Thouvenin Rechtsanwälte
Klausstrasse 33
CH-8034 Zürich

Phone +41 44 421 45 45
Fax +41 44 421 45 00
E-mail info@thouvenin.com

www.thouvenin.com

IT and Internet Newsletter Switzerland

Legal Aspects of Cloud Computing

1. What is Cloud Computing?

1.1 Introduction

For the purpose of this article, the term cloud computing is used to describe a model under which an enterprise or private user ("customer") uses the services of a third party ("provider") to host data either on dedicated or shared servers and under which applications are made available to such users as a service over the internet, sometimes over the intranet and/or dedicated data connections. Cloud computing therefore consists of a combination of services such as managed data centre services, software services and communication services and may include parts or the entire IT-services of a customer.

Under the concept of cloud computing, the customer data will be hosted on a server or combination of servers outside the customer's premises. Generally, data will be stored in location often determined by the availability of the servers at the very moment data are transferred, e.g. taking advantage of free capacity in other time zones. Unlike traditional managed data centre services, the customer no longer owns the servers or the software licenses required to run the systems and applications. The respective licenses are made available by the provider as a service.

1.2 Benefits of Cloud Computing

Cloud computing offers a range of benefits to a customer. It reduces capex spending significantly, since hardware and software is no longer purchased but licensed on a per use or capacity basis, improves scalability (more flexibility in case of increased data storage capacity needs), increases cost control, arguably lowers the total costs of ownership and results in energy savings (energy, hardware and rack space) through the sharing and virtualization of servers. Since a significant part of the work previously performed by the customer's IT-department will become the responsibility of the provider, head counts in the IT-department are also expected to decrease significantly.

Cloud computing further facilitates updates and the introduction of new services and applications in a large enterprise and the deployment of the services to new users.

Finally, if carefully selected, the providers of cloud computing services are generally in a better position to offer state of the art protection against unpermitted access to data, loss of data, higher availability and quick disaster recovery mechanism than enterprises that usually have a limited IT-budget and inhouse capacity.

1.3 Prejudices Against Cloud Computing

Many prospective customers seem still somewhat sceptical of cloud computing. Having dedicated hardware sitting on their own premises or dedicated hardware in a third party owned data centre is often viewed as having control and security.

However, as more and more enterprises have moved to outsource the management and operations of their IT-systems (or parts thereof) to trusted partners and have overcome their prejudice against outsourcing, it would seem that the next natural move from outsourcing and managed services will be to cloud computing. Careful selection of the provider is key to a successful transition to cloud computing.

It is also feared that cloud computing may increase the dependency of the customer from the provider of the services and therefore make it difficult to resource and back source the cloud services. This is however also true for managed IT-services and can be overcome by agreeing on the exit management upon conclusion of the cloud computing agreement.

Lastly, cloud computing is only as good as the data connection between their users and the provider.

When the communication fails, the business comes to a halt. Redundant access is therefore recommended.

1.4 Why Location Matters

According to a recent research made by British Telecom (http://www.btplc.com/News/Articles/ShowArticle.cfm?ArticleID=45062EB2-D5D5-4A6E-AD1E-885EA2A64759) it appears that data security is one of the main concerns to customers when considering cloud computing.

From the provider's end, the implementation of state of the art technical and organisational security measures is necessary. From the customer's side proper data encryption while data is still in its custody is recommended to avoid unpermitted third party access to the information.

However, as it has become obvious at the latest since Snowden's revelations, location of data is also of paramount importance when it comes to data security, data protection and and access to data by governmental authorities. If the data is located on servers in the United States or any other jurisdiction, the law of that jurisdiction will determine who may obtain access to such data and under what circumstances. This concerns primarily the location of servers, on which data are stored, but also on the routing path of data.

The place of location of the data is also important in case of insolvency of a cloud computing provider or if a provider refuses to allow a customer to access its data for any reason whatsoever, as it will determine the place of jurisdiction in case a claim needs to be filed.

2. Contractual Framework

2.1 Freedom of Contract

As a general rule, the parties are free to stipulate in their agreement the terms that should govern their relationship, subject of course to the mandatory provisions of Swiss law.

2.2 Cloud Computing as "Innominatkontrakt"

Given the combination of various services containing elements of lease agreements, software license agreements, hard- and software support agreements, service level agreements, data storage agreements and data transmission agreements and even body lease agreements, cloud computing does not fall under a contract which is explicitly dealt with in the Swiss Code of Obligations ("CO") as a typified contract and must therefore be qualified as a so called *"Innominatkontrakt"*.

When a court is in charge of analysing an *Innominatkontrakt,* it will have to analyse the characteristics of the agreement and the services provided and will then decide, whether or not and to what extent the provisions of the CO dealing with statutory typified contracts will have to apply to the contract under review. This becomes particularly important when the contract is silent on certain issues and in respect of the application of mandatory provisions of the CO.

Mandatory provisions in the context of cloud computing could include the right to terminate a mandate agreement at will (art. 404 CO), should a court should find a cloud computing agreement or parts thereof to fall under the provisions of a mandate agreement in accordance with art. 394 et seq. CO or the transfer of employees to the service provider where the transfer of the operations qualifies as a transfer of a business unit (see art. 333 CO).

2.3 Lease Contract Elements

One element of cloud computing is the availability of storage media and process capacity on a server. The lease of hard disk space on a server against payment of a fee could be qualified as a lease agreement in accordance with art. 253 et seq. CO. However, the processing ability does not form part of a typical lease contract but qualifies more as a mandate agreement (art. 397 et seq. CO) or depending upon the specifications of the contract, as a contract for works in accordance with art. 363 et seq. CO. The interdependency of the services shows the limits to typifying cloud computing agreements. Thus, the court should refrain from applying statutory rules of one contractual type, such as the termination right at will as foreseen in the mandate (art. 404 CO).

2.4. Licensing Contract Elements

The use of the hardware and processing capacity typically requires all sort of software licenses for the operating systems as well as for the applications. It is typical for cloud computing that the software licenses are not purchased by the user but the provider charges the user on a pay per use or other basis. The licensing agreement itself is again not a typified contract under the CO.

The impact of customer not being able to use software licensed by the cloud provider due for instance of its delay in payment of the license fees by the provider needs to be analysed and addressed in proper contractual clauses.

2.5 Service Levels and Support Agreements

Service levels and support agreements are crucial to cloud computing agreements. The user wants to be assured of the availability of the services and support at all times. Such service level and support agreements are again not typified under the CO. These agreements contain mainly elements of a mandate agreement but could also contain elements of the contracts for works in respect of fault repair.

2.6 Disaster Recovery and Protection

Cloud computing agreements will need to address disaster recovery scenarios and these will have to address also a potential insolvency of the provider (see section 4 below). The customer must therefore be put in a position to quickly resume its operations. Solutions can range from simple back-up storage as the cheapest solution to a full-fledged duplication of the entire cloud structure and operations with a third party provider. By placing the data storage services in a separate legal entity or even a trust or foundation, a provider of cloud computing services may further enhance the protection of its customers in the event of provider’s insolvency.

2.7 Transition Services Agreements

Transition services agreements will need to govern the transition of the customer operated IT-infrastructure and the migration of its data to the provider as well as back to the customer or a third party in the case of the termination of the agreement with the provider (exit provisions).

Typically these agreements will have elements of a mandate agreement in as far as the planning is concerned, but may also contain elements of a contract for works where data need to be transferred from one server to another, depending upon the parties' agreement.

2.8 Employee Transfer

The parties to a cloud computing agreement will also need to consider, whether or not the agreement may result in a transfer of a business unit and therefore the automatic transfer of the customers' employees belonging to such business unit to the provider.

2.9 Service Description and Prices

Cloud computing agreements will need to carefully specify the services rendered and the costs charged by the provider. As it is the case with outsourcing agreements where the services and the respective charges are not clearly identified, it is only a question of time until a dispute occurs over the prices and service expectation.

2.10 Termination Provision

Cloud computing agreements will have to contain termination provisions for both ordinary and extraordinary circumstances and to provide for detailed exit provisions and post termination assistance. Adequate notice periods must be agreed upon in order to permit the parties to transfer the services to a third party or take them back in-house.

2.11 Dispute Resolution

Careful attention must be given to dispute resolution mechanisms. Time is often of the essence and a customer must make sure that it obtains fast relief which can be quickly enforced against the provider of the services if needed.

3. Data Protection and Business Secrets

3.1 Data Protection

Any cloud computing agreement must address the data protection issues. Clear rules will have to be established on the storage location of data, access to such data and monitoring of access to customer data (log files). Standard data processing agreements will need to be entered into between the cloud services provider and the customer.

Depending upon the data in question, the customer may need to obtain the consent of the parties whose data will be stored on the provider's server and, depending upon the location of the server, access and type of data, the data protection officer may need to be notified as well.

Industry specific regulations must also be considered such client attorney privilege in the case of law firms, privacy of medical records as well as of other data such as telecommunication and banking data which all benefit from increased protection under Swiss law.

3.2 Protection of Business Secrets

Since data which is the object of the cloud computing agreement may contain customer sensitive information such as business and trade secrets, intellectual property rights of whatever nature, cloud computing agreements must also address the confidential nature of data stored by the provider and the consequences of a breach of the confidentiality obligation. Such data should also be encrypted for added customer protection.

4. Provider Insolvency Risk

When considering its IT-security and back-up structure, a customer will have to carefully analyse the impact of provider insolvency on its ability to continue to operate. Since typically the infrastructure to provide the services will be owned or leased by the provider, a customer will have no segregation rights in the event of insolvency and, even if the customer did have such rights, the question is, whether the customer may be able to operate. Access to data which typically will be stored on servers shared with others or placed with the provider, will become difficult and may be obtained only with substantial delays.

A customer must therefore assure that it is able to continue its operations in the case of provider insolvency and the provider must have an adequate disaster recovery plan. These protective scenarios should be measure tailored to the customer's needs. A provider of cloud computing must therefore be in a position to offer solutions to the customer in the case of the provider's insolvency and address the customer's concerns. The negative impact of provider insolvency on the customer may also be reduced by carefully selecting the data and applications that will be operated by the provider.

5. Conclusions

Cloud computing is a trend that cannot be reversed. The demand of having access to data from anywhere through various devices will increase. Many applications on our smart phones and other mobile devices and data related thereto are already hosted in the cloud. This shows exemplarily where IT-industry is heading to.

However, when cloud computing is used for business critical applications or when critical or sensitive data are hosted in the cloud, it is of paramount importance that detailed cloud computing agreements are entered into with the provider of cloud computing services, addressing in particular access, security and availability of the data, also in case of disaster recovery and the exit scenario, including data portability.

January 20, 2015

David Känzig and Katia Favre

For further information please contact:
Katia Favre (k.favre@thouvenin.com) or
David Känzig (d.kaenzig@thouvenin.com)

THOUVENIN rechtsanwälte compact
THOUVENIN rechtsanwälte is an innovative and partner-centred law firm with more than three decades of experience in business law.

Our experienced TMT team advises on a wide range of contentious and non-contentious issues related to telecommunication, broadcast and information technology, including licensing and registration, data protection issues, mergers and acquisitions as well as technology licensing. The Thouvenin TMT team has been ranked by Chambers & Partners and legal 500.

More detailed information and further Newsletters can be accessed at www.thouvenin.com