the supplier, an inter-supplier agreement must be established or otherwise a right to maintain for the customer must be granted in the contract with the cloud provider.

In respect of interfaces to other applications it may be difficult to obtain certainty that interfaces used upon entry will remain over time. This may in turn cause uncertainty as to how the cloud services can be combined with the rest of the customer's applications in the future. This particular issue could in principle be resolved in the contract with the cloud provider. However, many cloud providers would not commit to continue interfaces.

---

[6] The standard agreement may be downloaded from the Danish IT- and Telecom Agencency website (http://www.itst.dk/it-arkitektur-og-standarder/it-styring/standardkontrakter/k01).

4.2 Breach of contract situations

Lawyers would of course focus on the remedies available in the event of breach of contract. However, for cloud services the concern should not so much be on termination for cause. Normally, the customer may discontinue the contract at any time with a very short notice or no notice. This is part of the flexibility included in the concept. Therefore, focus is rather held on how to ensure compensation for failure to make the solution available at the level promised in the contract. Applying the general practice on limitation of liability used in existing IT contracts would not meet the demands for compensation if the compensation should meet the actual losses suffered. Also it may not give a sufficient incentive of the cloud provider to perform (the best incentive is by the far the incentive not to get a bad reputation in the market). This issue is not new when it comes to IT contracts, but since the depencies of the cloud provider is higher, a satisfactory solution to this issue becomes critical. As will be discussed below it is not likely that suppliers will meet such demands – on the contrary based on the approach taken by cloud providers so far, limitation of liability is normally tightened when it comes to cloud computing.

In terms of safeguarding itself against adverse consequences of a cloud providers breach of contract and ensuring business continuity, the protection should not so much be found in the contract and the remedies provided for. Instead the customer should seek to select a provider that will never get there. Such comfort could be obtained through due diligence as to how the cloud solution has been and will be managed by the cloud provider:

- Is there sufficient and comforting information about the data centres used?
- Have the data centres been audited and what does the audit tell (if made public)?
- What is the track record of the provider on availability?
- What is the track record on security?
- What is the policy on interfaces and how are these managed?
- What do former and existing customers tell?
- What is planned to happen with the solution during the following 12 months and what is on the horizon 3-5 years ahead?

4.3 Business continuity

One thing that could be done in respect of ensuring business continuity under the contract is to address the situation of the cloud provider's insolvency/bankruptcy. In traditional IT, focus has been on escrow of the source code with a third party. In a cloud offering the customer should not focus on the licensed software (this you only have as long as the subscription runs). Instead the customer should focus on a way to ensure claw-back of data upon insolvency. No standard method exist yet, but what could be a satisfactory solution would be to have some access to pull back data by use of a "key" which would automatically be released upon the cloud provider's insolvency. This would not ensure business continuity in the short run since you would have to migrate to a new solution to have an effective solution running. But at least it would make the customer feel comfortable that data is not trapped and that you can control pull back should the situation occur. Such solution

would require that the solution is still accessible, which may not necessarily be the case in the event of bankruptcy. To obtain a better solution you would have to have a back up with a third party with whom you have a separate agreement and this may increase costs and to some extent reduce benefits.

5 The approach taken by cloud providers so far

So far cloud services have primarily been provided as a commodity where the customer has been asked to accept non-negotiable "click and accept" terms. The price of the services is often very low compared to traditional IT-offerings and services are offered as a mass product. This has led the cloud providers to introduce broad disclaimers and waivers. As a concrete example the terms and conditions of Amazon Web Services could be referred to.[7] In the said terms and conditions Amazon may e.g. terminate the agreement for convenience with a notice of 30 days and may at its own discretion change the services including the application programme interfaces (API) used upon entry. In terms of liability and indemnification the following is stated:

"WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (c) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL BE LIMITED TO THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS PRECEDING THE CLAIM."

The provisions used by Amazon Web Services are not unusual and similar provisions can be found in most terms and conditions used by cloud providers. Seen from the perspective of the cloud provider it may be justified to reduce liability significantly due to the nature of the services as a "mass product". Also it

7 See Amazon Web Services Customer Agreement (http://aws.amazon.com/agreement)

is necessary to retain right to adjust services in order to ensure right of change on the cloud platform used for the offering. However, exactly this need for flexibility and limitation of liability on the part of the cloud provider (leading to inherent legal risks in the product seen from the customer side not being managed) combined with the lack of control experienced by the customer side is probably one of the main reasons that businesses (save for small businesses and start up businesses) are reluctant to use cloud services at a larger scale - despite all the advantages.

6 The way in the middle - customised cloud services

As illustrated above, there is a significant gap between what the cloud providers want and what the customers expect. The big question is therefore whether a zone in the middle exists where both cloud providers and customers would feel comfortable and safe in order to make use of cloud services at a larger scale? Some will probably say that cloud computing is by definition a commoditized product and that customised cloud is a contradiction in terms and will "kill" the concept. However, my answer to the question is yes, and the way forward is in my opinion to leave the path of commodities and enter the field of customised products. It will still be necessary for the customers to accept a lower degree of control with the IT-solution in question, and a customised approach will of course have an impact on price, since it will no longer be possible with a "one-size-fits-all" solution. Nevertheless, it will still be possible to obtain significant savings for the customers allowing salient features of cloud computing to remain in the offering.

Customised cloud computing services means that customers are treated individually and are allowed to have special wishes and demands acknowledged while at the same time allowing the cloud provider to retain the possibility of large scale operations. One way of obtaining such a situation would be to divide the application into core and add-on respectively. This will mean that the customers would have to accept the core as being the exclusive domain of the cloud provider, subject to warranties on basic functionality remaining, whereas the add-ons may be modifications specific to the customer and something that the parties have to deal with jointly, and where the customer will have a right to retain functionality also after termination. It also means that the customer should be assured that interfaces will remain in a long term perspective and that changes cannot be made easily.

To ensure scalability and effectiveness on the part of the cloud provider, customers should not expect tailormade service levels. This would just increase costs of the provider and probably not add to the protection since the organisation will probably not be able to handle to may different service level regimes. Instead the cloud providers should have various standards and service level modules which can be used to adapt to the customers individual needs.

When it comes to protection of data, the cloud provider should be able to meet individual demands such as provision of a location guarantee (i.e. the customer's data will not be stored or processed other than in specified jurisdictions). Also specific measures on access and authority should be considered.

To give comfort to the customers, it will be necessary to have liability caps of a size that will allow the customer to obtain a reasonable degree of compensation. This will have to be factored into the price, and the cloud provider will still have to disclaim indirect losses in order not to accept unforeseeable consequences of failed performance.

When it comes to retrieval of data, the customer should be able to obtain comfort on termination assistance being provided by the cloud provider and that reasonable measures have been taken to ensure a smooth return of data being possible. Not all customers are in need of the same degree of comfort so this will have to be dealt with on an individual basis.

The above is illustrative examples of how the parties can meet each other in the middle. However, for each wish or demand for customisation both parties should consider whether it will make sense from an operational as well as financial point of view to deviate from a given standard. Only the market will tell how to strike this balance and adjust demand and supply properly.