Cloud computing

Bc. Ondřej Švehla, demonstrator, Faculty of Business and Economics, Mendel University, dukeeenho@gmail.com

Abstract
This article deals problematic of the cloud computing. In the article is described general cloud computing as first. Further, article gradually summarizes law norms and aspects, which limit the cloud computing. The article summarizes also the various models in the importance model as a service, which provides a service on physical and software layer. And in conclusion the article includes a list of cloud providers that are depending on these models.

Key Words
cloud computing, models as a service, cloud providers, norms of the cloud, low of the cloud

Introduction
Cloud computing, or something being in the cloud, is an expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Cloud computing is a term without a commonly accepted unequivocal scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user—arguably, rather like a cloud. [1]

It can be simply said this way. Cloud computing is the sharing of hardware and software resources over the network. Figure 1 displays principle of the cloud computing, where the cloud provides services such as are collaborations, communications, finance etc.
Objectives and methodology
The questions arise with using services of cloud computing, how legally deal a relationships and emerging issues in this problematic. Because laws not exist to relationships in the cloud computing, questions are solved concluding contracts with relevant contractual terms and conditions. The most vulnerable points in the cloud computing are the issues of legal data protection and especially protection of personal data.

The relationship between cloud providers and the clients may have in principle three forms:

- Customer is physical person - not an businessman, which acts as the end user. In this case, the contract arises between the provider and the physical person, who is the consumer. Terms of inception contracts concluded by electronic means are secure by adjusting of the consumer law.
- Customer is businessman - which acts as an end user, and use the Services only for their own purposes. It is the most widely used model on commercial plane.
Customer is an businessman who uses services of cloud computing and the outcomes of these services offers third party. Here comes some questions that need to be treated. It is a questions of copyright, liability, etc.

**Subject of the contract SaaS**

The contract between the client and the provider is innominate. The subject of contract can be for example, a obligation to available the software, grant the rights necessary for its use (license) and ensure its availability. An essential part of the contract for the provision of SaaS is SLA (Service Level Agree) regarding the guarantee of service availability. Given the sensitivity of the data stored in the cloud is also advisable to close the SSLA (Security Service Level Agree). This condition should include an obligation of provider services of the cloud computing to perform the defined security measures and guarantees. Basic requisites of the contract for the provision of SaaS can be summarized as follows:

- The right to use the software, which is located at provider servers
  The customer does not solve the question of hardware, for it is fully responsible the provider. The right of use is allowed by license.

- The right to use the server space of provider
  This is absolutely key provisions of the contract, when the customer must have under the sanction in the form of contractual penalties ensured that you always have access to your data, that will not be misused and will be anytime transferred to the servers specify by the customer.

- The obligation to pay the price SaaS
  Price depends both on the type of cloud services, so from guarantee of the availability SLA and agreed or required of server space.

- SLA (Service Level Agree)
  Provider of SaaS guarantees the availability services of software and is responsible for damage caused by unavailable their.

- Secrecy and manipulation with data of customer
  Provider must be bound by the strictest confidentiality obligations, so that client data were not disclosed to third parties or otherwise misused. Breach of this duty should always be sanctioned contractual penalty.

- Support of software services
User has guaranteed support from the provider, whether in the form of a Help Desk or in a form immediate upgrade used software after it is released from the software manufacturer.

So Cloud Computing could be legally treated as a whole, it must be divided into several areas of law, namely:

- Specification of performance and price
- Guarantee and liability for defects
- Liability for damages
- Data and data backup
- Confidentiality
- Security
- Personal information (or data protected by specific legislation)
- Governing law and dispute resolution

**Data and data backup**

When Cloud computing using can customer lose track about where his the data is located and how they are secured. In order for a provider of cloud with data could not do what he wants, are introduced into the contract the contractual conditions (liability, sanctions, security, etc.).

But under conditions, that data are declared as trade secrets. It sou data:

- are not in the pertinent business rings normally accessible.
- have be in secret by will of businessman.
- businessman adequately ensures their confidentiality.

When using services of cloud computing, in which the customer has placed their corporate data in the cloud, should take care to treatment of archiving and access to archived data. Entrepreneurs are according to legislation obliged to archive many documents and data over a period of time. The most important legislation, which include the obligation to archive documents are:

- Act No. 499/2004 Coll., about the archival and records management,
- Act No. 563/1991 Coll., about accounting,
- Act No. 582/1991 Coll., about the organization and implementation of social security
Personal data

The issue of protection of personal data in connection with the use of cloud computing is one of the most important topics. Especially because the customer is not the ruler of their data and this data are stored on servers around the world.

Proactive obligations of the contractual parties

The law on the protection of personal data, provides a number of obligations that have proactive nature. The customer and the provider are especially obliged to take measures to prevent unauthorized or accidental access to personal data, their alteration, destruction or loss of, unauthorized transfers or unauthorized processing or abuse, which is not explicitly mentioned in the statutory definition (§ 13 paragraph 1 of the Act on the Protection of personal Data). Both contractual parties should take technical and organizational measures. First of all, the customer must specify the purpose of the processing of personal data and the principles of their processing. Technical measures is a way of security data or their means of delivery (encrypted access to applications, pseudonymisation of data, etc.). Technical and organizational measures may determine the service provider or the customer.

According to Article 17 paragraph 2 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the customer must choose such provider that provides sufficient guarantees with regard to the technical and organizational measures. The customer is even obliged to ensure compliance with those measures. This is done adequate contractual regulation and guarantees.

The Law on the Protection of Personal Data says a lists of the duties of the client and the provider in the automated processing of personal data, which include the obligation:

- Ensure that systems for automated processing used only by authorized persons.
- create electronic records that enable identify and verify who and why personal data were recorded or otherwise processed.
- Prevent unauthorized to access to data carriers.

Regulating the transfer of personal data abroad

The European legal regulation of personal data is based on the principle, that personal data can be move freely within the EU Member States, with the condition to conserve all obligations to their protect. The personal data can be moved without permission of data owner in to third countries only exceptionally. The legal regulation of personal data pay particular attention to the countries, to which personal data are transferred. These countries have to create sufficient guarantees for special protection of personal data.
Scalability of the Cloud Computing is mainly provided by support the use of parallel servers and capacities. This feature brings one aspect that is in direct conflict with the requirements for limiting the transfer of personal data outside the EU Member States. Data can be move as customer required without control, and can cause storing of servers anywhere. This is a fundamental breach of regulation of personal data. Therefore it's recommended for customer that you negotiated limits the jurisdiction in which the provider may use servers. [2, 3]

**Results**

Cloud computing providers offer their services according to several fundamental models, such as the:

- **IAAS** – Infrastructure As A Service
- **PAAS** – Platform As A Service
- **SAAS** – Software As A Service

These models are the most widespread. The next model used is XaaS, which was published in 2009. This model provides services such as Strategy-as-a-Service, Collaboration-as-a-Service, Business Process-as-a-Service, Database-as-a-Service. Models network as a service (NaaS) and communication as a service (CaaS) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models in 2012.

The model IaaS is usually labeled as basic/lowest layer from above models. This model provides physical sources (scalable infrastructure) or virtual machine. The user pay for only sources, which uses. This sources are for example storage system, servers, network (VLAN), computing capacity etc.

The model PaaS delivers a computing platform. It mean, that this model typically provide development tools, databases, web servers etc. This model used mainly of software developers. Some Paas models provides dynamic allocations of sources by performance of applications.

The model SaaS provides users access to apps and databases, such as e-mail, virtual desktop, communications, CRM software etc. The cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. Cloud applications are different from other applications in their scalability—which can be
achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand. [1]

**Discussion**

Providers of cloud services exist many currently. But do not all providers provide services in the all domain of cloud. Therefore, the above models is good connect with these providers. The figure 2 shows the largest world providers of cloud services. Providers of services in model IaaS are for example:

- Amazon
- Hewlett-Packard
- Microsoft

Providers of services in model PaaS are for example:

- Google App Engine
- Oracle

Providers of services in model SaaS are for example:

- Drop box, IBM
- SAP

![Figure 2 Cloud providers](image)
**Conclusion**

The purpose of this article was briefly summarize the problematic of cloud computing. Further, this problematic has been briefly summarize from the aspect of law. Further, this article describes a forms of legal relations of cloud computing. Further, the article describes basic requisites of the contracts for providing SaaS services. The article also describes vulnerable points in the cloud computing, such as the issues of legal data protection and especially protection of personal data. At the conclusion would be good say this thought. User has not full control on the technologies, that are used to provide services. Therefore, user should been careful, when working with provided services and with data.

**References**