Records in the Cloud - Switzerland

Research paper done by:

Marion DESTRAZ

Arina GRAZHENSKAYA

Aurèle NICOLET

Lucie PETRELIS

Under the direction of:

Dr. Basma MAKHLOUF SHABOU, PhD.

Geneva, 18th January 2016

Haute Ecole Spécialisée de Suisse occidentale

Master in Information Science

Haute École de Gestion de Genève (HEG-GE)

Déclaration

Ce mémoire de recherche est réalisé dans le cadre du Master en Sciences de l'information de la Haute école de gestion de Genève. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans ce travail, sans préjuger de leur valeur, n'engage ni la responsabilité des auteurs, ni celle de l'encadrant.

« Nous attestons avoir réalisé le présent travail sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Declaration

This research paper has been realized in the context of the Master in Information Science of the University of Applied Sciences of Western Switzerland - School of Business Administration. The student accepts, if necessary, the confidentiality clause. The use of conclusions and recommendations formulated in this word, without presuming of their value, engages neither the responsibility of the author / authors, nor that of the professor.

"We attest that we realized the present work without using any sources other than the ones cited in the bibliography"

Fait à Genève, le 18 janvier 2016

Arina Grazhenskaya

Marion Destraz

Lucie Petrelis

Aurèle Nicolet

Acknowledgements

In the realization of these works, we received support from many people.

For the impression of the scientific poster, our thanks go to Mr. Claude Destraz,

For the time they gave us and the kindness with which we were received, we thank all of the people who accepted to answer our questions,

For tutoring us during the whole process of this project, we thank Dr. Basma Makhlouf Shabou.

Executive summary

The purpose of this research is to study all the necessary aspects in order to implement the cloud computing project “Records in the Cloud” in Switzerland. “Records in the Cloud” is a collaboration between several universities, aiming to study management, operational, legal, technical issues on cloud computing, as well as clarifying policies and procedures in order for a provider to implement cloud services while understanding risks and benefits.

Qualitative research was used in this study. It is composed of a state of the art, followed by the collection of primary data in the form of six interviews with Swiss cloud services providers. During these two parts of the research, the Swiss cloud was examined under five different aspects: managerial, economic, legal, security and technology.

Results show that Switzerland is not particular in regards to managerial and technical aspects. However, Swiss legislation, specifically concerning data protection, makes Switzerland an attractive country to host data, a fact that has not escaped the providers. It allows for better security, a that is a sales argument for some of them.

A set of good practices was concluded from these results. First, the use of open source solutions is unanimously supported by providers. Data security is an important point for many cloud customers and is becoming more and more of a concern for them. A cloud provider needs to be aware of those concerns and able to address them. The legal situation of Switzerland can be an asset in this matter, as well as the country’s reputation as a safe and stable place to have your data stored. Finally, cloud services are constantly evolving along with the technology that supports them and providers needs to be aware of the quick changes in the domain.

As a next step, research focusing on the customers of Swiss cloud services, whether Swiss or international, is suggested.

Keywords: cloud computing, Switzerland, information security, Records in the Cloud, data management, data protection, cloud providers

Table of content

List of figures

1. Introduction

1.1 What is cloud computing?

In 2011, the National Institute of Standards and Technology defined cloud computing as:

> *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Mell, 2011)*

It is composed of five main characteristics:

- On-demand self-service
- Broad network access
- Resources pooling
- Rapid elasticity
- Measured service

This study relies on this definition, but will allow for imprecisions when dealing with cloud professionals or services defining themselves as cloud computing, even though they might not match this definition absolutely.

As a result of the dot-com bubble burst in the beginning of the 2000s, many Internet companies started looking for "more efficient solutions for data storage and general IT architecture" (Baird, 2015). By 2006, Amazon launched the Elastic computer cloud (EC2) with the first real public utility computing service that had been envisioned a decade earlier (Sandholm, Lee, 2014). Since then, a shift has started in the computing landscape, where cloud computing is becoming an increasingly popular choice for many organizations (Askhoj, Sugimoto, Nagamori, 2011). Being able to host multiple users or tenants on the same infrastructure allows the provider to utilize the resources more efficiently and thereby increase the return on investment (ROI). This win-win relationship between users and providers is the reason most companies switch to cloud architectures (Sandholm, Lee, 2014).

If cloud computing has many benefits, like cost reduction, it also implies risks. The most important of them is the loss of control over data. By putting its data on the cloud, the organization accepts the risks of having it in a foreign country which other data protection laws, of IT outsourcing from the provider or of vendor lock-in issues (Switzerland, 2014).

1.2 Records in the Cloud

Initiated in 2012, Records in the Cloud (RiC) is a collaborative project between several universities of North America and Europe and "supported by a Social Sciences and Humanities Research Council of Canada (SSHRC) Insight Grant" (Records in the Cloud, 2015). Its purpose is to enable small and medium-sized organizations which cannot afford a full-fledged digital recordkeeping and/or records preservation system, to decide what is the best way to ensure that their records, or the records of others entrusted to them, will be safe, accessible, trustworthy, and under their control by developing the knowledge supporting such decision (Recordsinthecloud.org, 2015).

2. Objectives

The Records in the Cloud - Switzerland research project seeks to study all the necessary aspects in order to implement the cloud computing project “Records in the Cloud” in Switzerland. Switzerland, as a country, has the particularity of being divided into 26 Cantons under one Federation. The Cantons are split into three linguistic areas where German, French and Italian are spoken. Since the German and French part sums up the 85% of the Swiss population, our study will be focused on those two geographical territories.

The main purpose of this study is to suggest a set of good practices related to the use of cloud computing in the Swiss context.

In this purpose, five main objectives will be studied:

1. Describe the managerial aspects and risks of cloud services in Switzerland
2. Describe the economic aspects and risks of cloud services in Switzerland
3. Describe the legal aspects and risks of cloud services in Switzerland
4. Describe the security issues and challenges of cloud services in Switzerland
5. Describe the technological and technical aspects and risks of cloud services in Switzerland

By managerial aspects we mean a broad range of issues related to communication and relations between customers and cloud service providers, including: examination of possible cloud solutions and cloud service offerings, determining if the service offered meets the business and technical requirements of the customer; negotiating the terms for the cloud service and accepting the contract for the cloud service.

By economic aspects we mean the relation between cloud computing providers and their customers, the pricing of cloud services, the economic benefits and drawbacks of cloud computing for companies of various sizes and the economic particularity of cloud computing compared to other goods and services.

By legal aspects we mean information pertaining to legislation, Swiss or international on cloud computing and the issues linked to cloud computing, including the sharing of data.

By the term security issues, we mean everything involving: Security of data, violation of security, security concerns and threats, security tools, cloud security evaluation, the cloud Security Alliance (CSA)

By technical and technological aspects, we mean everything about Information Technologies used by cloud computing, like virtualization or monitoring tools.

These five aspects were chosen after a first foray into the scientific literature on the subject of cloud computing, as we think they encompass all issues related to cloud computing. Even though some issues may overlap on two or more aspects, this separation into five precise aspects allows for a more precise analysis of the data.

3. Methodology

Our study was conducted in two parts: a review of the literature, followed by a series of semi-structured interviews with various cloud service providers in Switzerland. The data collected from these interviews was then analyzed.

3.1 State of the art

The literature review has been conducted following the five axes that structure our whole study: managerial, economical, legal, security and technical issues were looked at separately and each article or book we read was described according to what issue or issues it was relevant to. Furthermore, each issue was subdivided into four parts depending of the scope of the text. Those parts are: international, Switzerland as a whole, German speaking Switzerland and French speaking Switzerland. Sources were found in diverse websites, including:

- LISA/LISTA, to discover resources and research in the library and information sciences domains
- Google Scholar, to find out the most recent studies on the subject of cloud computing, whether Swiss or international
- Réro Doc, to keep an eye on Swiss research in the domain of cloud computing
- ICT journal, to keep in touch with the evolution of the cloud computing market

It quickly became apparent that some aspects have not been examined in a specific Swiss angle. This is especially the case for the technical and technological aspect. It also became apparent that there was no notable difference between the French speaking and the German speaking parts of Switzerland.

We concentrated most of our efforts on this part of the study early on, so as to get a better view of cloud computing as a whole. However, we kept on reading on the subject during the whole duration of the project. The result of this study is an annotated bibliography that is separate from the present report.

3.2 Interviews

Based on our first foray into the literature, we devised an interview grid that we would use for every interview. As the interviews would be held with different kinds of cloud providers, some offering only an IaaS while others would be more PaaS, some of the questions were not relevant to every provider. However, for reasons of reproducibility, we chose to not have multiple grids but to use the same every time, skipping some questions if necessary. Like the state of the art, the interview grid was built around the five main themes. It also included a series of introductory questions to get to know the person interviewed and the company, and a few general questions allowing the interviewee to give their own opinion on cloud computing as a whole and on its evolution over time.

We aimed to interview eight cloud providers: four in the French speaking region, and four in the German speaking region. We reached out towards twenty-one different providers, which we chose according to two points: first geography, so that the interviewers could attend meetings easily. We chose interviewers close to Geneva for the French speaking region, and to Zürich for the German speaking region. These two cities are also two of the main Swiss

trade centers which is why most cloud providers are based there. Secondly, we chose providers that were either entirely Swiss, or which had been founded in Switzerland, disregarding international providers with a branch in Switzerland, so that we could get a complete Swiss point of view on all questions on cloud computing. We did not set a definition of what we considered cloud computing and cloud providers to be for these interviews, but instead reached out to any companies who defined themselves as cloud services providers and who offered something they called cloud computing, so that we could get a better grasp of what exactly “cloud computing” means to Swiss professionals.

A consent letter, stating that all interviews would be recorded and that anonymity would be respected, was sent to all providers prior to the interview. All interviewees agreed to sign this consent letter before starting to answer our questions.

Among the twenty-one providers contacted, only six ultimately accepted to be interviewed. Others either did not answer at all, or answered asking for more details, which were provided, and then stopped answering our messages. One provider was willing to answer questions but could not find a date before the end of the period set for interviews.

While six interviews are less than expected, all interviewees were eager to help and all meetings were allowed to go for their full course. On average, interviews lasted for an hour, with some being over in forty-five minutes while other went for an hour and a half. All interviews took place in the offices of the provider. Interviewees were all men, of various ages, and all had a higher position in their company - CEO, head of cloud teams, system engineer, etc. Two students were present to all interviews whenever possible, with one group of two students interviewing German speaking providers and the other two interviewing the French speaking providers. When not possible, one student was present in person and a second one participated over Skype. This allowed students to compare notes and make sure the interview went smoothly. One student was responsible for each interview, but students sometimes shared the questions.

Providers were supplied with the questions beforehand, but some declined to have a look at them.

Each interview was recorded, and the recording was shared with the whole group. Each interview was also transcribed. Four were in English. Two providers in French speaking Switzerland were more comfortable answering in their native language, so these two interviews were conducted in French. The transcriptions were then translated into English.

Providers were promised anonymity and the names of the person interviewed as well as that of the enterprises will not be used. Here is an overview of who the providers interviewed are:

- Provider 1 is a small, relatively new provider which only offers Infrastructure as a Service (IaaS). This company has always been a cloud provider and nothing else.
- Provider 2 offers IaaS and Software as a service (SaaS) services. Before working in the cloud, the company has been active in IT and computer sciences and has been collaborating with various higher education institutions in Switzerland for about thirty years.

- Provider 3 is a large enterprise that has been offering telecommunication services, then internet services, for a long time before adding cloud services to its catalog. It proposes IaaS and Platform as a Service (PaaS) to a wide array of clients.
- Provider 4 is a SME that's been active in the telecommunication business in Switzerland for about 25 years. As it evolved, it started offering physical hosting, then cloud hosting in the form of IaaS.
- Provider 5 is a small company created about five years ago, that offers cloud services only. It proposes IaaS and PaaS to a wide array of clients.
- Provider 6 is a medium sized enterprise that has been active in the Swiss IT market for about twenty years. It offers IaaS and Paas services.

3.3 Interview Analysis

For the analysis, each student once again focused on one of the main themes previously outlined. This was made easier by the structure of the interview grid, with questions being grouped according to the theme, but sometimes the interviewees expanded on their answer and touched on other themes than the one aimed at by the question. Sometimes, they also interpreted the questions in different ways. It is possible that, since English is none of the researchers first language, some of the questions were not precise enough. Most people interviewed also answered in their second or third language and may have had some difficulties in expressing themselves. However, we chose to let the providers talk freely about what they felt was important so as to get as wide a range of answers as possible.

Results were shared with the group. Once again, we saw no difference between the French speaking and the German speaking parts of the country, in any of the main themes.

Originally, we planned to analyze the interviews using Nvivo, a data analysis software for qualitative research. However, due to technical constraint, we were unable to use the software. Therefore, all analysis was done by hand using only the transcript. To facilitate this, interview transcripts were divided into chapters according to what aspects the questions related to. Since interviewees sometimes talked about other themes than the one aimed at by the question, every aspect analysis had to check the whole interview transcript.

4. State of the art

4.1 Managerial aspects

At the international level, the issue of the contractual relationships between cloud providers and their customers is the most developed topic. Terms and Conditions offered by cloud computing providers were analyzed in a detailed survey published in 2010 (Bradshaw and al.). Some authors try to provide potential clients of the cloud services with practical recommendations in order to help them make informed decision (Oppenheim, 2012) and encourage them, particularly small and medium-sized enterprise users, to negotiate providers' standard terms to make them more suitable for their requirements (Hon and al., 2012).

There is a limited number of studies focusing on cloud computing in Switzerland in general, and there is almost nothing regarding managerial aspects in particular.

There are two official documents, or Policy Papers, developed in the framework of Swiss E-Government conception which describes the cloud solution strategy of the Swiss authorities from 2012 to 2020 (five main objectives), and outlines the needs and expectations of the Swiss Confederation regarding a cloud computing solution. These objectives include the progressive use of cloud computing in Switzerland, the adaptation of existing legislature and collaborations with companies and international environment regarding cloud computing (E-Government Suisse, 2012). They could get us acquainted with general and official state approach.

Switzerland has a reputation of the "particular" country. And it's not surprising that among such a limited amount of publication it was possible to find only one paper with analysis of such particularities, which may affect the perspectives of cloud services in the country (Rey, 2011). In particular, Swiss federalism and the relative autonomy of its more than 2500 municipalities, makes low-cost solutions like cloud computing potential very attractive. This is despite the fact that Switzerland does not have a strong IT tradition. However, the above conditions can be considered only as a kind of pretext for the development of relations "cloud provider-customer"

From this point of view, hopefully, our research could make a contribution to cover the lack of materials about existing practices.

4.2 Economic aspects

There are not many studies focusing on cloud computing in Switzerland on the economic aspect, however a few interesting points have already been raised.

First is the fact that cloud computing solutions are more attractive to SMEs than to larger enterprises. The flexibility of cost efficiency of cloud solutions is the cause (Brender, 2013). Switzerland is not unique in that regard, as pointed out by Hsu and Li-Hsieh, in their study of Taiwanese companies (Hsu, 2014): the different pricing mechanisms make cloud computing more of a benefit to SMEs and start-ups, because it allows them to not invest a lot in IT up front. Before the advent of cloud computing, IT solutions were adopted by largest companies first, as they were more expensive. This study also finds that "business concern is the most

important factor influencing the choice of deployment model, with higher concerns leading to private deployment options." (ibid)

The possibilities of modular payment reduce economic risks to SMEs and in 2014, in Switzerland, 58% of companies up to twenty-five persons used some kind of cloud services. This is more than the Western European average of 45% of companies.

> *"A new study shows that 58% of Swiss companies up to 25 employees claim to use Cloud Computing services, against 45% of companies in Western Europe." (Borner, 2014, our translation)*

However, another study from the same year points out that Swiss IT managers are, as a whole, more cautious when it comes to choosing a cloud computing solution than their colleagues in other European countries. (Badel, 2014). Interestingly, in 2012, French speaking Swiss IT managers saw cloud computing as an interesting opportunity. (Koller, 2012)

It is possible that Swiss SMEs are more eager than other SMEs to get into the cloud, while larger Swiss enterprises are especially cautious in that regard. However, as Nkidiaka (2012) pointed out, PMEs in Geneva may not have been ready for the cloud in 2012; not because they lack the money or technical capabilities, but because of a "conservative ideology" that makes them wary of changing habits that have been proved to work. A fear that Swiss enterprises will have to overcome, and might already have. As far as Swiss providers are concerned, it seems that cloud computing will inevitably become the norm in all enterprises in the future. Some compare it to the beginning of electricity:

> *"To measure the importance of the phenomenon, think of the beginning of electric power, in the 1890s. Before that, every enterprise produced its own electricity. Then networks were created and electricity became a service. Cloud computing is the same: the enterprise focuses on its activity and subcontracts its IT, which becomes a service accessible remotely through the power of today's internet connections." (Seydtaghia, 2014, our translation)*

More and more money will be spent on cloud computing services in Switzerland, according to another study (Brodar, 2013), and this should save money in the long run. Even though, as Nolle (2015) points out, going to the cloud is not an automatic money saver and enterprises need to carefully choose their provider according to the service level they need and to the pricing model proposed.

4.3 Legal aspects

4.3.1 Legislations

One of the most important problematic on cloud computing nowadays is its fast changing legislation. More specifically the fact that there still isn't a common legislation causes confusion among countries. Anthony Gray, in his study *Conflict of laws and the cloud*, compares Australia, the United States and the European Union legislations and points out the notion of conflict between national legislations which are based on territorialism. As international cooperation is missing, there is the need of common agreements. He points out three important questions to clarify on which the set of laws should be followed: 1) The legislation of the country the client is located 2) The legislation of the country the provider is located 3) The legislation

of the country the cloud is physically located (meaning the storage units) In Europe for instance, the regulations (EC) No 598/2008 of the European Parliament and of the Council on 17 June 2009 gives the right to the service provider to apply the “choice of law”. It means that he will most likely select the laws of a jurisdiction with more “friendly regulations”. On the same matter, Australia and the United States follows like this: the law of the place of performance, the place of contract, the location of the subject matter or the place of the business of the parties. Gray states at the last part of his study that in 2012 there has been a proposal on a unified legislation among EU countries (Gray, 2013).

The article *Political agreement on EU data protection* presents the political agreement made by the European Commission, the European Parliament and the Council of the European Union on the reform of EU data protection law. The voting took place on the 17th of December 2015 and will be used from 2016 and onwards. It consists of a General Data Protection Regulation and a Data Protection Directive which will be used by the police and the criminal justice sector. As far as Switzerland is concerned, the article explains that since the country is neither a member of the EU nor of the EEA, these new European directives won’t affect the Swiss data protection law. However, it will concern Swiss companies that will be making collaborations with clients within the EU where data processing will take place. Also, the EU data protection regulation will affect the reform of the still on process Swiss Federal Act on Data Protection (DPA). (Walder Wyss AG, 2015)

The Swiss Federal Data Protection Act of 19 June 1992, aims to protect the privacy and the fundamental rights of persons when their data is processed. In order to have all the details on the DPA, the website of the Swiss Government makes it available to everyone (Switzerland, 1992).

The DPA has the following structure:

1. Purpose, Scope of Application and Definitions
2. General Data Protection Provisions
3. Processing of Personal Data by Private Persons
4. Processing of Personal Data by Federal Authorities
5. Federal Data Protection and Information Commissioner
6. Legal Protection
7. Criminal Provisions
8. Final Provisions

The Swiss Federal Data Protection Ordinance (DPO) was adopted on June 14, 1993 by the Swiss Federal Council in order to implement the DPA. It entered into force on July 1, 1993. (Walder Wyss AG)

Since Switzerland has the particularity of being divided into 26 Cantons, it’s important to mention that each Swiss canton has its own legislation which regulates data processes by cantonal and municipal entities. Each canton has its own cantonal data protection commissioner which is in charge of these laws. (ibid)

As Switzerland is geographically located in the center of Europe, it is very much affected by the EU law. This is the reason why the Swiss data protection law is in the state of revision in order to be more aligned with the EU directives. As presented at The Privacy, data protection and cybersecurity law review (Schneider, Sturdy, 2015):

> *"The Swiss Federal Council has instructed the Federal Department of Justice and Police to submit a preliminary draft for a revision of the DPA by the end of August 2016 at the latest. The aim of this reform is to lay the foundations allowing Switzerland to ratify the modernised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and, to the extent this is necessary in the context of further development of the Schengen/Dublin acquis, the adaptation of the DPA to the EU data protection revisions" (p.316).*

This review is a very important asset to the Records in the Cloud - Switzerland project since it's presenting the most recent state on Swiss legislation and data protection in Switzerland. While describing every key definition of the DPA, the review specifies that: "Unlike the data protection laws of most other countries, Swiss data protection law protects personal data relating to both individuals and legal entities" (p.317). On the matter of international data transfer, any leak of personal data from Switzerland to another country has to be conform with the DPA. A list of countries (Switzerland, 2015), put in place by the Commissioner is available in order to be informed on the countries that have an adequate data protection level with respect to individuals. The countries that are following the EU Directive 95/46/EC are assumed to have a sufficient data protection. In case of a transfer of data to a non-EU or non-EEA country, there should be a case by case examination. (Schneider, Sturny, 2015)

It's reasonable to think that data protection is a crucial issue and is affecting many countries. Another important and very recent change was the invalidity of the Safe Harbor (or Harbour) Privacy Principles. After the declaration of the Court of Justice of the European Union on the 6th October 2015 on the cancellation of the US-EU Safe Harbor Framework, the Swiss Commissioner expressed the insufficiency on the legal basis of personal data transfer from Switzerland to the US. (Schneider, Sturny, 2015)

An article on Reuters explaining about the invalidity of the Safe Harbour, presents its use. Prodhan precisely says that "the Safe Harbour was a fast-track process that U.S. companies could use to comply with European data protection law, which prevents EU citizens' personal data being transferred to non-EU countries deemed to have insufficient privacy safeguards". (Prodhan, 2015). As presented in the article on The Guardian, it all started when an Austrian citizen made a request to the Irish data protection commissioner in order to investigate if the protection of the data transferred to the US by Facebook is adequate. The headquarters of Facebook are located in Dublin. (The Guardian, 2015)

4.3.2 Certifications

The possession of certifications is not mandatory for a cloud provider but it is a valuable asset for its clients. A certification represents the recognition that processes have been evaluated and followed.

4.3.2.1 DPCO

The Swiss Federal Ordinance on Data Protection Certification (DPCO) was adopted on September 27, 2007 by the Swiss Federal Council in order to implement certain provisions of the Data Protection Ordinance (Walder Wyss AG). The DPCO specifies that "The organizations that carry out data protection certification in accordance with Article 11 FADP (certification organizations) must be accredited". (Switzerland, 2007)

4.3.2.2 ISO

Until recently, security certifications specifically devoted to cloud computing didn't exist. Instead general security certifications were used, as the well-known ISO 27001 and also ISO 27002 (Cloud Security Standards Customers Council, 2013). ISO 27001 is a standard applied to all types of companies on how to plan, implement, monitor, review and improve a system on information security management. ISO 27002 is not a management standard but it is a collection of security controls, the same as found in ISO 27001 but much more detailed. You can't get ISO 27002 without having been certified first with the ISO 27001. (Kosutic)

In 2015, the first ISO certification on cloud computing was put in place. ISO/IEC 27017:2015 specifically concerns security controls for cloud providers and cloud customers. It is based on ISO 27002 security controls but it is focused on the cloud. A second certification on cloud is the ISO/IEC 27018:2015 which is about privacy aspects of the cloud (Hussainali, 2015) aiming an international approach on cloud data protection. (Saran, Cliff, 2015)

One important point of the ISO 27018 standard is that it suggests how to handle the Personally Identifiable Information (PII). The customers should be asking themselves how their PII has been obtained, stored and used by the cloud provider. This kind of data should be accessible only by authorized users within the company. In addition, these privacy policies should be included in the SLA contract. It's worth mentioning that depending on the services, the degree of responsibility of the provider on the PII differs. For instance, if a customer is using a virtual machine within an IaaS service, the provider doesn't have access to the data stored so he's not responsible for the data, other than the minimum data required from the client. And in the case of a SaaS service, the provider is the one responsible for the protection of the PII, especially if data is encrypted. One of the established framework, in relation to privacy and to the PII, was the US-EU Safe Harbor framework, mentioned above. (Cloud Security Standards Customers Council, 2013). In his article, Kemp says:

> *"In its first year, it is emerging that complying, and being seen to comply, with ISO 27018 is providing genuine assurance for customers in managing their data protection legal obligations. This reassurance operates across the continuum of Cloud services and through the procurement and contract lifecycle, regardless of whether or not any particular data is PII'. (Kemp, 2015, p.3)*

4.4 Security issues

We strategically selected to present security directly after the legal part because they are very much related. There wouldn't be any issue on cloud computing security if legislations on data protection and regulations were respected. There wouldn't be any trust issue if everybody was honest. So even though cloud computing offers many benefits to the users, security is a major concern.

4.4.1 Handling security issues abroad

When security measures are not properly followed, data operations and data transmissions are at a very high level of risk. Security challenges need to be identified in order to find appropriate solutions. At the International Conference on Intelligent Computing, Communication and Convergence (ICCC-2015) in India, major challenges on data security have been presented, with on top of the list “Data Segregation and Protection” and “Data Leak Prevention”. Three issues of security have been raised: Confidentiality, Integrity and Availability (due to downtime). As a solution to data security challenges, the option of encryption of the data was presented. This procedure makes data completely unusable, preventing access from unauthorized users. (Rao, Selvamani, 2015) In the review *Addressing Security and Privacy Issues in Cloud Computing*, important points on cloud security have been gathered. There are two main issues affecting the growth of cloud computing market and that is security issues from the providers’ side and from the clients’ side. (Kumar, Goudar, 2012) In order to improve security, trusted technologies should be used, which would be beneficial for both parties. There are three categories of threats: those studied by the Cloud Security Alliance, those concerning the location, and those coming from the network used. (Ashktorab, Taghizadeh, 2012) Interesting solutions have been described by the authors of this review, like for example the use of a data flow chart. This option allows IT managers to have the control on where the data is at all time, the location it is stored in and whether it is shared. They also suggest that in order to solve security issues, data isolation would be a solution where each customer's data would be isolated from one another. They also point out that threat prevention is very difficult to handle, due to the fact that the cloud takes place in a shared environment on a shared infrastructure. (Sinjilawi, Al.Nabhan, Abu Shanab, 2014) As they mention in their review, based upon the article of Merabti and Kifayat, in the matter of data transfer between countries while dealing with local regulations, the anonymity of information would be a solution, insuring data privacy and security. (Younis, Merabti, Kifayat, 2013) One other issue mentioned on security is the risk of multi-tenancy, which may lead to data visibility between users. (Fernandes, 2014)

An important aspect on the matter of security is the lack of trust between providers and clients. Xu Wu believes that:

> *“Trust is a critical part of the process by which relationships develop. It is before-security issue in the ad hoc networks. By clarifying the trust relationship, it will be much easier to take proper security measures, and make correct decision on any security issues.” (Wu, 2015, p.177)*

The most critical threats on security are data integrity, user confidentiality and trust among different parties - providers, users and users group. Each service offered has different security demands. The SaaS requires all protection to be set at all levels. IaaS requires protection at the networking, trusted computing and storage levels. And PaaS requires the same protection as IaaS but also protection at the resource-management level. (Hwang, Li, 2010)

In their paper, Sun et. al. presents the most important aspects of security, privacy and trust issues on the use of the cloud. They divided the security issues into six sub-categories that need to be solved: 1. how to provide safe mechanisms, 2. how to keep data confidentiality 3. how to avoid malicious insiders 4. how to avoid service hijacking 5. how to manage multi-

instance in a multi-tenancy environment 6. how to develop appropriate law and implement legal jurisdiction. On privacy issues they present four sub-categories that need to be addressed: 1. how the users could have control of their data while stored in the cloud, 2. how to avoid data leakage and unauthorized modifications when replications are made in order to secure the data's integrity, 3. who is responsible of personal information provided by the client, 4. how to make sure that sub-contractors are identified, checked and ascertained. When talking about trust issues, they explain that "trust is the most complex relationship among entities because it is extremely subjective, context-dependent, non-symmetric, uncertain, and partially transitive". (Sun, et al., 2001, p.2854)

4.4.2 Handling security issues in Switzerland

In one of the very few existing articles devoted on cloud computing in Switzerland, Markov and Brender presents an empirical study on the adoption of public cloud from Swiss companies. Regarding the security of data during its transportation, the result of the study shows that the best protection against malicious attacks is data encryption and data anonymization. It's also mentioned that the security practices of the customer and the security practices of the provider should be on the same level, having an equal importance. In the same study, attention is given to the standardization of the service level agreement (SLA) when referring to the security of financial transactions. Also, when presenting the threat related to physical security, it is being said that even though physical intrusion is very much possible due to the decentralized resources, natural disasters can be an even bigger risk, severely affecting the state of data centers. (Brender, Markov 2013)

In their paper on issues on cloud computing in Switzerland, the attorneys of BCCC say that in Switzerland the public sector is skeptical of implementing cloud services, especially for security and legal reasons. The Swiss Government is putting in place an eGovernment strategy including cloud computing services. The biggest concerns are on data protection, confidentiality and security related to IT. The Federal Data Protection as well as the Commissioner points out in their guidance document that the user of the cloud computing has a big responsibility on his data. (Métille, 2013)

When referring to the security of data, the Commissioner of Switzerland orders that personal data should only be process by a provider based on an agreement or on the law. He also says that "the assignor must ensure that the cloud service provider guarantees data security" (Article 10a Paragraph 2 DPA). (Schneider, Sturny 2015)

4.4.3 Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) offers guidance and recommendations in order to diminish the possibility of risks on cloud computing security issues. CSA is a leading organization put in place by volunteers all around the world aiming to offer best practices in order to assure a secure cloud environment. This framework has security controls trying to cover as many areas as possible. As seen in the cloud security alliance guide (Cloud Security Alliance, 2009), it's a quick method for evaluating tolerance for moving an asset to various cloud computing models. We should understand what kind of material we decide to put into the cloud. Since 2010, the CSA provides the first cloud security user certification, as a benchmark for professional competency in cloud computing security. It offers two certifications: CSA Security, Trust and

Assurance Registry (STAR) and Certification of Cloud Security Knowledge (CCSK). (Cloud Security Alliance)

4.5 Technology aspects

First of all, it appears to us important to note the difficulty to make a state of the art on Swiss technological aspects, because, generally, the technology relies on international standards which differ little from one country to another and the cloud computing components tend increasingly to be standardized.

Moreover, the elements about security, such as data encryption, constitute an overlap with security aspects, already treated in the preceding point.

That is why we choose to focus on several points which appear us to reflect the issues of cloud computing's technological aspects in Switzerland:

- the growth of the open source's adoption
- the interest in the containerization
- the issue of cloud computing energy consumption

4.5.1 The growth of the open source's adoption

Several Swiss providers choose to give priority to open source. For example, Swisscom, one of the company which succeeded to the state-owned PTT (Post, Telegraph and Telephone), use an open source environment for his PaaS and, since August 2014, deeply collaborates on the source code and finally has, since February 2015, a seat in the Cloud Foundry Foundation committee (Swisscom, 2015), which deals with the "development of the Cloud Foundry, an open source industry standard platform for cloud applications" (Cloud Foundry, 2016).

Another open source software, Docker, encounters a growing success in the world and also in Switzerland. Several Swiss providers use it and a community grows around it (Praa, 2016). Docker simplifies the creation and the deployment of containers.

4.5.2 The interest of containerization

The containerization is an "operating system-level virtualization" (Wheeler, David A., 2015). Contrary to the hardware virtualization, the containerization does not make "a full copy of the operating system along with the various libraries required to host an application" (Wainewright, Phil, 2014.) as illustrated in the diagram.

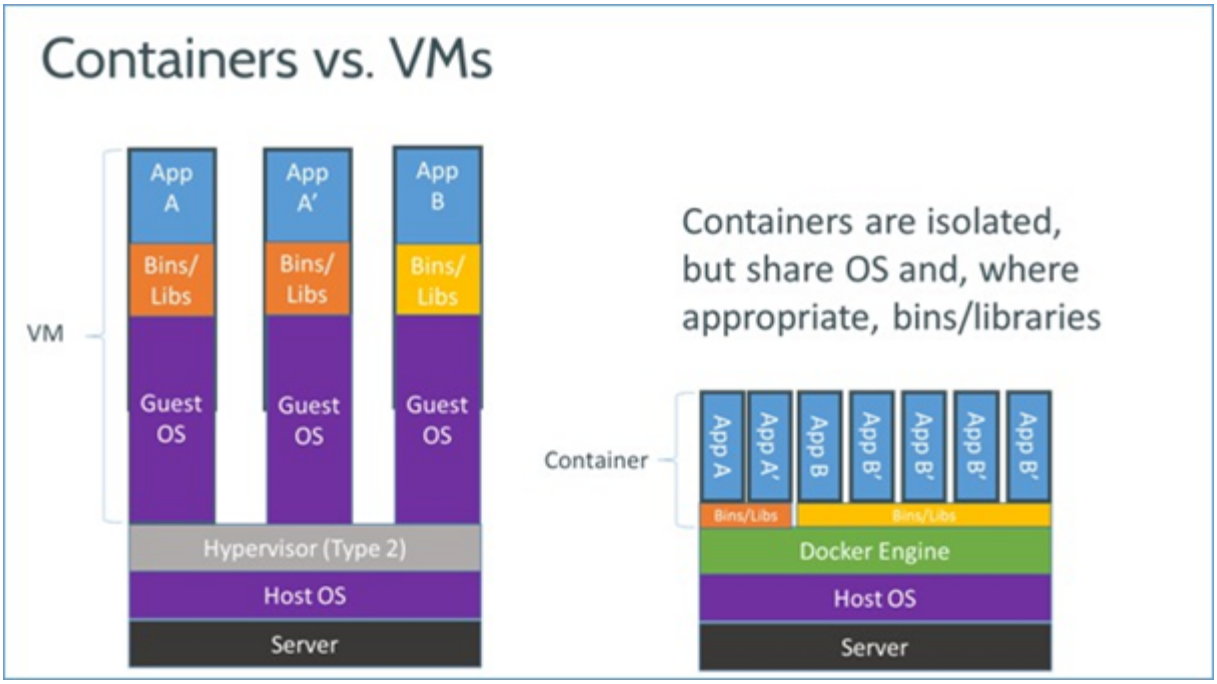


Figure 1: Wainwright, Phil, 2014

4.5.2.1 Its advantages

By avoiding resource redundancy, such as guest OS or libraries, containerization is lighter, resulting in a rapidity of processing and, hence, being “much more efficient than full hardware virtualization” (Wheeler, 2015).

Moreover, the scalability, one of cloud computing’s five characteristics, is improved, because the container installation is “much less as compared to VMs” (Gupta, 2015, p.3).

4.5.2.2 Its flaws

However, the container’s utilization has not only advantages, but also flaws. The main one is to reduce security. Indeed, one important security component is to isolate data. Although the container remains isolated from underlying host, “the separation is not as strong as that of VM”. (Gupta, 2015, p.3)

4.5.3 Cloud computing energy consumption

It is known that cloud computing needs a lot of energy. Generally, we think especially about datacenters, but this is just the tip of the iceberg. According to a study of the Centre for energy-efficient telecommunications (CEET), 90% of wireless cloud’s consumption “is attributable to wireless access network technologies, data centres account for only 9%” (CEET, 2013). In the future, the link between cloud computing and wireless will be stronger, because the “demand for enterprise mobile apps will outstrip available development capacity five to one” (Gartner, 2015). Internet of things and mobile devices need wireless to access cloud computing services.

Faced with this issue, solutions to reduce or control the energy consumptions are sought. In Switzerland, The InIT Cloud Computing Lab, from Zurich University of Applied Sciences, looking mainly into cloud interoperability and open cloud computing interface standardization (Tmb, 2012.); but it also has projects about energy efficiency of cloud computing. One of them is concerned with “understanding cloud energy consumption”.

Started in January 2014, Arcus is a project internal to the InIT Cloud Computing Lab “which focuses on correlating energy consumption with cloud usage information to enable a cloud provider to understand in detail how her energy is consumed” (Murp, 2014.).

The main goal is to offer a tool which will allow a provider to see the relationship between the energy consumption in the system and how the systems are used. “Developed to be totally integrated with Openstack” (GAEA, 2014), the tool is now available on GitHub.

5. Interview analysis

5.1 Managerial aspects

5.1.1 Contracting

Speaking with the providers about managerial aspects of cloud computing, first of all we asked about their contractual relationship with customers to find out what kind of contracts are used in their practice and (perhaps most importantly) if the company is ready to negotiate them.

All providers prefer to work with one type of Service Level Agreement (SLA) with a single set of terms and conditions. And most of them have pointed out the increasing demand for standardization.

> *"… we see with the new generation - demand for SLA. One Standard SLA for everybody". (Provider 2)*

Such a tendency can be explained by the global nature of the cloud. SLAs usually span many jurisdictions, with often varying applicable legal requirements, in particular with respect to the protection of the personal data hosted in the cloud service. Swiss cloud providers are well informed about the last European initiatives in the field of SLA standardization. They have expressed their readiness to incorporate it in the future, but without enthusiasm. However, some providers already had such an experience of adapting their SLAs to the customer's requirements:

> *"…we do this for our German customers already… with addendums regarding the data protections. Because Germany is quite advanced regarding personal data protection, so we require set a documents that neither Swiss nor other jurisdictions taking place." (Provider 1)*

In spite of the prevailing opinion, that supposes that most cloud services offer are in general non-negotiable (Oppenheim, 2012), generally speaking, Swiss cloud providers are ready to negotiate and integrate the interests of the customers.

Only one of the biggest providers (Provider 3) announced its principal disagreement to discuss the terms of the proposed SLA with different clients.

Others have shown greater flexibility. However, almost every provider has its own approach, which determines his willingness to negotiate SLA and takes into account various factors (size of the provider, size of the customer, complexity of the project and etc.):

> *"…we cannot manage having different SLA with every single customer because they might have a small instance, let's say 70 CHF per month and if you have to talk to them about special SLA's it will be a nightmare. But for other companies like PWC, it's not a secret I can say that… they just take our SLA as the bases and then they add just a few points that are important to them. And then if there is, you know, nothing unusual, if it's something logical we agree to that and we sign it." (Provider 5)*

However, despite the general trend with standard contracts, some providers retain the practice of "particular contracts with privileged clients" as we were informed by the Provider 6.

5.1.2 Information governance practices

In the frameworks of our research we also wanted to find out if Swiss cloud providers contribute to support customers' information governance practices.

When we asked them about it, most of the respondents have asked us to clarify the question. Furthermore, reflecting on this topic, they have expressed a common vision of the situation: if the data remains the property of customers - it's their responsibility to manage it:

> *"I'll say, everyone is free to manage their data. If they ask us for help we can offer it, but it's very rare". (Provider 4)*

Cloud providers are ready to help customers with support, but on customers' request only. They could also provide customers with required guidelines:

> *"We certainly give guidelines. That's a nice offer… we can forward this to customers and tell them the procedure, what they need to do inside the company." (Provider 1)*

Only Provider 3 (the biggest one) gave his answer immediately: "Governance is real important stuff". In relation to this type of service the company acts as outsourcing provider (outsourcer) and has appropriate international certificates for this activity.

Nevertheless, we can conclude that most providers are not currently participating in the process of information governance.

5.1.3 Service implementation: before, during and after

A significant number of questions concerning the various aspects of the provided services (from the moment of its testing and transferring of the customers' data into the cloud until the termination of the contract) have been posed to find out if Swiss cloud providers meet the business and technical requirements of the customers.

Getting ahead, we can say that in general Swiss cloud computing could be characterized as customer friendly.

Trial experience (before signing of the contract) is available for all clients.

At the same time several providers see an advantage in the possibility to try the service without getting in contact with cloud provider. They have pointed out the necessity to simplify the direct access to the testing trial. One of the providers sees the difference in this relation between USA and European cloud services:

> *"…many providers or products that come from the USA they are a step further than Europe. It's normal that you have a free trial and that you can try a product without having to contact a sales guy... Everybody is a «cloud provider», but when you want to get in details, it says "please contact us" and then you have to talk to a sales guy and then blablabla". (Provider 5)*

During the testing phase most Swiss cloud providers are ready to propose to their customers monthly free credits.

Implementation timeframes within a customer' company depends of its size, internal management cycle, complexity of the implementation, business software and many others technical issues.

Therefore, the timeframes of implementation can vary from 30 seconds to several years:

> *"Just go on-line, register and account in 30 seconds you wholly have a virtual machine of storage running with us" (Provider 1)*

> *"…the processes, for big businesses, can take up to three to six months. For the small ones, there is less information, less things to take care of, we close the deal more quickly..." (Provider 4)*

> *"If you are really in a big company… So let's talk about, example: Swiss television. Swiss television starts the journey to the cloud and they are now learning how to handle with the cloud and they plan to migrate all their systems into cloud…within the next four years". (Provider 3)*

5.1.3.1 Implementation methods

The methods of technical implementation: big-bang (all at once) or a slow roll-out also depend on the customer's decision.

But almost all Swiss cloud providers prefer and use slow roll-out. One of the providers shared with us his own statistics: "So I would say 20% big-bang and 80% slow roll-out." (Provider 5)

5.1.3.2 Deployment mechanism.

We have asked cloud providers about their participation in deployment of the services. Those who positioned themselves as SaaS providers are usually in charge for the entire deployment mechanism. Many customers ask about this type of support.

> *"Most of the time we do soft transitions. We migrate. First, there are what we call "proof of concept", which means we build a test infrastructure so we can tell them: that's what it would look like, do we all agree? And little by little, we build a complete infrastructure…" (Provider 4)*

And from the other side, providers see that many customers do not have a sufficient level of technical skills to make deployment themselves. (Provider 5).

5.1.3.3 Training of the staff

Swiss cloud providers are ready to propose their customers all required guidelines, supportive documentation and training sessions or webinars (if requested) as they see this as a part of the "Professional service" (Provider 3).

5.1.4 Data Hosting

Running ahead, we can make the main conclusion: Swiss cloud computing is hosted in Switzerland...and exclusively in Switzerland. Currently, this is the basic requirement both for the customers (Swiss and international) and providers. Swiss cloud providers are ready to guarantee that customers data remains in the country. And this is crucially important for data control and protection issues:

"The reason is not the cost, because I think it would be much cheaper to do it somewhere else. No, the reason is so we can control the data." (Provider 4)

In their hosting practices, cloud providers use from 2 to 6 datacenters. Some of them are the owners of the datacenters, some providers just rent a Rackspace. Generally speaking, datacenters locations are determined by geographical separation, political aspect and by international recognition. There is also a technical reason:

"When we need to move a machine, after it breaks or something like that, ideally it has to be as close as possible" (Provider 6)

Most datacenters are located in the Zürich and Geneva regions. There are also several datacenters in Bern, Lausanne, Basel, Olten, Lugano. Two providers have mentioned that they have already opened or plan to open in the near future their datacenters in the heart of Swiss Alps - in the Canton of Uri (in reconverted army bunkers):

"So we say to our customers that even if we disappear in a nuclear attack, our data will stay. We are also thinking of renting a room there, so if something happens we can stay with our data!" (Provider 5)

Only one provider has shared with us their plans to expand out of Switzerland:

"...in jurisdiction some sort of equivalence as Switzerland, but it's not easy to find. For sure, we'll not go to London or US!" (Provider 1).

5.1.5 Cancellation or termination of the contract

As a rule, cancellation or termination of the contract does not cause any difficulties in the relationship between providers and their customers. Usually, all reversibility conditions and procedures are specified in the contracts and each party knows its obligations.

"It's all in our general conditions. The client remains the owner. So if a client wishes to leave, we give him his data back, it's his." (Provider 4)

Cloud providers are ready to assist customers to transfer the data back. For most of them (like for Provider 3) this is a part of the "professional service".

We also asked cloud providers if they maintain a client data exit and recovery plan, if their business should unexpectedly fold. We have received various answers dependently of the type of the company and service provided.

Provider 2, which is not a private commercial business, has noted note that they never thought of such a situation:

"I don't think we ever considered that option, to be honest. Because we don't expect to fold." (Provider 2)

Provider 1, who strongly positioned himself as an IaaS provider, does not see any necessity to do it:

"We provide the tools, but it up to the customers to implement it. Why it is such? Because we are not a software service; we are infrastructural services. We do not do automatic

copies on behalf of the customer to the datacenters. First, it will be expensive and the customers do not expect it." (Provider 1)

One of the SaaS and PaaS providers has mentioned that "this is in SLA…" (Provider 3).

But in general, we have had an impression that Swiss cloud providers look to the future positively and hope that this situation will not happen.

5.1.6 Cloud computing service and data retention schedule and lifecycle management.

We also wanted to find out if the cloud computing service works along with the retention schedule of the client's documents. One of the providers has willingly explained the situation:

"If a customer has Infrastructure as a service, they are responsible for this, of course. If it's PaaS, they are responsible for that, if it's software as a service we are responsible for it then." (Provider 3)

The process of data destruction (if required) is also determined by the type of the cloud service. IaaS providers, who are responsible for destruction of the data only in the case of cancellation or termination of the contracts, do it at the end of the contract period:

"So it will be automatically shredded after 7 days that they end the contract, at the end of the contract period...So we don't have any policy with shredding any data, it happens automatically." (Provider 5)

Other providers mentioned that they have a special process. Provider 4 acts in accordance with ISO 27001's requirements. They work in cooperation with subcontractors, who specialized in destruction of the hard drives:

"We work with third party businesses whose job it is to destroy hard drives. If we need to go up to physical destruction they come, they crush, they give us a certificate that the disks, or the tapes, have been physically destroyed". (Provider 4)

If customer needs any confirmation that the documents had been destroyed, they are ready to provide him with required certificates.

We also asked cloud providers about their experience with transferring a client's records to an archival institution. Almost all providers were even surprised by this question, as none of them had ever heard of such a practice.

5.2 Economic aspects

5.2.1 Economic advantages of cloud computing

We have asked the providers to tell us about the economic advantages of their particular services. All providers have pointed out the advantages of cloud computing, as a whole, over traditional IT. Rather than have a whole IT department, they explained, with their own servers and a staff to maintain them, it's cheaper to subcontract to a cloud provider. *"... if the client has decided to outsource his solution, he doesn't have material costs anymore, nor license costs, all this is part of a global service."* (Provider 4) All providers agree on this. Most providers also have large or very large companies among their clients, which might mean that cloud computing is economically advantageous, even for those large companies which can raise the

cost of an in-house IT department. Of course, those companies might see other advantages in using a cloud-based service; and the question of how many of Switzerland's largest companies use cloud services, and for what, remains to be answered.

But the cloud providing market, all providers agree, is a very competitive one. None can boast of offering much cheaper prices than the concurrence. The virtualized nature of cloud computing, of course, also means that this is a global market and that Swiss customers can easily chose to do their business with international cloud providers:

> *"You have a global market. You have competition. And the prices are more or less transparent. So it's not possible to be more expensive than Amazon, Google and things like that, if you don't have any special services." (Provider 3)*

As a result, most Swiss providers don't use any economic arguments to distance themselves from the concurrence. Rather, they try to find other niches to fill, while keeping their prices in line with the global market.

What arguments they use differs from provider to provider. One proposes an ecological argument, pointing out that shared storage space is more advantageous for the environment than multiple machine rooms spread over a large space:

> *"[...] we hear talking more and more about "green IT", and this, it can be an argument for the clients. It's true that to mutualize instead of having machine rooms spread over all of Switzerland, if we only had a few data centers, it would cause less pollution." (Provider 4)*

Several providers were older companies that were active in IT or telecommunications before offering cloud services. Therefore, they had a base of loyal clients to draw on, and they use their experience in related businesses to attract new customers: *"Sales relationship. Those are the advantages that we have primarily."* (Provider 2)

One argument that most provider used, however, was the one of being Swiss. This argument can be used on Swiss clients as well as international ones. For Swiss clients, having a Swiss cloud provider has the advantage of proximity and familiarity. Customers can visit the providers in their office if they want to, or even visit the datacenters if the provider allows it. They feel a more direct connection to their provider.

> *"We have our account managers, we have our people here you can talk with them… Try to discuss this with Microsoft. It's not possible. And important decisions for the product development… they are made here in Switzerland. And not in US or Germany or in other countries. We are more local than the other ones." (Provider 3)*

For international clients, choosing a Swiss cloud provider with data hosted on Swiss territory comes with its own set of advantages, the first of which is the provider's compliance to Swiss data protection law. This is something that most providers agree is demanded by clients:

> *"Today we can guarantee that the data remains in Switzerland. That, too, is something that is requested more and more. [...] They remain on the territory. In particular for questions of data protection, law, regulations. The clients who are constrained to that are mostly the banks, the insurance companies and people who are sensitive to where their*

data is stocked. But we see that it's something that comes up more and more." (Provider 4)

Swiss data protection law is indeed very strict, but it isn't the strictest in Europe. While the providers we interviewed didn't raise this point, a quick look at various Swiss providers' websites (not necessarily the ones we interviewed), where they promote their services, shows that it is not only Swiss law that helps them sell their service, but the fact that they are, indeed, Swiss. Swiss flags, mountains and safes are symbols that are used on the providers' websites, showcasing a certain idea of Switzerland as a country of safety, a place where data will be kept by discreet and efficient workers.

For example, Swiss crosses on Swiss red mountain promote this providers safe cloud services:

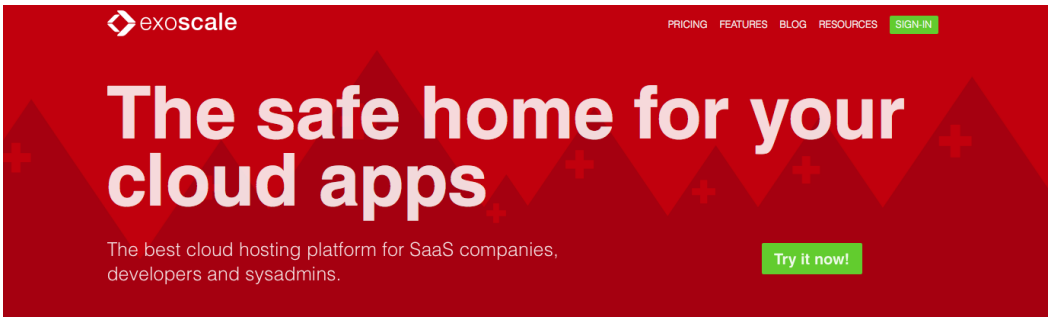


Figure 2: exoscale.ch

And a picturesque view of Swiss mountains illustrates these « 100% Swiss cloud solutions »:

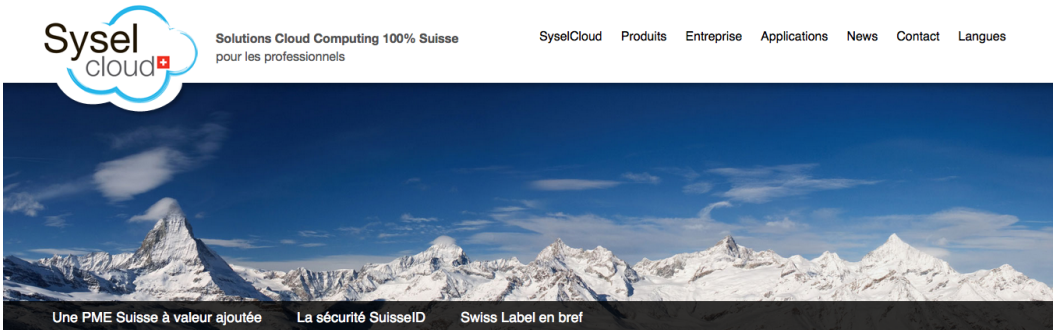


Figure 3: Syselcloud.ch

For those providers, being based in Switzerland is clearly a sales argument, and according to what the interviewees had to say, it's an argument that works. Some customers are glad to know their data is kept in Switzerland, by Swiss people. Whether data is really better kept in the country, however, is a question that remains open.

5.2.2 Return on investment of cloud services

We asked providers about the return on investment (ROI) of cloud services for their clients. While all providers agreed that there was probably one, they usually didn't calculate it, nor had they the means to do so. *"I can't calculate the return on investment for a customer perspective…"* (Provider 3) This is coherent with the fact that most providers don't use an economic argument to win customers over to the cloud. Whether going to the cloud is advantageous is left for the clients to decide and all work related to calculating the possible

return on investment is left to them; or, in one case, to web agencies with whom the provider works: *“Then we work a lot with partners, big web agencies in Switzerland which do the calculation for their clients.”* (Provider 6). As the clients are the ones who know the cost of their own IT, as well as the provider’s cost, this is somewhat understandable but again, providers don’t try to communicate on that, though most feel, without being able to give us any number, that there is, in general, a return on investment in going to the cloud for private companies - which are often their core business target.

5.2.3 Pricing mechanisms

The pricing mechanisms of the various providers tend to the same model. Pay-as-you-go is now the preferred option, though the pricing mechanism vary from one service to another. More and more, the providers are going towards more detailed prices. At this point, most customers pay by the hour. There are also storage services that get paid by storage unit. Some providers are already going into pay by the minute.

Monthly prices are still in use for some service by some providers, but those tend to disappear. *"And now we have pay-as-you-go. We started with monthly prices and now we are going to hourly prices."* (Provider 3)

Newest providers offer the most detailed paying option:

> *"Everything is by the hour. Our processing is by the hour or if it’s storage it’s by size of storage, by gigabyte unit. [...] Because it’s go down to the minute." (Provider 1)*

On the other hand, older enterprises who offered or still offer standard IT or telecommunication services are still billing the old way, each month:

> *“The pricing mechanisms at the moment with one of our products is on a monthly basis with a monthly plan and the other one you can pay it on a monthly basis or even hourly basis." (Provider 5)*
>
> *"We offer by month, by term or by year. So the client chooses for how long he pays and that’s it". (Provider 6)*

This may be due to habit, as older providers are used to a certain way of billing their services, while newer providers who started by offering cloud services are more aware of the capabilities of cloud computing, and offer more detailed payment options.

Indeed, one can wonder if monthly payment models are even compatible with cloud computing at all. The National Institute of Standards and Technology definition mentions “rapid elasticity” as one of the defining characteristics of cloud computing (Mell, 2012). Just how elastic can a service be that doesn’t scale its pricing mechanism to more modest uses? However, all the providers interviewed considered themselves cloud providers and we choose to consider them as such as well.

5.2.4 Cloud computing customers

One of the question we asked ourselves was who the users of the cloud services in Switzerland were. Based on our survey of literature, we expected small and medium enterprises to be the main users of those services. We also wondered whether they were all private businesses or if public entities numbered among them, or some of the many NGOs based in Switzerland. We

also wondered what measure of those clients were Swiss, and what measure were from other countries.

Except for one provider which has traditionally worked with universities, most provider we have met deal mostly with private companies. These companies vary in size, from very small start-ups to very large international groups. The activity sector of these clients, too, are varied:

> *"We can talk about activity sectors. I told you insurance companies, banks, industry, what do I forget… people who work in the travel business, people whose business is based on the internet, people whose job is security…" (Provider 4)*

When the provider offers PaaS services, most customers using those services will be in the software development business. Developers are more likely to find a use to the platform model than other users, who will either want to fully outsource their IT and go for SaaS, or who will want to keep more control over their data and opt for an IaaS that allows them to deal with their data themselves. Providers have not reported a majority of PMEs in their clients, rather outlining the fact that enterprises of all sizes use their services. However, no actual numbers have been provided.

As for the geographical provenance of those clients, most are Swiss, but a good number of them are international clients. The rate between Swiss and international clients varies from provider to provider, with some having almost only Swiss clients, with a few exceptions, and some having as much as 70% of international customers. Most providers agree that having their data stored exclusively in Switzerland is valuable to the clients. This is a newer development, as a few years ago clients didn't seem to wonder or care where in the world their data was hosted. *"What we talked about earlier, I mean that people, now, want to know where their data is located. If we can tell them it's in Switzerland, it reassures them."* (Provider 4) Non-Swiss clients that were mentioned came from the United States, Italy, Singapore, Brazil, Latin America, France, French speaking Africa and other, undisclosed locations.

It would be interesting to see the actual numbers of international versus Swiss clients using Swiss cloud services. However, our first foray into the question showed us that Swiss cloud computing is attractive to foreign businesses, whether coming from neighboring European countries or from much farther away, like the Americas or Asia. The Swiss law on data protection is certainly a draw, but is not actually the strongest in the world, or even in Europe. Beyond Swiss law, the main draw seems to be the stability, both political and geological, of the country. This is, at any rate, what some providers (again, not necessarily the ones we met) display on their websites.

> *"Switzerland has a reputation not only for privacy, but for delivering quality which in our case manifests itself as reliability, accuracy, innovation and being there for customers with 7x24 support." (Cloud Computing Safe Swiss Cloud.ch, 2016)*

> *"In one of the last countries allowing un-tamperable data storage, our expert team - battle hardened from experience in highly critical environments and industries - will ensure your data and services are safe from technical or legal harm." (Exoscale.ch, 2015)*

The reputation of Switzerland as a country where secrets lie safely, and where quality of service is a way of life, is an economic argument that multiple cloud providers use to attract

customers both at home and abroad. And it does seem to work. Certainly the events of recent years concerning the US PRISM program, which allows data collection on non-us citizens, have made the population at large more aware of who has access to their data, and in search of a way to protect them (Whitley, 2013).

5.3 Legal aspects

5.3.1 Legislations, certifications and standards

During the interviews, the cloud providers were asked to talk about legal aspects on cloud computing in Switzerland and what their company do in order to follow the legislation. What came out of these interviews is that providers have a variety of certifications.

The cloud computing providers interviewed are all subject to Swiss law, meaning that they follow the DPA. According to the legal department of provider 2: “The most important principles are listed in articles 4, 5, 6 and 7 of the DPA”. These articles are about the Correctness of the data, Cross-border disclosure and Data security. Provider 2 also mentioned that Cantonal compliance varies from one Canton to another, but they generally require each subject organization to dispose of a legal basis for the processing of personal data. Their own cloud company is not subject to cantonal law, but they will have to apply in the case they become an outsourcing provider.

Provider 4 and provider 1 are subject to the Swiss Federal Ordinance on Data Protection Certification (DPCO). Provider 4 added:

> *“We completed this certification called DPCO, which is the Swiss norm for data protection and which respects the information security law. And we’ve been certified Good Privacy, too, it’s the international equivalent of this DPCO norm. So it means, we have one certification in information security and one certification in data protection. We’ve been audited two years ago, there were jurists, technical people, and they audited every process: how we manage our client’s data, where it is stocked, how they are kept, do they leave the company, the territory, all these things have been analyzed. And then they put their OK stamp, certified DPCO. This certification is re-newed, we underwent it a short time ago. Every year all these things are looked at again, with the evolution of the company. They call it “major nonconformity” or “minor nonconformity”, we haven’t had any on these two certifications. It means we respect the law on data protection as we promised we would, and information security in the same way”.*

A certification adopted by the providers 3, 4 and 5 is the ISO 27001 certification. Provider 5 says: “There is one standard certification which is the most popular one and the most stable one. This one is accepted by 99.9% of the customers and that is ISO 27001”.

Provider 3 has also obtained the certification ISO 20 000.

Since this certification haven’t been presented in the state of the art at the legal aspect and in order to understand what it is about, here is a small explanation: ISO 20000 is an international IT standard that allows companies to demonstrate excellence and prove best practice in IT management. The main goal of this standard is to make sure that companies can achieve evidence-based benchmarks in order to improve the IT services they deliver. ISO/IEC 20000

was released in 2005 based on the IT infrastructure library (ITIL) best practice framework. It has been updated in 2011. (ISO/IEC 20000 Certification, 2013)

Provider 1 doesn't have an ISO certification but rather comply with the framework of the Cloud Security Alliance. He says:

> *"We've chosen this framework because it covers not only the datacenter or the support system but it also covers all the cloud provider's services. So it goes from the bottom, from the physical access to the data centers, up to our bidding systems, the HR, etc. It has more than 130 controls that we regularly check."*

Provider 2 doesn't have any certification on data protection, but is subject to the Swiss Federal Data Protection Act. The legal department of this company formalizes legal documents that govern how their services are used, how their customers interact with them, what the company's and the client's rights are, and so on.

In order to insure that all legislations are respected, provider 3 has been certified by ISO and by ISAE3402 (International Standard on Assurance Engagements) and SAS 70 report (Statement on Auditing Standards). His company also has a legal and an audit department that makes internal and external audits. The provider talked about how different industries deal with legal compliances. He specifically added:

> *"Legal compliances depend on the business. Between different industries you have different regulations. So if you are a Swiss retail banking, for a Swiss retail bank, the data must be in Switzerland. But if you are a private Swiss bank and you have your mergers and acquisition company or your investment banking which are in the UK or the US, it's important to have the UK and the US regulations in place. As a cloud provider, at the end, it's about the service, an outsourcing, a sourcing service. It's not really different from that. And we have to be careful that we have all regulations of Switzerland in place. If another company, from Brazil, they are in our cloud and they have financial systems, for example, in the cloud, and it's forbidden by Brazilian law, it's not our problem. It's the problem of the customer."*

In order to understand what the ISAE 3402 is, the ISAE 3402 website explains that the International Standard on Assurance Engagements was developed in order to provide standards for international assurance in order for public accountants to issue reports for organizations and for their auditors on internal control for financial reporting. (ISAE, 2016)

In order to understand what the SAS 70 report is, the SAS 70 website explains that the Statement on Auditing Standards No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). An auditor is making an in-depth examination in order to see if the control objectives and the control activities are in accordance with SAS No. 70 (also commonly referred to as a "SAS 70 Audit"). (SAS 70, 2016)

At this point, it's important to say that none of the providers interviewed mentioned at any time the new ISO 27017:2015 and ISO 27018:2015. Customers are advised to check if their cloud service provider conforms to these standards, since it is specific to cloud computing (Cloud Security Standards Customers Council, 2013)

5.3.2 How the Swiss legal system compares with other countries

We asked the providers to compare the Swiss regulations with the regulations of other countries. We heard repeatedly that the Swiss law has a strong data protection and it has often been compared with the data protection of the US. Specifically, provider 5 believes:

> *"In the US for example, with the Patriot Act, the Government or the NSA, can go directly to the cloud provider, like us, and ask for the data of a specific customer without even informing the customer. But in Switzerland, you must have a specific document from the Government or from the Court. So it's not like we can do it just like that. It's more complicated and it doesn't happen usually. We never had a request like this."*

The USA PATRIOT Act (officially the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) is an anti-terrorism legislation in response to the September 11, 2001 attacks. It was signed into law by President George W. Bush on October 26, 2001. (Electronic Frontier Foundation)

Provider 4 referred to the international clients of the company and specified that his American clients want their data to be in Switzerland. He explains:

> *"I think there's an interest in Swiss law on data protection. There are some guarantees given in Switzerland that don't exist abroad. For political reasons, Switzerland is relatively stable, data protection law is quite restrictive, so people have an interest in putting their data in Switzerland."*

Concerning the US, the provider ads:

> *"There has been a voting. The Americans rejected the Safe Harbor so that American businesses could put their data in Europe and they wanted that the data could go back out. There have been some conflicts of interest between Swiss Law and American Law and there has been a voting on the 6th of October 2015 and Americans have put this procedure into question. I don't know if it will change things drastically but they are trying to say that, if you have American clients, the data must be provided to the United States. It's a political debate. Until today it was "what is in Switzerland remains in Switzerland". I don't know if it will change in the future. Something might happen in the months to come".*

A member of the legal department of the provider 2 added: "I would say that Switzerland has a decent data protection law which is however not the strictest and most effective. It is more stringent than that of the US but less so than for instance German data protection law". On the same line on how the Swiss law compares to other legal systems, provider 3 says:

> *"It's more or less the same. In the European Union it's more or less the same stuff, also with data protection. They are not really different. They are not. And if you look at the American law, everybody heard about privacy, privacy is something different in the US. But within Europe, it's more or less the same; Swiss people always think that Swiss data privacy is the strictest in Europe. It's not correct. German is more."*

Provider 6 when explaining why his clients want their data to be held in Switzerland, says:

"We had a lot of questions recently concerning the last laws in France. Laws on IT, and so we know that some clients came to us because of these laws. Those who are interested in this and who want to be sure their data are not seen by the government, at any rate. But it's still laws in brackets… I don't know in what measure they are applied. It's more theoretical as long as no one asks for them to be applied. We can't check what happens in France, but we know that some clients feel more secure because in Switzerland some laws don't exist and they are not, potentially, subject to that here."

On the matter of European regulations, provider 1 expresses his distress on the fact that there will soon be a unified European regulation that will be much more complete than the Federal DPA. And he's afraid that this big change will "set the business back". He believes that this new regulation will concern all European countries.

This new unified European regulation is a fact, as also mentioned from the legal department of the provider 2: "Currently, for European compliance, each European country has to be looked at individually, as the current Directive is not self-executing. This is likely to change with the planned Regulation which will apply directly in all member states".

5.3.3 Data collection and anonymity

Depending on the provider different data are collected from their customers.

Provider 2 says:

"We have privacy policies and those are public and we specify what data is being used, for what use, how long they are stored and so on." When asked if the anonymity of data is guaranteed he replied: "The guaranty on anonymity and security is that we will not use that data for anything else than the operationality of the service, whatever the service we are talking about. The people who are working on these services have signed in their work contract agreements on how they have to treat customers' data. And the breach of that contract will lead to human resources consequences. The customers cannot opt out of the data collection because the system will just collect data, usage data and that cannot be opted out of".

Provider 4 says that the data belongs to the customers so they don't treat them. They only treat the data linked to invoicing. They do no statistics or stocks and they don't sell back the data to anyone. He adds: "It's more a question of ethics than anything else."

Concerning this question, provider 3 says:

"We have to log all data according to client services and client systems. If we are responsible for the operating system, we manage it and we log who is entering on this virtual machine, who makes changes, things like that; But if everything is managed by the customer, than we don't have rights and permission to get into the virtual machine."

Provider 6, which also hosts websites, when asked if their clients are aware on what data are being known about them, replied:

"We ask them for some data when they sign up with us through the admin interface (email, telephone, etc.). Then in regards to their website, we keep some of the logs. It's standard in the business, for providers, as the law asks for it; we don't keep more

information than the law asks us to. It's still a lot in terms of disk space. We don't want to put too many resources in something we don't use".

And when asked on anonymity, the provider said: "We guarantee it naturally. Data are used internally. We don't use them for partners". He added that if data is need from partners, they always ask the consent of their client first.

On the other hand, provider 1 says that

"We must collect their addresses, etc. We have data classification policy, it's public, it's on our website. We have different levels of protection regarding this data. We also apply in our system whether it's only just the name or it goes up to the banking records of customers, biding records and stuff like that. So there is a whole set of data that we also communicate, but it's public".

And when asked if their clients are being aware of that data collection, he replied: "Yes, because this is the minimum set of data we need in order to operate this business".

5.4 Security issues

5.4.1 Security measures and policies on data security

It's interesting to notice that when the cloud providers are asked about the security measures and the policies they have on data security in their company, they reply in a variety of ways.

In order to control all aspects of security, Provider 1 has elected the Cloud Security Alliance (CSA) framework. Provider 2 doesn't have any formal policy on that matter but rather follow industry's best practices. He uses firewalls and limits the access to the customer's data. Provider 3 said that the company is certified according to ISO 27001, that they have the regulation ISAE 3402 as well as the PCI DSS (Payment Card Industry Data Security Standard) for the banks, for secure money transactions. Provider 4 when asked about data security, he mentioned again that the company is certified ISO 27001 and then added:

"We correlate all data in terms of security, rather than treating them independently, we put into place mechanisms to centralize the information on a security point of view. There is an alarm to watch over 3.000 clients routers spread over four data centers. Digital attacks come by different ways, it's not humanly possible to check them; so we put in place those mechanisms and from there, when attacks are detected by these malicious IPs, we ban them from all our infrastructures".

Provider 5 replied that there are no real policies or measures and that everything is based on their SLA. They save the data within Swiss borders and within Swiss data centers and they protect the data from any disaster, it's the key point of their job. Provider 6 says they are using antivirus to scan files before the clients put them on their space which detects viruses and intrusions.

5.4.2 The importance of security for the clients and hesitation issues

All six providers agree that security is very important to their customers.

In the matter of how they deal with their clients hesitation on the security of their data, provider 1 and provider 3 point out the fact that they are available to meet with their clients in person if

required, in order to explain them more on security issues. Provider 1 also gives guidance to encryption or to other technical best practices to his clients. Provider 4, even thought he believes that security is important to his clients, also adds that not all clients are conscious that security should be their priority. They rather put production first. They focus on the operational part but don't realize that their data is stored on the other side of the world, he exclaims that "We're far from having educate everyone". Provider 5, in order to manage client's fear, offer in their services integrated back-up, disaster recovery plans and replications of data in other datacenters in different locations. Everything is included even for the lowest price offers. Provider 6 reassures his customers, which usually share the same virtual machine to host their websites, that the provider uses antiviruses so if one site gets infected the others won't be contaminated.

5.4.3 Protection against malicious insiders within the company

In order to protect their clients from their own employees, cloud providers are taking some measures.

Provider 1 says that HR control is part of Cloud Security Alliance controls. They make a lot of background checks of their employees. Provider 2 simply makes legal contracts on that matter, it's part of their employment contracts. Provider 3 also makes background checks and criminal record controls. On the other hand, provider 4 employees have to sign a document called "Acceptable Usage Regulation". This document states what are their rights and what are their obligations. The provider says: "If you use confidential client data, if you don't use adequate ways to transfer them, it's a professional misconduct". Provider 6 says that his support service doesn't have access to the data and that only the small production team does. They try to have versioning systems so they will be able to go back to the source if there is a problem.

In the case of a security breach due to a malicious insider, providers said that even though they haven't experienced that situation yet, they will inform their client if they have such an incident (One provider did experience an incident but in order to preserve anonymity no additional details will be presented). Provider 5 says that if it was the case, the first thing he would do would be to make sure the intruders are no longer present in the system and then he would find out how the leak happened and then correct the mistake. Providers 1, 3 and 4 declares that they have compensations and penalties in case of security breach in their SLA.

5.4.4 Back-up systems and random tests

In order to secure the data, some providers have back-up systems which are made automatically or on demand by the customer.

Provider 1 makes back-ups and has a replication system mainly for the data that are required in order to provide the service. But if the client is the one who is actually creating the virtual machine, then the company doesn't do any automatic back-ups. It's left up to the customer. So if something unexpected happens the data will be lost. Provider 2 claims that they don't back-up the data because it's the customers' responsibility to do so. Provider 3 has the possibility to offer a back-up system as an extra charge. As already mentioned, provider 5 has a back-up system. He ads: "Since we are all digital, we have the back-up system and a replication data center, so in case of physical damage we have it all on a totally different location". Provider 6 offers a back-up system only in the case he is managing the service. If

the deal concerns a non-managed offer, then the client is the one responsible for backing up his data. But still if the clients need it, they can ask the provider to do that for them.

In order to make sure that the data assigned to the provider is in a good shape at all time, random tests are a possible solution. We asked the providers interviewed on that matter and we realized that they are using their own technique in order to control the data hosted.

Provider 2 says that "Basically the storage system we have does that automatically. It continuously checks for data corruption and will repair data that became unreliable". Provider 3 claims that they don't make random tests but they control the amount of data stored. And, in the case they are assigned of doing the back-up of their clients data, just to be sure, they do it three times a day instead of just one and then store one version. Provider 4 is doing what he calls "restore tests", it's like a back-up test. That consists on taking a file which they already know the content and see if they can take it back. In that way they assure consistency while the confidentiality of their client's data is respected. Provider 5 is doing on a weekly basis an automatic test which consists on using the backed-up data, creating a clone of it and then restore it to see if the data is consistent. Provider 6 is using a monitoring control to make sure that backups are done correctly and that the data is still accessible.

5.4.5 Dealing with data loss

Provider 1 and 5 provides a very limited insurance policy on data loss. Provider 2 says that it has happened once that they lost some data. They eventually managed to retrieve most of it. They deal with that issue with a lot of stress. Provider 3 explained that the legal department have some sort of insurance policy in case of data loss. They need that because some of their clients are in the banking system. More specifically he says: "In the banking zone we have services in place where we can see if we have a problem with data loss and who has access to the data. Is this usual, or normal or is there any curious action." Provider 6 explains that they have general conditions with service levels that are more or less by default. In case they lose data of very important clients, after informing them, they can offer gratuity of a service, but this will be dealt on a case by case principle.

5.4.6 Levels of security

Provider 1 has one level of security. Provider 2 has a basic level but implement more levels is possible. There is also the possibility of encryption of file systems. Provider 4 offers different levels according to different needs of the customers. Specifically, he says that

> *"We have a client in the travel business which makes online sales, so there are credit card number transitions. This client should answer to PCI DSS (Payment Card Industry Data Security Standard). So we have auditors coming to us, saying: "Show us how you manage data". This very precise environment, not everyone internally has access to it. We agreed with the client that only a few defined persons can access this environment."*

On his part, provider 5 has three different level of security for an intruder to hack to be able to reach the stored data.

When having subcontractors, provider 2 requires to have contracts signed with them in order to agree upon the same level of security. Provider 3 as well, requires the same level of security from its subcontractor. Provider 4 explains the importance they put on security when it comes

to subcontractors. Since it was a strategic choice to collaborate with external data center providers who host their clients' data, they need to guarantee that there is security, guards, air conditioning, enough energy and enough electricity. He ads: "We ask the data center for accountability. I want every month, the log of all people who entered the data center. We gave them an authorized list on who has permanent access and who has access on demand". Provider 5 doesn't work with subcontractors for the moment, but if it was the case, he would require the same level of security from them. Provider 6 don't work at all with subcontractors so this is not an issue for him.

5.4.7 Who is having access to the data

We asked the providers if their customers want to know who is dealing with their data.

Provider 1 doesn't give the details to his customers because of lack of time, but he offers the possibility to his client to have an external audit held in order to find out details about their data. Provider 2 says that he absolutely does provide that kind of information. Provider 3 also claims to informer the customer on who is dealing with the data if that is required. Since some of their clients are banks, they are obliged to do so. Provider 4 also provides this information to his customers. Provider 5 can tell this information but reassures his customers that by using the encryption method that not even them, as providers, they can't have access to their data. Provider 6 says that since they are a small team, all the employees are on their website so the customers know who has access to their data.

5.4.8 Who is in charge of the data and where is it hosted

Provider 2 says that the customers are basically in charge for their data as well as the team that runs the operations of the Infrastructure as a service, which keep the data secure. Provider 3 believes that data is the customer's responsibility.

Provider 1 expressed that the clients know where the data is hosted in Switzerland because it's written in their website. Provider 2 says that the clients do know where their data are hosted and that they can even select on their own in which data center in Switzerland they would prefer to store them. Provider 3 and 5 also says that their customers know the location of their data.

To the question, if it is an argument that the data centers are in Switzerland, Provider 1 said "Yes!". Then he added that it's more like a marketing argument the fact that the data is hosted in Switzerland for law protection reasons. The fact that in order to get access to someone else's data you would need to provide a court document and also notify the customer is a real key advantage for international clients. Then he completed by saying that if a provider wanted to store the data outside Switzerland, he could easily do that without anyone knowing about it. Provider 2 simply says that the customers rather have their data in Switzerland. Provider 3 says "Yes, only in Switzerland" and provider 5 explains that most of his customers do care and want to know if their data are located in Switzerland. Provider 6 believes that the reason some of his clients need to have their data stored in Switzerland has to do with the legislation in order that international customers data won't be seen by their own Government. He specifically mentioned the French law that is in the process of being changed concerning data claim from authorities. This new law will be based on the American Patriot Act.

5.5 Technological aspects

First of all, we feel obliged to point out that we are not specialist in information technologies. That is why we have not be able to dig any deeper into the subject.

Through the interviews, we have looked at several points:

- Consumers' control about their data, like possibility to use records management's tools, or existence of vendor lock-in
- Encryption, integrity and authenticity of data
- Multi-tenancy and its issues

5.5.1 Customers' control

We started by asking how much control the customers have over their data. All our providers answered: full control. Indeed, the majority of the providers we have asked offer IaaS mainly, some offer PaaS and only one offers SaaS. Data is not part of what they are committed to manage, except for SaaS, as provider 3 points out:

> *"All. They are responsible for that. Can they visualize the state of the records? It's depending of that that they have in place. I can't say, it's depending of their systems. It's not in our hands."*

5.5.1.1 Records management tools

When we ask if the cloud computing application can be combined with other tools used for record management, the answers are more mixed. Two providers argue that it's not a part of their competence, because they provide IaaS. Two others, although it is not their field, say that the customer can use without problems a third-party software dedicated to records management.

The two last providers do not really know what records management means. The first (provider 4) mistakes it for cloud monitoring:

> *"Yes. Typically, the monitoring tools we use. We guarantee functional platforms, that we do not reach the disk limits, the CPU's, the RAM's… All these things we keep an eye on. The client's services we keep an eye on. We have our own monitoring tools, we monitor our network of course, to be sure it's still in good shape, we monitor our DNS, our servers, we monitor the whole infrastructure. It ads up to the services we offer but we are obliged to be sure everything is functional."*

The second also seems to mistake records management for monitoring or data analysis and reminded us that its offer is about website hosting and virtualization (provider 6).

5.5.1.2 Vendor lock-in

About vendor lock-in and open source solution, our providers are unanimous: vendor lock-in is not a good practice and open source must be favored. The main reason given is the risk of a feeling of imprisonment for the customers. If a potential client feel that he will not be able to easily switch providers, he will not come, as provider 3 says:

> *"But in a cloud, we believe that proprietary systems, or proprietary APIs are not the right way in the cloud. (…) And if one cloud provider starts with them, he will lose all*

customers. Doesn't make sense. Cloud is, from my perspective, against lock-in. If you have a classic outsourcing, it's much more difficult to change the provider. If you are in a cloud it's easier to change the cloud provider." (provider 3)

Moreover, open source is perceived as a trend which is good to follow:

"So as mentioned before, we are also trying to offer just products and services that don't have any vendor lock-in. And the general trend today is that almost all servers and popular solution out there, which we are also using are based purely on open source basis. Maybe 10 years ago, Windows and Microsoft, have been the standard in enterprises but this is changing right now. Linux is growing and it's more popular even in enterprises, it's going into them so that's a good development." (Provider 5)

For provider 6, this is also philosophical choice:

"Yes, absolutely. In all projects we use, even outside of the cloud, we try to do open source. It's a matter of philosophy. As much as we can, at any rate, there are some products where we can't, because they are not as good as conventional products but it's very rare. All that we can, we do in open source, yes."

5.5.2 Encryption, integrity and authenticity of data

5.5.2.1 Encryption

For performance reasons, the providers opt to not systematically encrypt the data. One provider, provider 3, always does it, but the enterprise is well entrenched in Switzerland and one of the few who did explicitly mention banks among its clients.

Another provider, provider 2, considers that "user encryption doesn't really help" or does not provide "additional level of security" for his SaaS product, because "the keys are still on the server and the administrator could still use that additional access to get access to the data." To fix the problem, our interviewee muses about "a system that provides end to end encryption, so that the customer can encrypt the data himself and we don't see that." However, it raises another problem:

"If the user forgets his password, the data is unrecoverably lost. Unless you have kind of a master key, at which point we're back into why do we encrypt in the first place, if you have somebody who has a master key."

Nonetheless, the IaaS customers can encrypt their data themselves, if they wish.

As for the confidential data about their clients, our providers encrypt them. Provider 4 specifies that all communication of data with federal organizations or the police, when it needs to happen, "are transmitted in an encrypted way".

5.5.2.2 Integrity and authenticity

For IaaS providers, the integrity and authenticity of data are the customer's problem. If the providers want to insure that they are protected, they do it by following the ISO 27001 certification.

However, most providers do not seem interested to offer technical solutions to authenticity issues. Only one does mention and explains that his SaaS "has mechanisms that authenticate

the users and only allows a user to upload files into his directory and so on" (Provider 2). Our interviewee recognizes that "we don't take any special precautions, but the product that we're using has mechanisms that help with that." (Provider 2)

5.5.3 Multi-tenancy

The question of multi-tenancy's use does not arise for our providers. One of them even says: "It's an only way to go." (Provider 1) This is why the majority of the providers do not offer any alternative to multi-tenancy. Only two of them propose another solution, and then only if the client asks for it. However, this choice has a cost.

> *"Yes we do. We have this, I talked about that at the beginning, it's called Flow App engine, it's a Platform as a Service, and it's a solution which is built on a multi-tenant model and if they are customers that have really super special requirements, I would say 95 percent are covered with that solution, but if there are they can go with dedicated servers. But then they have to manage it or let as manage it, extra for them. But all this costs extra. So it's a question of money and of how much time intensive it is. But it's possible we offer both alternatives." (Provider 5)*

Similarly, the providers do not consider particular protection or insurance services. In case of trouble, they rely on the SLA. Generally, they consider their system is safe enough and do everything to manage risks before they happen.

5.5.3.1 Information about customers

The providers do not disclose information on who customers share tenancy with; they don't consider that is an information the customer needs to know.

In general, the providers we have asked do not seek to collect more information than they need to manage their customers, like invoicing (Provider 4), and this data is encrypted. About the data on the cloud, the providers assure us they can't access it and the data isolation is absolutely safe. (Providers 3 and 5)

6. Swiss cloud particularities

From this analysis, we can deduce a few points that are characteristic of Swiss cloud computing.

6.1 Swiss legal landscape

The Swiss Federal Data Protection Act, which guarantees the right to privacy, is the one law that all Swiss cloud providers are subject to. Among other things, it obliges cloud provider to have a certain level of security on the data, and to protect the privacy of their clients. This law seems to be reassuring for some customers conducting businesses from other countries where data protection law is less friendly, like France for example.

> *"We can't check what happens in France, but we know that some clients feel more secure because in Switzerland some laws don't exist and they are not, potentially, subject to that here." (Provider 6)*

Swiss data protection law is not the strongest there is but it is strong enough and, combined with Switzerland's reputation as a secure and stable country, it tends to attract international customers who want their data stored somewhere safe. As for Swiss cloud customers, we can't say whether they appreciate this law or if they'd rather have their data hosted in another country, as this was not covered by this research.

The DPA hasn't changed since it was established in 1992 and this apparent stability of the legislation might also be reassuring to customers. However, Swiss legislation on the subject is about to change, as *The Privacy, data protection and cybersecurity law review* (Schneider, Sturny, 2015) points out. What those changes in legislation will mean for Swiss cloud providers remains to be seen. The first revision draft, to be released by August 2016, will provide some first answers.

6.2 Switzerland's reputation

Most providers are very aware of the fact that they can't compete with in the international cloud market in matters of price. There are no Swiss providers in the top ten cheapest cloud services listed by CloudScreener (Crochet-Damain, 2015), for example. And in some cases and service offers, the providers are not even finding their own economic advantage. As provider 3 puts it, "*And with IaaS, nobody's earning money. Nobody.*"

Therefore, all providers need to find another niche to stay relevant. For a lot of Swiss provider, their "Swiss-ness" has been such a niche. Some communicate on this overtly, others don't, but all point out that the Swiss data protection law has been an advantage in getting foreign clients to sign with them. And all point out that their clients, Swiss or international, attach importance to the fact that their data is hosted in Switzerland. The reasons of this attachment may well not be the same for all clients. For Swiss customers, staying in Switzerland makes sense in a lot of ways: habit, trust in their fellow citizen, ease of use and of payment, etc. But for international clients, the decision to come to Switzerland is not anodyne and providers seem to have understood that their geographical localization, and the stereotypes that go with it, is a strength that they can use.

6.3 Evolution of customers of Swiss providers

Cloud customers are changing. All providers agree on that. More and more, the customers asking for cloud services are aware of the possibilities of the cloud, and consequently have more elaborate demands. They want more flexibility and more specialized services. Consequently, the providers have to keep updating their offers.

> *"There's a lot of people now who do cloud so we have more demands like, do you do such or such particular cloud thing… Sometimes we can't say yes so they go somewhere else. But it's true that there are a lot of clients who ask for new services or things we don't do yet." (Provider 6)*

And they can't just keep offering the same service, either:

> *"In 2013 looking at the market, we strongly believe that [...] platform as a service, was a way to go. For us it was moving from infrastructural service to offer a system that's closer to developers. [...] So, we internally discussed a long time about should we provide such a service. We said "yes". [...] We have now, as a partner, doing the platform as a service on our own infrastructure. Now, looking back, platform as a service has been something trendy, but the adoption is not quite there. [...] There is more flexibility now at platform as a service. That's hard topic at the moment and most advanced customers are experimenting and asking about it. This is likely shift will be doing in the next 12 -18 months." (Provider 1)*

Cloud computing is still evolving and the flexibility that characterize it is growing. At the same time, users are understanding the possibilities of cloud more and more as they get familiar with it. It is imperative that providers keep on with the evolution and even spearhead it, if they want to stay relevant in the future. This, however, is probably not a specifically Swiss point as familiarity with cloud computing happens everywhere the cloud is used. Further research on the nature of cloud customer internationally would be needed to see if Swiss providers' customers have a particular profile.

7. Good practices

From what the providers have told us and from the analysis of our data, we have inferred a set of good practices that can be of use to cloud providers in Switzerland. These good practices are in no way exhaustive, but we believe they can be helpful.

7.1 Stay open source

Asked about what good practices they would recommend to other Swiss cloud providers, our interviewees had different things to say. All providers were very interested in open source solutions as a whole and one provider in particular saw it as the future of cloud computing and the main hub on innovation in the field. More than just free code, open source is for them a new kind of innovation factor and the future of cloud computing will come from here. But this means learning new ways of working, not in an enterprise but in a community.

> *"...it's open source, we are member in the community, we are working with the community. So quite a lot of things. You have to see that we have… some people which are working together, or within a community. And the most innovative tools are open source. They have much more power than IBM, HP, Dells and whatever. They are more innovative, and if you want to use that you also have to work together with the community. That's something that we have to learn. Before, we had a supplier, we had a contract. But now, how to have a contract with a community?" (Provider 3)*

For everyone, open source is an obvious choice, as often as possible. *"It's a matter of philosophy"*, says provider 6. And *"I think no customer really likes [vendor lock-in]*", according to provider 5, who gives a very practical reason to stay away from proprietary code. If the customers want open source, then the provider better give it to them, or the customer may well look somewhere else. Four out of six providers mentioned using OpenStack, an open source software solution to deploying IaaS services.

7.2 Protect the data

Data protection is another point on which some providers are very keen. Providers must have control over the data entrusted to them, allow their clients to have control over those data. This supposes, among other things, to think about the geographical location of the data and what it implies.

> *"I think that good practices, for us, are mainly axed on the two terms we talked about: to have control over the data, physically, geographically, and to protect it. Today those two points seem crucial to me. You can't say anymore: "we're hosts, you can stock your data here, and that's all." I think that's over. And then, the geographical consideration, I think, are taken into account." (Provider 4)*

And while providers seem more aware than their customers about the security issues surrounding cloud computing, this is an important point for their customers as well. *"One of the most important"*, according to provider 3. New service providers had better keep this in mind and think about how to manage those fears when offering new services.

7.3 Give more for less

Provider 5 insisted on serving the client as much as possible, adding more levels of service without making them pay more:

> *"...you should just focus to serve the customer with everything and not just to say we are the cloud provider but we don't take care of the back-up for example, and many of them they maybe write it and they do back-ups if you additionally pay for it and check it on the order box. So our experience is just, serve it, with the food, salt and pepper! It should be there without them asking for it, don't ask additional money for it. Serve it! Like energy from the wall." (Provider 5)*

Honorable intentions that may be a reaction to a very real fact in Swiss cloud computing: customers are asking for more and more: more level of services, more security, more ease of use. And they are learning, too the use they can do of cloud computing and expect the providers to follow with the times. For many providers, cloud computing will become a fixture. *"...for the new generations cloud services are just normal. It's like having the energy coming out of the wall"*, as provider 5 says.

If his is true, then cloud providers will find themselves part of a growing market as more and more businesses will go in the cloud, but it also means that as awareness and knowledge of the cloud increase, the services offered have to reach higher and higher expectations.

8. Conclusion

8.1 Current state of the research

At the end of this project, we can say that we reached the objectives we had set at the start, despite some bumps on the way. The prospective timeline, which we set up in April 2015 (Annex1), was not respected. This was due to underestimating the time it would take us to reach providers and get appointments with them. The people we reached out towards were often busy and finding time to answer questions was not always possible for them. Moreover, time was lost on the analysis by trying to find a software that would help us treat the data, which was never found. We chose to analyze our data without electronic help, which might have extended the time spent on this part of the research.

As mentioned before, we achieved only six of the eight interviews expected. This was, again, due to time constraints. Given more time we would probably have reached more providers, but the end point of this project being set in stone, it was decided to go ahead with what we had.

Despite these problems, we were able to get a good first view on the cloud computing landscape in Switzerland at this point in time. The gathered data was of high enough quality to allow examination of all five aspects that were deemed as important. From this data, we were able to extrapolate a set of good practices that would be useful for cloud providers wanting to offer services in Switzerland.

It must be noted that cloud computing is currently at a very special point in its development, being well on its way to becoming a standard practice in business, while not being there yet. Are we going towards cloud computing being as essential as “energy from the wall”, as Provider 5 says? It’s too early to tell, but cloud services and their adoption are certainly evolving quickly. Would-be providers have to keep a close eye on the market before launching their services.

8.2 Ideas for further research

However, our study is necessarily limited. While we have found some interesting common points among the six providers we met, our sample might not be representative of Swiss cloud providers as a whole. Because we asked for a bigger commitment in time from them and asked many questions about how they worked, the ones who accepted to answer were probably more open, as a whole, than their competitors. It is possible, for example, that the overwhelming support of open access solutions that we saw is not shared by others, more secretive providers, who like to keep their code as well as their work processes to themselves and thus declined to answer our questions.

A continued study on the same line, trying to reach even more providers, may help to alleviate this problem.

Another way to continue this research on Swiss cloud computing would be to take a look at the clients instead. Providers were understandably rather vague on the number and nature of their clients. A quantitative research targeting Swiss businesses, whether start-ups, SMEs or big enterprises, would be an interesting complement to this study. A short questionnaire could be sent to as many businesses as possible, asking whether the enterprises used cloud

computing, why or why not, and if they chose a Swiss provider or an international one. This would help plug the holes in our current understanding of Swiss cloud computing.

Finally, examining why international clients choose to make use of Swiss cloud computing service would be very helpful in expanding the set of good practices we tried to enumerate with this research project. While Switzerland's legal landscape and reputation as a safe and secure country is one of the answers to this question, as closer examination at other countries legislation, and the changes in those legislations, might provide a more precise understanding of Switzerland's appeal in that regard.

Bibliography

ASHKTORAB, V. and TAGHIZADEH, S. R., 2012, Security Threats and Countermeasures in Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM). 2012. Vol. 1, no. 2, p. 234–245.

MÉTILLE, Sylvain and GUYOT, Nicholas, 2013. Cloud computing in Switzerland [online]. 2013. BCCC Avocats Attorneys-at-law. Available from: http://www.bccc.ch/shared/media/docs/contributions/390_1_c.pdf

BORNER, Silvio, HAURI, Dominik, KOCH, Patrick and SAURER, Markus, 2014. eEconomy in der Schweiz: Monitoring und Report 2014 [online]. May 2014. E-Government Suisse. [Accessed 4 June 2015]. Available from: http://www.egovernment.ch/dokumentation/studien/00174/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdYJ4g2ym162epYbg2c_JjKbNoKSn6A--

BRADSHAW, Simon, MILLARD, Christopher and WALDEN, Ian, 2010. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary School of Law Legal Studies Research Paper No. 63/2010. Available from: http://dx.doi.org/10.2139/ssrn.1662374

BRENDER, Nathalie and MARKOV, Iliya, 2013. Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management*. October 2013. Vol. 33, no. 5, p. 726–733.

BRODAR, Bastien, 2013, Suisse: le cloud public représentera 249 mios de dollars en 2017 - *ICT journal*. [online]. 6 February 2013. [Accessed 26 March 2013]. Available from: http://www.ictjournal.ch/fr-CH/News/2013/02/06/Suisse-le-cloud-public-representera-249-mios-de-dollars-en-2017.aspx?pa=1

CENTRE FOR ENERGY-EFFICIENT TELECOMMUNICATIONS (CEET), 2013, The Power of Wireless Cloud [online]. 2013. University of Melbourne. [Accessed 15 January 2016]. Available from: http://www.ceet.unimelb.edu.au/publications/downloads/ceet-white-paper-wireless-cloud.pdf

Cloud Computing Safe Swiss Cloud: About Us, [2016]. [online], [Accessed 10 January 2016]. Available from: https://www.safeswisscloud.ch/en/about

CLOUD FOUNDRY, 2011, Cloud Foundry | The Industry Standard For Cloud Applications. cloudfoundry.org [online]. 2016 2011. [Accessed 16 January 2016]. Available from: https://www.cloudfoundry.org/

CLOUD SECURITY ALLIANCE, 2009, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 [online]. December 2009. Cloud Security Alliance. [Accessed 17 January 2016]. Available from: https://cloudsecurityalliance.org/csaguide.pdf

CLOUD SECURITY ALLIANCE, [no date], About : Cloud Security Alliance. Cloudsecurityalliance.org [online]. [Accessed 17 January 2016]. Available from: https://cloudsecurityalliance.org/about/

CLOUD STANDARDS CUSTOMER COUNCIL, 2013, Cloud Security Standards Landscape [online]. October 2013. Cloud Standards Customer Council. [Accessed 17 January 2016]. Available from: http://www.cloud-council.org/Cloud_Security_Standards_Landscape_Final.pdf

CROCHET-DAMAIN, Antoine, 2015, Comparatif Cloud : IBM talonne Google, Azure passe devant AWS. [online]. 21 December 2015. [Accessed 10 January 2016]. Available from: http://www.journaldunet.com/solutions/cloud-computing/1167190-comparatif-cloud/

DIRECTION OPÉRATIONNELLE E-GOVERNMENT SUISSE and UNITÉ DE PILOTAGE INFORMATIQUE DE LA CONFÉDÉRATION UPIC, 2012. *Stratégie d'informatique en nuage des autorités suisses 2012-2020*. 25 October 2012. E-Government Suisse.

DIRECTION OPÉRATIONNELLE E-GOVERNMENT SUISSE and UNITÉ DE PILOTAGE INFORMATIQUE DE LA CONFÉDÉRATION UPIC, 2012. *Catalogue de mesures soutenant* la stratégie Cloud Computing des autorités suisses. 25 October 2012. E-Government Suisse.

ELECTRONIC FRONTIER FOUNDATION, [no date], PATRIOT Act. Electronic Frontier Foundation [online]. [Accessed 17 January 2016]. Available from: https://www.eff.org/issues/patriot-act

FERNANDES, Diogo A. B., SOARES, Liliana F. B., GOMES, João V., FREIRE, Mário M. and INÁCIO, Pedro R. M., 2014, Security issues in cloud environments: a survey. *International Journal of Information Security*. April 2014. Vol. 13, no. 2, p. 113–170.

GAEA, 2014, A Web Application to Monitor and Understand Energy Consumption in an Openstack Cloud. InIT Cloud Computing Lab [online]. 7 October 2014. [Accessed 15 January 2016]. Available from: http://blog.zhaw.ch/icclab/web-application-to-monitor-and-understand-energy/

THE GUARDIAN, 2015, Ireland, Facebook's European base, pushed to act on "safe harbour" ruling. The Guardian [online]. 7 October 2015. [Accessed 17 January 2016]. Available from: http://www.theguardian.com/technology/2015/oct/07/ireland-facebooks-european-base-pushed-to-act-on-safe-harbour-ruling

GUPTA, Udit, 2015, Comparison between security majors in virtual machine and linux containers. arXiv preprint arXiv:1507.07816 [online]. 2015. [Accessed 14 January 2016]. Available from: http://arxiv.org/abs/1507.07816

HON, Kuan, MILLARD, Christopher and WALDEN, Ian, 2012. Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now. *Stanford Technology Law Review*. 1 Fall 2012. Vol. 16, p. 79-126. Available from: https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/cloudcontracts.pdf

HSU, Pei-Fang, RAY, Soumya and LI-HSIEH, Yu-Yu, 2014. Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of* Information Management. August 2014. Vol. 34, no. 4, p. 474–488.

HUSSAINALI, Ladha, 2015, Security Control Guidelines for Cloud Services - ISO/IEC 27017:2015 | Cyber Security Community. [online]. 21 December 2015. [Accessed 17 January 2016]. Available from: https://securitycommunity.tcs.com/infosecsoapbox/articles/2015/12/21/isoiec-270172015-guidelines-security-controls-cloud-services

HWANG, K. and LI, D., [no date], Trusted cloud computing with secure resources and data coloring. Internet Computing, IEEE. Vol. 14, no. 5, p. 14–22.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2005. Information technology – security techniques – information security – managements systems – requirements. Geneva: ISO, October 10th 2005. ISO/IEC 27001.

ISAE 3402, 2016, ISAE 3402 - Overview. [online]. 2016. [Accessed 18 January 2016]. Available from: http://isae3402.com/ISAE3402_overview.html

ISO/IEC 20000 Certification, 2013. [online], [Accessed 17 January 2016]. Available from: http://www.isoiec20000certification.com/

ISO 27001 vs. ISO 27002, [no date]. *27001Academy* [online], [Accessed 17 January 2016]. Available from: http://advisera.com/27001academy/knowledgebase/iso-27001-vs-iso-27002/

KEMP, Richard, 2015. ISO 27018 and personal information in the cloud: First year scorecard, Computer Law and Security Review [online]. 8 June 2015. Vol XXX, p.1-3. [Accessed 15 June 2015]. Available from: http://www.sciencedirect.com/science/article/pii/S026736491500093X?via%3Dihub

KOLLER, Rodolphe, 2012. Top100: le secteur IT, bénéficiaire et contributeur de l'économie romande. ICT journal [online]. August 2012. Available from: http://www.alpict.com/multimedia/docs/2012/07/ICTjournal-juillet2012-top100.pdf

KOSUTIC, Dejan, [no date], ISO 27001 vs. ISO 27002. *27001Academy* [online]. [Accessed 17 January 2016]. Available from: http://advisera.com/27001academy/knowledgebase/iso-27001-vs-iso-27002/

KUMAR, S. and GOUDAR, R. H., 2012, Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. *Journal of Future Computer and Communication*. 2012. Vol. 1, no. 4, p. 356–360.

MELL, Peter and GRANCE, Tim, 2011, The NIST definition of cloud computing. [online]. 2011. [Accessed 14 January 2016]. Available from: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

MOORE, Susan, 2015, Gartner Says Demand for Enterprise Mobile Apps Will Outstrip Available Development Capacity Five to One. [online]. 16 June 2015. [Accessed 15 January 2016]. Available from: http://www.gartner.com/newsroom/id/3076817

MURP, 2014, Arcus – Understanding energy consumption in the cloud. InIT Cloud Computing Lab [online]. 14 January 2014. [Accessed 15 January 2016]. Available from: http://blog.zhaw.ch/icclab/category/projects/arcus-understanding-energy-consumption-in-the-cloud/

NKIDIAKA, Ndongala Brady, 2012, L'intégration du cloud computing au sein d'une PME genevoise [online]. Genève : Haute école de gestion. [Accessed 22 May 2015]. Available from: http://doc.rero.ch/record/209341

NOLLE, Tom, 2015, Avoid strapped IT budgets with cloud cost optimization. TechTarget [online]. May 2015. [Accessed 11 September 2015]. Available from: http://searchcloudcomputing.techtarget.com/tip/Avoid-strapped-IT-budgets-with-cloud-cost-optimization?utm_medium=EM

OPPENHEIM, Charles, 2012. Cloud Law and contract negotiation. El profesional de la información. [Online] September - October 2012. Vol. 21, no. 5, p. 453-457. [Accessed 12 June 2015]. Available from: http://recyt.fecyt.es/index.php/EPI/article/view/epi.2012.sep.02/17881

Our Vision | Exoscale, [2016]. [online], [Accessed 10 January 2016]. Available from: https://www.exoscale.ch/about-us/

PRODHAN, Georgina, 2015, U.S. sees new EU data-sharing pact within reach. Reuters [online]. 29 October 2015. [Accessed 17 January 2016]. Available from: http://www.reuters.com/article/us-eu-privacy-usa-idUSKCN0SN1O620151029

RAO, R. Velumadhava, and SELVAMANI, K, 2015. Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science* [online]. 17 April 2015. Vol. 48, p. 204-209. [Accessed 30 May 2015]. Available from: http://www.sciencedirect.com/science/article/pii/S1877050915006808

InterPARES - Records in the Cloud, [no date]. [online], [Accessed 17 January 2016]. Available from: http://www.recordsinthecloud.org/

REY, Lucienne, 2011. Cloud Computing: ein umnebeltes Thema [online]. Bern : Centre d'évaluation des choix technologiques TA-SWISS. [Accessed 25 March 2013]. Available from: http://www.ta-swiss.ch/?redirect=getfile.php&cmd[getfile][uid]=1943

SARAN, Cliff, 2015, Microsoft achieves ISO cloud certification. *ComputerWeekly* [online]. 17 February 2015. [Accessed 17 January 2016]. Available from: http://www.computerweekly.com/news/2240240498/Microsoft-achieves-ISO-cloud-certification

SAS 70 - Overview, 2016. [online], [Accessed 17 January 2016]. Available from: http://sas70.com/sas70_overview.html

SCHNEIDER, Jürg and STURNY, Monique, 2015, Switzerland. In : The Privacy, Data Protection and Cybersecurity Law Review [online]. 2. Law Business Research. p. 315–396. [Accessed 17 January 2016]. Available from: http://www.dataprotection.ch/fileadmin/dataprotection.ch/user_upload/redaktion/Docs/151229_Data_Privacy_Data_Protection_and_Cybersecurity_Chap._Switzerland_2nd_edition_JSchneider.pdf

SEYDTAGHIA, Anouch, 2014. Pourquoi les entreprises optent pour l'informatique en nuage. *Le Temps* [online]. Geneva, 18 March 2014. [Accessed 2 June 2015]. Available from: http://www.letemps.ch/Page/Uuid/95a96f20-adfd-11e3-ae93-6dabe775afc9

SINJILAWI, Yousef K., AL-NABHAN, Mohammad Q. and EMAD A. Abu-Shanab, 2014. Addressing Security and Privacy Issues in Cloud Computing. Journal of Emerging Technologies in Web Intelligence [On line]. May 2014. Vol. 6 no 2, p. 192-199. [Accessed 21 May 2015]. Available from: http://www.ojs.academypublisher.com/index.php/jetwi/article/view/jetwi0602192199/9465

SUN, Dawei, et al., 2011. Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Engineering [online]. 5 August 2011. Vol. 15, p. 2852-2856. [Accessed May 30 2015]. Available from: http://www.sciencedirect.com/science/article/pii/S1877705811020388

SWISSCOM, 2015, Swisscom marque la plate-forme Cloud de la nouvelle génération. Swisscom [online]. 12 February 2015. [Accessed 16 January 2016]. Available from: https://www.swisscom.ch/fr/business/enterprise/actualites/news/20150212-MM-Cloud-Plattform.html

SWITZERLAND, 1992. Federal Act on Data Protection (FADP) of 19 June 1992 (Status as of 1 January 2014) [online] 19 June 1992. RS 235.1. [Accessed January 17 2016]. Available from: https://www.admin.ch/opc/en/classified-compilation/19920153/201401010000/235.1.pdf

SWITZERLAND, 2014, FDPIC - Guide to cloud computing. [online]. 2014. [Accessed 17 January 2016]. Available from: http://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=en

SWITZERLAND, 2015, FDPIC - Transborder data flows. [online]. 2015. [Accessed 17 January 2016]. Available from: http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=en

SWITZERLAND, 2007, *CC 235.13 Ordinance of 28 September 2007 on Data Protection Certification (DPCO)* [online]. 28 September 2007. [Accessed 17 January 2016]. Available from: https://www.admin.ch/opc/en/classified-compilation/20071826/index.html

TMB, 2012, The InIT Cloud Computing Lab. InIT Cloud Computing Lab [online]. 20 May 2012. [Accessed 15 January 2016]. Available from: http://blog.zhaw.ch/icclab/the-init-cloud-computing-lab/

WAINEWRIGHT, Phil, 2014, Virtualization is dead, long live containerization. diginomica [online]. 2 July 2014. [Accessed 14 January 2016]. Available from: http://diginomica.com/2014/07/02/virtualization-dead-long-live-containerization/

WALDER WYSS AG, 2015, Political agreement on EU data protection reform. *dataprotection.ch* [online]. 18 December 2015. [Accessed 17 January 2016]. Available from:

http://www.dataprotection.ch/en/news-details/political-agreement-on-eu-data-protection-reform/

WALDER WYSS AG, [no date], National. *dataprotection.ch* [online]. [Accessed 17 January 2016]. Available from: http://www.dataprotection.ch/en/at-a-glance/legal-framework/national/

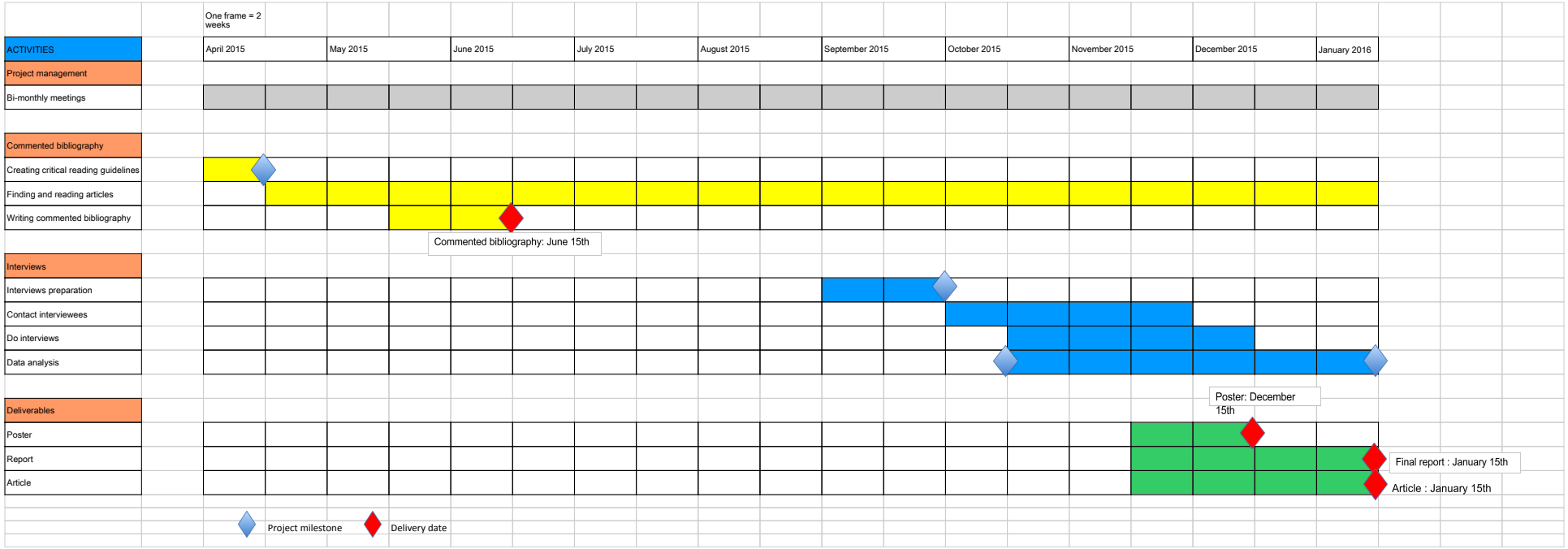
WHEELER, David A., 2015, Cloud Security: Virtualization, Containers, and Related Issues. David A. Wheeler's Personal Home Page [online]. 21 December 2015. [Accessed 14 January 2016]. Available from: http://www.dwheeler.com/essays/cloud-security-virtualization-containers.html

WHITLEY, Edgar A., WILLCOCKS, Leslie P. and VENTERS, Will, 2013. Privacy and Security in the Cloud: A Review of Guidance and Responses. Journal of International Technology and Information Management Volume [online]. 2013. Vol. 22, no. 3. [Accessed 10 January 2016]. Available from: http://personal.lse.ac.uk/whitley/allpubs/jitim2013.pdf

WU, Xu, 2015, A new trust model in cloud computing environments. International Journal of Hybrid Information Technology. 2015. Vol. 8, no. 3, p. 177–184.

YOUNIS, Younis A, MERABTO, Madjid and KIFAYAT, Kashif, 2014, Secure cloud computing for critical infrastructure: A survey. In: The 14th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting [online]. Liverpool. 14 November 2014. Available from: https://www.researchgate.net/publication/262817790_Secure_Cloud_Computing_for_Critical_Infrastructure_A_Survey

Annex 1: Calendar


One frame = 2 weeks
ACTIVITIES
April 2015
May 2015
June 2015
July 2015
August 2015
September 2015
October 2015
November 2015
December 2015
January 2016
Project management
Bi-monthly meetings
Commented bibliography
Creating critical reading guidelines
Finding and reading articles
Writing commented bibliography
Commented bibliography: June 15th
Interviews
Interviews preparation
Contact interviewees
Do interviews
Data analysis
Deliverables
Poster: December 15th
Poster
Report
Article
Final report : January 15th
Article : January 15th
Project milestone
Delivery date

Annex 2: Consent letter

Dear Sir/Madam,

We are a group of four students at the University of Applied Sciences of Western Switzerland - School of Business Administration (HEG of Geneva, Master's degree in Information science). As a part of our degree program, we participate in an international project doing a research on the state of cloud computing in Switzerland.

About the international project

Records In the Cloud (RIC http://www.recordsinthecloud.org) is a 4-year collaboration between the University of British Columbia (UBC) School of Library, Archival and Information Studies, the Faculty of Law, and the Sauder School of Business; the University of Washington School of Information; the University of North Carolina at Chapel Hill School of Information and Library Science; the Mid-Sweden University Department of Information Technology and Media; the University of Applied Sciences of Western Switzerland School of Business Administration; and the Cloud Security Alliance, supported by a Social Sciences and Humanities Research Council of Canada (SSHRC) Insight Grant.

Organizations are trusting cloud providers with their records and the RIC project intends to study the risks associated with security, accessibility, disposition and preservation issues.

Our involvement in the project

Specifically, our research seeks to study all the relevant aspects in order to implement "Records in the Cloud" in Switzerland. We shall focus on the German and French parts of this multilingual country, which account for 85% of the Swiss population.

The main purpose of our study is to suggest a set of good practices related to the use of cloud computing in the Swiss context.

To this purpose, five main objectives will be examined:

1. Describe the managerial aspects and risks of cloud services in Switzerland
2. Describe the economic aspects and risks of cloud services in Switzerland
3. Describe the legal aspects and risks of cloud services in Switzerland
4. Describe the security issues and challenges of cloud services in Switzerland
5. Describe the technological and technical aspects and risks of cloud services in Switzerland
6. Procedure

The interview in which you agree to take part will draw on your knowledge, experience and opinion about various aspects of cloud computing. This interview will be conducted by two students at a time mutually agreed upon by you and the researchers, either in person, over the

telephone, or by other means of electronic communication convenient to both. The session will last approximately 60-90 minutes. The interview questions will be sent to you prior to the scheduled interview, however no preparation is necessary. This interview will be digitally recorded and transcribed into textual format. Your participation is completely voluntary, and you may choose to end the interview at any time.

Confidentiality

Your identity will be kept confidential. There will be no personal information requested prior to, during the course of, or following the interview. All material will be stored in a secure location to which only the researchers of the RiC team will have access, and all computer files will be password-protected. Both the audio recording and the transcript will remain confidential and will be used only to facilitate the research. No identifying information will be used in any publication or presentation resulting from the research.

Potential risk

There are no known risks or potential risks from participating in this interview.

Contact for information about the study

If you have any questions or need to know more about the study, you can contact Basma MAKHLOUF SHABOU, professor at Haute école de gestion de Genève / University of Applied Sciences.

Phone number: +41 22 388 65 97

Email: basma.makhlouf-shabou@hesge.ch

Consent

Your participation in this study is entirely voluntary, and may be withdrawn at any time.

Your signature indicates that you consent to be interviewed for this study, and to have the interview recorded.

Annex 3: Interview grid

Dear Sir/Madam,

We are a group of four students at the University of Applied Sciences of Western Switzerland - Haute école de gestion de Genève (HEG of Geneva, Master's degree in Information science). In this context, we are participating in an international project doing a research on the state of cloud computing in Switzerland. This study is conducted under the supervision of our Professor: Dr Basma Makhlouf Shabou.

About the international project (RiC)

Records in the Cloud (RIC http://www.recordsinthecloud.org) is a 4-year collaboration between the University of British Columbia (UBC) and several European and North American universities. This study is supported by a Social Sciences and Humanities Research Council of Canada (SSHRC) Insight Grant.

Organizations are trusting cloud providers with their records and the RIC project intends to study the risks associated to security, accessibility, disposition and preservation processes.

Our involvement in the project (SWISS_RiC)

Specifically, our research seeks to study all the relevant aspects in order to implement "Records in the Cloud" in Switzerland. We shall focus on the German and French parts of this multilingual country, which account for 85% of the Swiss population.

The main purpose of our study is to suggest a set of good practices related to the use of cloud computing in the Swiss context.

To this purpose, five main objectives will be examined:

1. Describe the managerial aspects and risks of cloud services in Switzerland
2. Describe the economic aspects and risks of cloud services in Switzerland
3. Describe the legal aspects and risks of cloud services in Switzerland
4. Describe the security issues and challenges of cloud services in Switzerland
5. Describe the technological and technical aspects and risks of cloud services in Switzerland

This interview has been designed to investigate these issues from the point of view of the providers of cloud services. These questions have been provided to you prior to the interview for your information. They are not meant as a standardized questionnaire - rather, we encourage you to view them as speaking points or prompts to the larger topics that we wish to cover during the interview process. Equally, not all questions may pertain to your knowledge or area of expertise within your company - the questions are designed to offer you a sense of the areas we are investigating throughout the course of our study, rather than a firm script of what we intend to ask. The interview will be semi-structured, drawing when necessary on questions from the script on which you feel qualified to offer information or an opinion. Not all questions will be asked, and we expect the interview to last approximately 60 - 90 minutes. No

preparation is required or necessary. The answers you provide will be anonymized in the analysis. No personal information will be made public.

1. Introduction

1. Could you tell me your name and your position in the company?
    1. How long have you been in this position?
    2. How long have you been in this company?
2. What kind of cloud computing services does your company offer?
3. Is your company a cloud computing provider or does it collaborate with other cloud computing providers?
4. When did your company begin offering cloud services, and how has this evolved?

2. Managerial aspects

1. Are all your SLA's (Service Level Agreement) set in stone, or will the company negotiate or renegotiate each requirement with its clients when determining contractual obligations?
2. How do you contribute to support clients' information governance practices?
3. How long does it take to implement the service of the cloud within a company?
    1. Which method do you usually use, the bing-bang – all at once- or a slow roll-out?
    2. Are you in charge for the entire deployment mechanism?
4. After the implementation, are you in charge for the adoption and the training of the staff?
    1. Do you offer the possibility of a lifelong learning process or you make educational seminars at the beginning without further teaching sessions?
5. Is there the possibility to have a trial experience of your service before making the official contract?
6. How does the data hosting works, in which locations (city, canton, region) is it hosted and why did you select these locations? (With which criteria, financial matters? law concerns?)
7. When a customer cancels a subscription or terminates it, how does it go (off)?
    1. How long does the customer have to wait in order to get his data back?
    2. Do you provide any help for the transfer of data?
8. Does your company maintain a client data exit and recovery plan, should your business unexpectedly fold?

1. If the cloud architecture is maintained in proprietary code, what extraction tools or strategies does your company provide or guarantee in the case of sudden closure?
2. Would your company release source code to clients in the event of an unforeseen closure?

9. How does the cloud computing service works along with the retention schedule of your clients documents?
    1. If your clients have some data that, according to the retention schedule, needs to be destroyed, do you have policies to make sure that the data have been “shredded”?
    2. Could the clients check and audit those measures?
10. Has your company ever conducted a transfer of a client’s records to an archival institution?
    1. What issues, if any, were encountered in this process?

3. Economic aspects

1. Which are the economic advantages, for your clients, in choosing the cloud computing solutions offered by your company?
2. Do you use economic arguments to try and convince your clients of using your services?
3. Can we talk about a Return On Investment?
    1. If yes, how do you calculate it?
4. What are the pricing mechanisms? (One time license, monthly plan, “pay-as-you-go”?)
5. How many clients do you have at the moment?
    1. Are they in the public sector, private companies, NGO’s, international organizations?
    2. Mainly Swiss companies or international?
    3. Which field are they in?
    4. What size of business?
    5. In which countries are the companies’ infrastructures?

4. Legal aspects

1. If your company is international, are you subject to Swiss laws?
2. How do they compare to other legal systems in other countries?
    1. Are your policies, operations, and/or services around privacy and the protection of personal information different across countries and jurisdictions?

2. Concerning Swiss law on cloud computing, which procedures have been easier and which more complex in order for the company to operate in comparison with other countries?

3. What is required for national, cantonal and european legal compliance?

4. What procedures have you put in place to insure that those legislations are respected?

5. Are clients made aware of all data that you collect on their usage? What guarantees of anonymity and security are in place surrounding these practices, and can the client opt out of the data collection?

5. Security aspects

1. What measures or policies do you have for data security in your company?

2. Is data security an important point for your clients?
    1. How do you manage client's fear or hesitation about data security?

3. Do some of your clients have special demands concerning data security?

4. What kind of protection against malicious insiders and the misuse of client data by its employees and subcontractors does your company take? (E.g. Background checks? Certification? Legal contracts? Session and/or click monitoring?)

5. In the case of a security breach due to a malicious insider, is the client informed of the incident, the cause and the nature of the breach? How public is this information made?

6. What steps would your company take in such a case? Have there ever been criminal proceedings brought against an employee or subcontractor?
    1. What rights and/or compensations are awarded to a client in a case where you are at fault for data exposure or exploitation, if any?

7. Do you use a back-up system? Do you make duplications of the records or a printed version?

8. How do you deal with data loss? Do you have some sort of insurance policy?

9. Are there different levels of security?

10. Do you provide your clients with information about who is having access to their data if they request to know about it?

11. If your company has some subcontractor, do your require that your subcontractor have the same level of security and privacy policies as your own company?

12. Who is in charge for your customers data?

13. Do your clients know where their records are hosted?

1. Do they rather have them in Switzerland, or abroad, or they don't wander/ don't mind?

14. Do you make random tests to make sure that the data assigned to you from your customers are still present in your system and in a good shape?

6. Technology aspects

1. Can we combine the cloud computing application with other tools used for record management?

2. How much control do your clients have over their data?
    1. Can they visualize the state of their records using applications or software while using different devices? (PC, tablet, smartphone)
    2. Can they make modifications on the metadata of the records on their own?

3. How have the existing privacy legislation and requirements been factored into the controls and architecture of the system at your company?

4. What do you think about multi-tenancy?
    1. Do you offer your clients alternatives to a multi-tenancy model? (e.g. services based on a multi-instance architecture, etc.?)
    2. Do you offer insurance or other forms of protection for business losses resulting from a lack of access to records due to server seizure or other outages arising from a multi-tenant model?
    3. Do you provide clients with any information on who they share tenancy with? Do you know at any given time with whom your clients share tenancy?
    4. One of the critiques of multi-tenancy is that it can facilitate data mining by service providers, as client data is often held within a single database and/or application. For clients worried about privacy, how would you respond to these concerns?
    5. What does european, national and cantonal legislation require for multi-tenancy issues?

5. What do you think about vendor lock-in?
    1. Do you try to propose / suggest an open-source solution?
    2. What has your company done to ensure that the clients feel in control of their data/records at all times, including the ability to terminate the service without data loss?
    3. How can you assure the integrity and the authenticity of data?
    4. If there are data which are strictly confidential, do you use an cryption/encryption method?

7. Conclusion

1. Do you see an evolution in the kind of customers who request cloud services?

2. Have their demands changed over time?

3. Are there any best practices gained from your experience and adopted by your company on hosting a cloud computing service in Switzerland that you believe have been important assets?

4. Do you have anything to add? Is there any issue you believe we didn't treat/cover?

5. Are you willing to answer further questions at another time, should we need additional information?

Thank you for your interest and participation in the Records in the Cloud Research Project. Please feel free to contact members of our team with any further information you would like to share. As stated above, all interview data will be kept confidential, anonymized during its analysis, and destroyed after the public release of the research findings.

Annex 4: Interviews planning

	Company	Type	Internet site	Telephone	Address	link to online contact form	email	Person of contact	Kind of compan	Part of Switzerland	Method of 1st contact	Date of 1st contact	Student in charg	Reception of a reply	Date of the reply	Interview oppening	Date of the interview	Details: Where, when, name of person meeting	Student in charge of the interview	Interview accomplished	Comment
1	Safeswisscloud	Provider	https://www.safeswisscloud.ch		Alte Landstrasse 64, 8800 Thalwil			Prodosh Banerjee (CEO)	Swiss	German	E-mail	05/10/2015	Aurèle	Yes	14/10/2015						Positive reply to answer our questions by email, but do not reply for an interview
2	Swiss Cloud Computi	Provider	http://www.swisscag.ch				vito.critti@swisscag.ch	Vito Critti (CEO)	Swiss	German	E-mail	05/10/2015	Aurèle	No							
3	green.ch AG	Provider	http://www.green.ch/		Badstrasse 50 CH-5200 Brugg				Swiss	French and German	E-mail	07/10/2015	Aurèle	Yes	15/10/2015	No					
4	Exoscale	Provider	www.exoscale.ch	41 58 6685600	Avenue de Provence 4, Lausanne		sales@exoscale.ch	Antoine Coetsier, CEO	Swiss	French	E-mail	05/10/2015	Arina	Yes	05/10/2015	Yes	20/10/2015	Exoscale office in Lausanne, Marion and Arina	Arina	Yes	Positive reply was received from Exoscale/ CEO on the 5/10. After that we were in correspondance (around a week) trying to find the date and place of interview convenient for Mr. Coetsier.
5	DFI Service SA	Provider	www.dfi.ch	41 (0)22 706 2288	18, chemin des Aulx , 1228 Plan-les-Ouates Genève	https://www.dfi.ch/societe-it-suisse/contact.html	through website, isabelle@dfi.ch	Thierry Blanc, Director of governance	Swiss	French	Telephone	05/10/2015	Marion	Yes	07/10/2015	Yes	16/10/2015	DFI offices in Plan les Ouates, meeting with M. Blanc at 9am, Marion and Arina	Marion	Yes	
6	Innofield	Provider	https://innofield.com/	41 (0) 844 000 22	Brandschenkestrasse 150, 8002 Zurich		bojan@innofield.com	Bojan Jovanovic, co-founder	Swiss	German	E-mail	05/10/2015	Lucie	Yes	26/10/2015	Yes	19/11/2015	10.00 with Mr Jovanovic, in Zurich. Lucie present and Aurèle on skype	Lucie	Yes	The email adress belongs to one of the two owners of the company. After sending him an email on the 5/10 I received an automatic email that he will be back on the 13/10. / I wrote a second email on the 26/10 and he replied me that he would like to have an interview. On the 27/10 I proposed him 2 dates.
7	Cloud Sigma	Provider	https://www.cloudsigma.com/	Online chat	Badenerstrasse 549 , 8048 Zürich		info@cloudsigma.com 06/10 and patrick.baillie@cloudsigma.com	Robert Jenkins, CEO and Co-Founder and Patrick Baillie Co-Founder	Swiss	German	E-mail	05/10/2015	Lucie	No							Impossible to find any personal email or phone number of the company. 05/10 - I talked to someone using the online chat from their site and they suggested me to send an email to Patrick Baillie. So I did on the 14/10. / On the 28/10 I sent one more email to Mr. Baillie. No reply received.
8	Equinix	Works wit	http://www.equinix.ch/	41.43.508.4790	Hardstrasse 235, 8005 Zurich	http://www.equinix.ch/contact-us/general-inquiries/	online contact form 05/10 and servicedesk.ch@eu.equinix.com 14/10		International	French and German	E-mail	05/10/2015	Lucie	No							I called them on the 14/10 and they gave me an email adress to send my request and I must have a reply by the end of the week. Also the person on the phone explained me that the company doesn't provide c.c. but it's an Infraistructure aggregator and the main object on security concerns the physical security within the facility. Since it's a pretty big company, I believe that it's still important to see how they work even if they don't actually provide c.c.
9	Kodeo	Provider	http://www.kodeo.ch	022 870 40 00	Rue du Pré de la Fontaine 10, 1217 Satigny	http://www.kodeo.ch/contact/	sebastien.bajulaz@nginia.ch	Sebastien Bajulaz	Swiss	French	Telephone	05/10/2015	Marion	No							Sébastien Bajulaz was already interviewed by BSM, perhaps we should forget about him for now... Contacted again by email on 10.11
10	SyselCloud	Provider	https://www.syselcloud.ch	021 643 74 74	Chemin de Maillefer 36, 1052 Le Mont-sur-Lausanne		grégoire.galland@syselcloud.ch	Grégoire Galland, Technical director	Swiss	French	Telephone	05/10/2015	Marion	Yes	19/10/2015						Person is interested, will come back to me with a time and place. Edit: Person received the questions on 19/10/2015 and stopped replying emails
11	Interoute Managed S	Provider	http://www.interoute.com/office/switzerland	41 22 783 6300	Chemin de l'Epinglier 2, CH-1217 Meyrin (GE)		info@interoute.ch		International	French and German	E-mail	05/10/2015	Arina	No							
12	EVOK Genève	Provider	https://www.evok.com/fr/index.htm	41 22 552 90 80	Av. Cardinal-Mermillod 36, 1227 Carouge		geneve@evok.com		Swiss	French	E-mail	05/10/2015	Arina	No				On 20 th the letter was sent directly to CEO			
13	Rackspace Internatio	Works wit	http://www.rackspace.com/de	043 430 39 50	Pfingstweidstrasse 60, 8005 Zurich		Online chat	Lukas Appenzeller - Online chat and email sent	International	German	E-mail	14/10/2015	Lucie	Yes	14/10/2015					No	Sent an email after having an online chat. He replied the same day that he wants to help and then I sent him an email to try to get an interview. / On the 19/10 I received email from Simon Abrahams that he wants to do the interview, I replied with some dates and wait for confirmation. I never got a reply from him, so there was no interview afterall.
14	Swisscom	Provider	https://www.swisscom.ch/fr/business/enterprise/tendances/cloud.html	079 727 13 31			Eyup.Koc@swisscom.com	Eyup Koç (Senior Consultant)	Swiss	French and German	E-mail	14/10/2015	Aurèle	Yes	05/11/2015	Yes	13/11/2015	Swisscom office in Bern, Aurele and Lucie	Aurèle	Yes	
15	SWITCH	Provider	https://www.switch.ch/		Werdstrasse 2, Zurich		jens-christian.fischer@switch.ch	Jens-Christian Fischer	Swiss	French and German	E-mail	14/10/2015	Aurèle	Yes	14/10/2015	Yes	23/10/2015	Office of Switch, Lucie present and Aurele on skype	Aurèle	Yes	
16	Intersion Schweiz	Works wit	http://www.intersion.com/ch/	044 562 30 00	Sägereistrasse 35, 8152 Glattbrugg		ch.info@intersion.com 14/10 and info.ch@intersion.com 26/10		International	German	E-mail	14/10/2015	Lucie	Yes	02/11/2015				Lucie	No	I sent an email on the 14/10 to a general adress. I got no reply so I called and got an other email adress (again general) on the 26/10. / I received an email from the Director General, Mr Peter Moebius. He explained what the company does and asked me to confirm if I am interested on meeting. I confirmed that yes, I want a meeting and he replied that his PA will contact me for an appointment. / After having set a date, he cancelled. After having set a new date, he cancelled again. The interview didn't take place.
17	CAUSAL	Works wit	https://www.causal.ch/	41 26 301 30 14	Avenue de Tivoli 4, 1700 Fribourg		info@causal.ch, xavier@causal.ch	Xavier Perseguers	Swiss	French	E-mail	20/10/2015	Arina	No							
18	CISEL Informatique S	Provider	http://www.cisel.ch/		Route de la Sablière 1, Matran, 1753		contact@cisel.ch	Nicolas Roch-Neirey	Swiss	French	E-mail	20/10/2015	Arina	No							
19	Oracle	Works wit	http://www.oracle.com/ch-fr/index.html	41 56 483 31 11			clement.le.roux@oracle.com	Clement Le Roux	International	French and German	E-mail	02/11/2015	Lucie	No					Lucie	No	I used the online chat and talked to Clement Le Roux, he asked me to send all the documents at his email so he will send them to an appropriate person in order to answer our questions.
20	Servernest	Provider	https://www.servernest.com		Giessereistrasse 16, 8005 Zürich				Swiss	German	E-mail	04/11/2015	Aurèle	No							
21	Infomaniak	Provider	www.infomaniak.ch		26 avenue de la Praille, 1227 Carouge		simeon.gourlin@infomaniak.ch	Simeon Gourlin (System admin)	Swiss	French	E-mail	30/11/2015	Marion	Yes	11/12/2015	Yes	07/12/2015	Infomaniak office in Carouge, Marion and Arina	Marion	Yes	

Annex 5: Interview retranscriptions

Filename: 1. Exoscale Antoine Coetsier

Date of interview: 20th October 2015

Place: Exoscale offices, Avenue de Provence 4, Lausanne

Duration: 1:07:34

Interviewers: Marion Destraz, Arina Grazhenskaya

---

1. Introduction

AG: How long have you been in this position in your company?

AC: Since the beginning, because I was put strup of the company. In 2011 we founded this venture, which is called Exoscale. We incumbent by Vertigroup, which is in building that you in, in our separate entity, and we spent of Vertigroup last year. And now I'm more than 4 years in this position.

AG: What kind of cloud computing services does your company offer?

AC: Exoscale is only infrastructural service. And so we start with compute, elastic computing services and object storage. Then we have a marketplace of services, but we don't like to collect software services because it's many products used as… complementary products for infrastructural services. We define ourselves as being as a safe for cloud applications.

AG: Is your company a cloud computing provider or does it collaborate with other cloud computing providers?

AC: Both. We are a provider. And on the market place some services are done by us, and some services are done by partners. So we invite partners to expose their products on our market place and we have a revenue-sharing model. So customers can buy these imported services but some of them provided by partners most of the time still on their own infrastructure.

AG: And did your company started to provide these cloud services since its early beginning or later? And how you was evolved in this type of services?

AC: The company was registred in October 2011 and…but we are started the project a bit before this. But the real production was started in February 2012 and system had been operated.

MD: And it was always cloud services?

AC: Always, yes.

2. Managerial aspects

AG: Are all your SLA's (Service Level Agreement) set in stone, or will the company negotiate or renegotiate each requirement with its clients when determining contractual obligations?

AC: We have a pull of resources that are shared, and highly industrialized. And for this reason there are we two factors for the highest requirement from the customer. So we have a single set of terms of conditions that we evolve, but always ready to integrate the interest of customer. We do this for our German customers for already and… with addendums regarding the data protections. Because Germany is quite advanced regarding personal data protection, so we were required a set a documents that neither Swiss nor other jurisdictions taking place. But shortly, to be in the global aspect, because Europe is soon going to enforce the same set of rules as Germany. It's said to be voted by EU in December. Next year it will be a standard for us. And if we can work with it, we need to incorporate it for everybody.

AG: How do you contribute to support clients' information governance practices?

AC: Data? Data or information? I don't understand the question.

MD: Not necessary. Do you help your clients to manage the data and information inside their company?

AC: We certainly give guidelines. That's a nice offer. Just like as I was explained it, this data protection addendum – we can forward this to customers and tell them the procedure, what they need to do inside the company. But at no given time we have a look on the data, or we do not take ownership of the data. That's one clear statement on what term of condition that data is in all time is a property of our customers. And we also enforce a clear..., we call it "reversibility", so whether the issue, the contractual issue between us and our customers – that customers can always reclaim their data. This is something something that should be a requirement for all services.

AG: How long does it take to implement the service of the cloud within the company?

AC: For customer?

AG: Yes

AC: We like to say that you can start at least in 30 seconds! Well, we do this, as infrastructural service, we apply to the full definition. So, it's usage based, self-service and truly Internet and all five properties of the cloud computing are fully applied with Exoscale. Just go on-line, register and in 30 seconds you will have a virtual machine of storage running with us. So, with no phone call or manual account condition or what's ever to do with us. And when you start running work routs - the prices we publish on the website are usually vended by a month or the hour, because that's a common market expectation. We go down to the breakdown up to the minute. So, if you run your virtual machine for ten minutes you will only be charged for those 10 minutes.

AG: Are you in charge for the entire deployment mechanism?

AC: I'm not personally in charge for this. …Deployment mechanism for customers? No. We give tools for our customers to deploy. So, we give the documentation, recipes, automation scripts. We also provide support, but we don't do the deployment for customers. We are at the very bottom. The pure infrastructure. The responsibility of the customer to deploy the services or to have another partner deployed services for him. Therefor we have another partner who works, some people doing managerial services on behalf of the customers on top of the infrastructure.

AG: After the implementation, are you in charge for the adaptation and training of the stuff?

AC: No.

AG: It's not requested? Is somebody after implementation asking to explain some details?

AC: Yes, that's included; this is a part of the support. So, if there are questions regarding interface, or how to do this and that, they can ask and we'll provide guidelines.

AG: If there is a possibility to have a trial experience of your service before making the official contract?

AC: Yes, we do it, since it very easy to login, than you try and buy… I can give you some vouchers, if you like. We have alike some credit cards and we can hand out, and this credit activity or coupons of the Internet. Try to yourself and you can convert… We also have started programs for people that running educational programs for people and for students of startups, monthly free credit. So, they can start working with the project before getting coupon.

AG: How does the data hosting works, in which locations?

AC: We have 3 datacenters. Two of them are in Geneva area. And the third one we opened, more recently, last year – is in canton of Uri. It's sixty km south of Zurich. And it's in reconverted army bunker.

AG: And what was the reason why you selected these particular regions for your datacenters?

AC: We are already strong in Geneva. I mean two interests regarding allocation close to Zurich. That was, first, the best compromise. Actually we wanted to go further in distance then Zurich but… Anecdote: as example - if you want as cloud provider, you want to be considered – you need to have at least 2 locations separated by *20* of miles. So, we have them all. In Geneva – we advertised them as being Geneva and Zurich – two zones internationally well-known, and in development plans for Exoscale - we plan to expand out of Switzerland. Starting from the end of next year, in jurisdiction some sort of equivalence as Switzerland, but it's not easy to find. For sure, we'll not go to London or US.

AG: Did you pay attention for any financial moments, may be some legal aspects?

AC: Legal aspects? We have security frameworks or regulations.

AG: Legal frameworks for carrying data?

AC: Legal frameworks? Swiss law doesn't impose a way you do things. Ok? You do not have regulations for business, for Finmar, organisation which regulates the banking - they have a set of the best practices and what you must do, and you can order the datacenter against the Finmar requirements. That's not a law. You are not obliged to be a Finmar complaint. If you are in the banking business – yes, but it's not a law.

AG: And when the customer cancels a subscription or terminates it, how does it go? How long does the customer have to wait in order to get his data back?

AC: Instantaneous. The next minute!

AG: Do you provide any help for the transfer of the data back?

AC: Yes. It's part of our terms of conditions. If we want ourselves to terminate because the customer is in violation of our conditions, is doing illegal activities on the hosting, for example like spam or etc. If he'll ask - we'll back him data.

AG: Does your company maintain a client data exit and recovery plan; should your business unexpectedly fold?

AC: Of cause, ourselves, we have a disaster recovery plan for our own infrastructure and all backup services are continuing, etc. But for the services we provide to, since we are only providing, we have no aware of knowing of what data is located on the servers we provide to him. So, what we do is, that we provide data centers in Geneva, datacenter in Zurich and it's up to the customers to, if it's a critical information for him, it's up to him to deploy it in such a way the application. We provide the tools, but it up to the customers to implement it. Why it is such? Because we are not a software service; we are infrastructural services. We do not do automatic copies on behalf of the customer to the data centers. First, it will be expensive and the customers do not expect it.

AG: How does the cloud computing service works along with retention schedule of your clients' documents?

AC: That's not applicable question. Again, we provide only infrastructure. Press "delete", for example, on virtual machine and it will be deleted next ten seconds.

MD: Can you provide proofs that data has been destroyed?

AC: Not at the moment. But there is something we are working on to have two things. To have *loyally encryption and to date it*; and some kind of - for most *rangered* customers - because we can always say "yes, of cause, we destroy data". To looking out there is some ways to customer to be able to enforce client encryption. So we providing infrastructure, but we do not know what way it running. If the customer deletes or if the image, the data is still there, since we don't have the key. That's the way we are looking at this issue, but for example, for now it's not easy to implement it. Not aware if any infrastructural provider doing this, not of research at the moment on this. On the companies like Intel, also are implementing routines and CP user's system, so, as provider they can activate this.

AG: Has your company ever conducted a transfer of a client records to an archival institution?

AC: No, it's not applicable. That will be applicable if we were like a software service provider. That's not a case.

3. Economic aspects

MD: We'd like to assume the economic advantage for the clients in choosing of cloud computing solution.

AC: That's what we like to say!

MD: That's an argument for you

AC: Yes, it is. No investments - this one of the key things. And because of market pressure also the prices only go down. It's like telecom business and it's only going one way. So, yes. If you were to implement as a company the same service level as we provide as a cloud provider, it will be, if you come for everything - it will much more expensive then all we do. Why? Because

we have a bigger infrastructure and we share the cost. And this is only what we do so. Of course, we can be better!

MD: Is there a Return On Investment for the clients?

AC: Of course, yes.

MD: Do you know, how do they calculate this?

AC: Yes. It's something that we know only eventually, if we ask. Because…that's due to the question that is asked by medium to larger organisations where you still have people inside IT departments, that have not understood the benefits of cloud computing and internal fights between "let's go to the cloud because it's more secure and there are more guarantees for the company" and people that still want to do everything in house . So, it's difficult to get on our side the real numbers, sometimes we had examples where the numbers … were built on the price of the electricity, repair… and we know them very well because we are completely of, sort of the balance was unreal. But if the exercises on correctly with real life numbers without forgiving about the cooling, even if that foreseen to like general costs of someone's building, then it is no debate. It's always more expensive.

MD: We talk about pricing mechanisms, can you tell us more about it? One time license, monthly plan, pay-as-you-go"?

AC: Everything is by the hour. Our processing is by the hour or if it's storage it's by size of storage, by gigabyte unit. I can show you. On your invoice, for example, you have a medium-size virtual machine. So, for given month you have 200 hours or 2000 hours that will mean that you have much bigger machine, because there are 730 hours of average per month. So, it's a wrong number of hours with one digit after the 2 digits... Because it's go down to the minute.

MD: Can we talk about you clients?

AC: Sure.

MD: How many do you have?

AC: Exoscale has 1500 customers at the moment. We do as mainly…, the biggest *vertical are* people in a software services business.

MD: So, mostly companies – are they international or more Swiss?

AC: It was 50/50 before the summer. I should to refresh it. It's about 55% Swiss and others - people from other locations, people from Latin America using the services with us. It's a bit away because the whole Atlantic is in between us.

MD: Are they big companies or the small ones?

AC: At any given size. But the typical customer - you can call them "startups" or software startups, which are shifting to software license online. It's typically companies with 5 to 15 employees. Very technical, very development oriented with business on online products.

4. Legal aspects

MD: we are coming back to legal aspects… So, you are Swiss company. So, you are a subject of Swiss laws. Do you know what a legal system says in comparison with other countries regards to data manipulation? What you allowed to do or not?

AC: Yes. That's is an area in which we trying to stay very much aware. I can explaining European regulations and so forth. Right now my fears that are DPA is going to be…quite soon obsolete and what we are doing now is going to set as back tremendously.

MD: Why is that?

AC: Because there is a new version of European law will be global, uniformised for all European countries and it's much more complete than what we have in the Federal DPA.

MD: Do you have procedures about to put in place and ensure that current legislation is respected?

AC: For us? As a practice? Yes, what we do regarding security, is that we comply with a framework that is the cloud security alliance. Don't know if you are aware of it. We've chosen this framework because instead of *ISO* (there are a lot of ones). Because it's the one that covers not only on just the datacenter or the support system, but covers all the cloud provider's service. So, it's goes from the bottom, from the physical access to the data centers, up to our bidding systems, in HR, etc. So, it's more than 130 controls, that we check regularly. And when we do something we engineer it against those controls.

MD: And do you collect data on your clients?

AC: Yes, sure. We must collect their address, etc. So, we have data classification policy, it's public. It's in the website. You can go and check it. And we have different levels of protection regarding this data. And that we also apply on our system whether it's only just the name or it goes up to the banking records of customers, biding records and stuff like this. So, there is a whole set of data that we also communicate, but it's public.

MD: Are clients made aware of all data that you collect on their usage ?

AC: Yes, because this the minimum set of the data we need to operate this business.

5. Security aspects

MD: What measures or policies do you have for data security in your company?

AC: Cloud security alliance we could go through all of them! It's pretty deep.

MD: Is it (security) an important point for your clients?

AC: Sure. It's part of our values. Our logo would not be read. We define ourselves as being first and simple experience, but it's one of our first values. Second is our name you know, to offer something that is "scalable", and the last one is also to do more about security. So, about being transparent, about providing all this direct classification and still be in a country that it's quite good still for lawful access to data. I mean if you have a request from authorities with procedures are quite transparent and knowledgeable for the customers. Which is not the case in the USA, where there is a data access without you knowing, that's the worst.

MD: And how do you manage client's fear or hesitation about data security?

AC: It's a lot about still education. What we are doing? How do we operate. When they ask to meet us that can be part of our presentation. Apart from this, we don't have some special department that goes into customers business *and help* them re-do their internal policy and etc., that would be too costly before us. We don't have the size for this. It's not more than this. We can also give guidance to encrypt or some technical best practices. But that's it. But there are no magic solutions there.

MD: Do some of your clients have special demands concerning data security?

AC: The one that we do not provide, and we already talked about this, is "kind side encryption". But in infrastructural level it has the ability to, for example, run virtual machine without being able to access to, any manner possible. But for example at the moment there is no practical solution for this.

MD: Do you have protection against, for example, malicious insiders inside your company? Do your employees get checked?

AC: Yes, sure. It's also a part of cloud security alliance control. It controls on the HR part we do background check, a lot of requirements. They are also strengthen policy for employees that we don't use password and it's only *strong authentication* with public keys and etc. so it goes pretty far away. We have role-based access. So someone that is in accounting can not do technical stuff and vice versa. Everything is locked. What was done in the system, the changes - that's also a security matter plus if you look at ITIL, how to manage IT system, it's also a requirement there, it complies for both.

MD: In the case of a security breach due to a malicious insider, is the client informed of the incident, the cause and the nature of the breach?

AC: Yes, we put it in our terms also. This is different. The next EU law will be much more strange on any provider. To reveal the data at the moment, on the DPA, there is no indication of time, or procedure on how to do it. In the next version of the EU law – you have to -I do not remember – but it's very short - you have to also reported to authorities, etc. So, requirements are much higher. I think it's a better protection.

MD: If there was such an incident, what steps would you take? Would there be criminal proceedings?

AC: It depends on the nature.

MD: And would you give compensation to the client? If you were at fault.

AC: Sure, we have SLA's, and penalties. So, this system will mostly apply.

MD: Do you use a backup system? Do you make duplications of the records or a printed version?

AC: That is also something that we covered already. All the data, that we have on the customers that is required for providing the service, yes, we have a replication system and we have back-ups. But if they create a virtual machine – we don't have an automatic backup of this. So, if it gets destroyed or altered in any way, and if the customer hasn't done this on his side – as in setting-up some system - it will be lost. It's by design, it's because of our businesses. Because we are doing only infrastructure as a service. If we would be higher up the stack, then yes, we would have all the systems because the customers would not have access to those parts.

MD: Do you have a kind of insurance policy if you lose customer's data?

AC: Yes, but it's quite limited. That's an area, which is still grey; with insurance companies too.

MD: If your clients require any information about who is having access to their data do you provide it, do you give the names of people working for you?

AC: No. We provide if the *control is the fact that we do the background check* of our employees. It's our requirement regarding cloud security. We could allow this for customer to have an external auditor come and check those. The reason why we do this it's because it will be too much time' consuming. If an external auditor and data result can be then shared or reused - no problem. We had this in the past. And people auditing data centers and operation procedures. We've done it but it's not systematic; and the cost is to be billed by the customer.

MD: Do your clients know where their records are hosted?

AC: Yes, it's also public on our website. For example, if it takes a product in the marketplace, we specifically say who is the provider, where is the data stored, etc.

MD: Is it an argument for them that those data centers are in Switzerland?

AC: Sure.

MD: Why?

AC: Honest answer or marketing answer? Honestly, there is nothing, almost nothing that can prevent a company today to, even a Swiss company, to stores its data elsewhere. I mean, It's only a matter of having the right internal documentation implies and terms of conditions with a customer. But it's the misbelief *in* the poor knowledge of the field that most of the time conclude to "My data must stay in Switzerland". That's *very* for the Swiss customers. Why it's true this? *Law*ful access to data is much better in our country than in other countries. Even Europe. So, that's the real strong argument. It's for any authority to access data; you need to have *judge file a ruling,* you need to also notified the n customer that the data will be handed over. Those things can happen very differently in other countries. That's a real key advantage for international clients.

6. Technology aspects

AG: Can we combine the cloud computing application with other tools used for record management?

AC: Hmm…it will be true for the software services, for CRM, on IP solutions, but not for infrastructural service. …Not applicable!

AG: How much control do your clients have over their data?

AC: Full control.

AG: And how can they visualize the state of their records using applications or software while using different devices?

AC: The software is in their responsibility.

AG: Can they make modifications on the metadata of the records on their own?

AC: Yes.

AG: How have the existing privacy legislation and requirements been factored into the controls and architecture of the system at your company?

AC: By designers from the ground up. I mean, we've built this to be…; as the the company is quite knowing ? Young. And we've built everything to be complied with those frameworks. To the way we develop, the way we push new versions into projection, etc., it's done in such a way to enforce the controls that we have regarding security. Accounting, reversibility, change management, change approval - review the fact that someone's approved someone else' work, etc. All those both good practices in security control are enforced from the ground up.

AG: And what do you think about multi-tenancy?

AC: It's an only way to go. I usually compare it (*cloud computing*) to banking. May be two centuries ago you had some treasure chest, or you will store your gold as a private individual, even as a company which used some vault or staff like this. This is not happen any more and it's a long time now since even individuals and companies all financial assets are stored at the bank. So, the banks as a provider in its multi-tenancy, they are aggregate money of everybody and managed it for you. Cloud computing is just the same. We used to having companies *with* little computing power with utilization ratio. They could break down, etc. Cloud computing is just like utility business, just like banking, so we providing the massive scale of computing and giving slices of this to customers. Just like banking is done.

AG: Does it mean that you don't offer alternatives to a multi-tenancy model?

AC: No.

MD: Do they ask for it?

AC: If they ask for it - they are not customers for us.

AG: Do you offer insurance or other forms of protection for business losses resulting from a lack of access to records?

AC: No. We have a penalty system in place. If this takes place and a system is not available, we will enforce in 9995, so more than 4 hours. That's a couple of minutes per month when we interned in the system. So, if the system is only been available like 90 percent of the time in September – then we give back credit to the customer. The month will be free for this specific virtual machine that was not been available. If the customer was running on this system - this system was not back to open, not replicated and the system was making…, I do not know…If was earning million per month on this system, but if they will be costing only 15 franks because that's which we operate. We will not give back one million. We will only give back 3 franks because the instance was available.

AG: And do you provide clients with any information on who they share tenancy with? Who else has data in this datacenter?

AC: No.

AG: And do you know at any given time with whom your clients share tenancy?

AC: No. It's quite difficult to know. Any given time we can look where exactly the customer workloads are. But if this moving, this is an orchestration. And for some point in 2014 we've

launched twenty five thousand virtual machines. That's more then one day or more than an hour, if you count right. That's a scale, which we operate.

AG: One of the critiques of multi-tenancy is that it can facilitate data mining by service providers, as client data is often held within a single database and/or application. For clients worried about privacy, how would you respond to these concerns?

AC: That is not applicable. It will be true, again, for software service if you have CRM as a service, then, of cause, you have annual database, you have multiple customers and you can do some trends of the lawyer offices. They have dosen kinds of customers. So, you can do trends and do data analytics on this. Does not really apply with us. We can do this, we could say "Customers in this field area they can to run lots of small instances". Customers, for example, in transportation - where they run small range of instances. But we don't have access to what's inside. We can't say customers in transportation…I don't know…they *are* customers themselves because at this stage, that we can't do. We can do this, of cause, due to the type of customers, the size, from the data we know and that we told our customers: "we will be using it", but that's it.

AG: Again, little bit about legislation. What does european, national and cantonal legislation require for multi-tenancy issues? Is there some specific requirements?

AC: Yes. The requirements are that you must put the measures in place. That is sufficiently separated. What is "sufficiently" mean? For us it means to be at the best level of stage of engineering. But this is IT, if you put down your security *pitches* and box of the software. It's about us: always think of top of this and making sure that our systems are updated and always *approved* between tenancy. But that's applicable everywhere.

…Just simplify to go to cloud provider: the level of those issues, most of the time, even for large companies that's a benefit of using of cloud computing. For example, every fifteen day we make audit. We go through the full list of datacenter access and check if everybody are still all right to access the datacenter. I don't know, if any private company doing this… And, so, we keep a record of it, we archive it – but it's also a business - to provide infrastructure. We industrialize this. Just like a milk' producers - we check a milk everyday! Is it good? Yes. It's a quality control. We do a lot of quality control. It's the main our focus.

AG: And what do think about vendor lock-in?

AC: We hate it. We only use open-source. We are big open-source contributors too. For example, one of products to main products – computing and object storage – are paste on open-source solutions. In both projects, when we are contributors to the project; the other one, when we are the authors - it's also public. So, our own software we used to provide the service - we've made it available on open-source. It's a way also for us to show…, that you can go ahead, you can audit it (the software). It's the same software that we are running for the projection version.

AG: What has your company done to ensure that the clients feel in control of their data at all times, including the ability to terminate the service without data loss?

AC: So, it's self-service, they can do it any time, they can delete virtual machines and we have provisions and terms of conditions that serve to enforce the reversibility clause. It's both: technical – at any given time you can delete and there is also contractual obligation in the Terms of conditions.

AG: How can you assure the integrity and the authenticity of data?

AC: It's really depend of the size we have to give back. Some formats, the integrity is ..?.., others – aren't. If they aren't – we are make an archive and people can check it at the end.

AG: If there are data, which are strictly confidential, do you use an cryption/encryption method?

AC: Yes. You can read about it in a data classification. There are 5 classes.

7. Conclusion

MD: Do you see an evolution in the kind of customers who request cloud services?

AC: Yes, mostly. For us 2014 has been a real shift in cloud adoption, specifically in Switzerland. A statement from customers went from " it's interesting" to "I need it". I think we are now passed the early adopters. It's going into massive stream. It's still helpful infrastructure, that is running, to convert, just for the purpose of converting to cloud computing. But if they have a new project, a new version, a new venture in a company - if we can be in the mind of decision maker at this time – in most of the cases – it's a win. Because the advantages, the rapidity, scalability is the gains are right there.

MD: Have their demands changed over time?

AC: Shure. I can give you a concrete example. In 2013 looking at the market, we strongly believe that platforms like IRUKU (?), so platform as a service, was a way to go. For us it was moving from infrastructural service to offer a system that's closer to developers. And if people still less care about how this service is run, all be done automatically… So, we internally discussed a long time about should we provide such a service. We said "yes". Should we provide an engineer service and spend our company resources for building it? It was a long debate. At the end we choose to publish the service on the market place. We have now, as a partner, doing the platform as a service on our own infrastructure. Now, looking back, platform as a service has been something trendy, but the adoption is not quite there. There are lots of constrains for people building an applications for developers. And in the recent success of DOCKER is shifting all the ways in this direction. So, what we looking out to the future is, may be, sun setting of the platform as a service offering something, that's more in the way of DOCKER or containerization as a service. There is more flexibility now at platform as a service. That's hard topic at the moment and most advanced customers are experimenting and asking about it. This is likely shift will be doing in the next 12 -18 months.

MD: Are there best practices gained from your experience and adopted by your company on hosting a cloud computing service in Switzerland that you believe have been important assets? General advice? General recommendation?

AC: It's very depend of the field. One… general recommendation is that… do you know about OpenStack? It's the most popular software to do the cloud *…stration*?, to do the main part of *IF* service and to enforce multi-tenancy. Public cloud is based on OpenStack. Why I say? It's free. But it's not sufficient to be a cloud provider, just installing the software, just installing an OpenStack. If you'll do 50 percent of the business, but it's …the other 50 percent of that matter. So, it's all the user' expense, it's all the support system is all the *beating* experiments. So, that matter to *endorse* - you cannot find after shelf solutions. And you have to build your own company' version, company' image of this. That's been our experience.

MD: Thank you! If there is anything we did not cover?

AC: It was rather pretty detailed regarding security and data protection.

Filename: 2. SWITCH Jens-Christian Fischer

Date of interview: 23rd October 2015

Place: SWITCH office, Werdstrasse 2, Zurich

Duration: 1:06:34

Interviewers: Aurèle Nicolet, Lucie Petrelis

---

1. Introduction

LP: You have just to sign. Ok. Wonderful. We have questions for you. So we can do it together. So we split the questions. First of all, can you tell me your name and your position in the company.

JCF: My name is Jens-Christian Fischer. I'm a Team leader at SWITCH for data which concerns with the cloud, building the cloud and also the product owner of our cloud product *SWITCHengines*. I have been in this position for 4 months now, as a team leader and the product owner for about a year.

LP: Always in SWITCH?

JCF: Always in SWITCH, yeah.

LP: Just globally your professional background?

JCF: Umh… I have been self-taught in IT a long time ago. I've been working in various companies doing office automations in the 90s. I worked at ABB, the industrial corporation with Lotus Notes and intranet, then I've been self-employed for about 15 years at my company that did consulting on various kinds of software development. I was a part of various start-ups that didn't work out that well. The last one was some kind of mobile payment scheme in Switzerland. And I've been in SWITCH for a bit over two and half years now.

LP: All right.

JCF: As a cloud, in the cloud team, cloud engineering.

LP: Ok. Umh… What kind of cloud computing services does SWITCH company offer?

JCF: There are basically two things. We have infrastructure as a service offering called *SWITCHengines*, which is an OpenStack based umh… cloud that is located in Zurich and Lausanne, that we have build up as a product, and we will be starting to sale to the universities and academies in Switzerland, starting next year… We've been using it internally for various other services and it's been in pilot for everybody that are interested has to be able to get access, to be able to run stuff on it. The other service we offer is a software service called *SWITCHdrive* , which is a Synch and Share service that is based on owned cloud, open-source cloud. It's basically a Dropbox replacement. That have been in production for a year now. More than a year. It is open to all Swiss universities, students, faculty members. If they opt to use it and buy it. And we're, they'll start to have to pay by next year, so we're recruiting customers, paying customers, for that as well. Those are our two main cloud services.

LP: Yes. And you? You work mostly with which part?

JCF: I work with both. *SWITCHdrive* is running as kind of gallery of SWITCHengines, we use, we want to eat our own dog food, build a cloud and run service on it so what I did is, I both worked on the implementation of the infrastructure but also built the virtual infrastructure to run

SWITCHdrive on it. So I work on both, but now the focus is on infrastructure,somebody else is working on SWITCHdrive.

LP: So. Is your company a cloud computing provider or does it collaborate with other cloud computing providers?

JCF: We provide our own cloud services, our own cloud. Umh… But we talk with others, there is kind of an interest in federating cloud, we have had requests for being able to burst capacity using our cloud. There is nothing in particular that has been done already. It's something that might or might not happen in the future. But otherwise we are not reselling outer services, we are building our own.

LP: Ok. When did SWITCH company begin offering cloud services, and how has this evolved?

JCF: It started about 3 years ago with the idea that which should take a look at cloud, because it would become an important topic. We started with a pilot project, built a very small cloud, see if we could get it up and running, and when we saw that it's all good we decided to go ahead and build a product out of it So the actual offering is maybe a year ago as a pilot and now as a real product starting in January of 2016.

2. Managerial aspects

LP: Ok. Now we are gonna pass to the managerial aspects. Aurèle, are you ready?

AN: Yes, I'm ready. Ok. Are all your SLA's (Service Level Agreement) set in stone, or will the company negotiate or renegotiate each requirement with its clients when determining contractual obligations?

JCF: Ok. We try to have one service level agreement for everybody. But this is something that is new to us. SWITCH traditionally hasn't had any service level agreement… our customers are in general IT department of universities. We provide the internet LAN. There are no service level agreements. It's all on a best effort basis But we see with the new generation of IT managers coming into the universities there's a demand for SLA. So we want to keep one. But we want to keep one, just one SLA for everybody. But we will negotiate things with them, of course We cannot… well...It's one of the problems being designed at the moment.

AN: It's a Standard Service Level Agreement

JCF: Yes, because it is not a service yet that people pay for. We don't have to provide Service Level Agreement but we're working on having them ready for January, when people have to pay for it.

AN: How do you contribute to support clients' information governance practices?

JCF: That's a good question. I have no answer for you, because we haven't have that coming up yet. We are in talks with, not with governance but with data protection with … universities and that's difficult, because in Switzerland we have 26 different data protection standards. So every canton has its own Again we try, our legal department tries to wrap that up in one. Our interest is to have our infrastructures kind of certified as being part of the universities infrastructure network, they can apply the same data protection level as they would with their own IT. some universities it's work, some of them it doesn't. It's an ongoing process.

And other than that we don't have yet any kind of governance, like Health or EPA or financial stuff.That doesn't come to us yet. I'm sure it will, at some point. We'll see what happens. Of course, we are interested in having if necessary, having those certifications and help the customers with support.

AN: Is it essentially security aspect?

JCF: I'm not sure to understand the question.

AN: Is it essentially a security aspect?

JCF Oh… It's a part of it is security, yes. We're looking at the ISO 27001 standard, we're not complying to that, because the person who knew most of that has left, so. But it's something we have on the road map, but not with a very high priority at the moment. If somebody asks for it and says, we can only use your cloud if you have that, and we will pay huge amounts of money then we will…

LP: …consider…

JCF: We will reprioritize things like that.

AN: How long does it take to implement the service of the cloud within a company?

JCF: So within SWITCH or within to…

LP: SWITCH tries to implement the cloud in the universities or…

JCF: There are two aspects of that. The first we have to build our own, the cloud infrastructure itself, first. So that takes, if you count, from the start of the project to now, three years maybe one and half year for the current product service and there's also the cycle of going to the universities and getting them on board as customers, which is more of a sales cycle that you have to go through. And it's hard to tell, it can go very fast if the university sees and ease, that they absolutely want to do that and it takes a phone call and a meeting but sometimes it takes a lot longer. But in general we find that just rolling out a service into the universities is a process takes maybe a year or longer, because everything is moving very slow, we are not completely free in our offerings We are a foundation, there is a board, governance board that governs us, which is made up of the universities, we belong to the universities and they only meet once or twice a year and big decisions like even the pricing for the cloud need to be approved by that board, by that governance board. So it can take up to a year to just have decisions on things that you can then offer to the university and they themselves have a relatively long investment cycle. It could go fast. But, if you go back to the technical implementation, see you the next question is big bang or slow roll-out, I'm a big fan of continual improvement, so we roll-out something just minimum variable product if you will and then to continue improvement so that we would never be out with the cloud service if you have try to engineer to be fully functional and finished and so on.

AN: After the implementation, are you in charge for the adoption and the training of the staff?

JCF: What are you asking? For whom are you asking? For my team or for…

LP: For the clients.

JCF: For the clients. In the universities?

LP: Yes.

AN: Yes.

JCF: No, we're not. We would offer some kind of training. We have, we will do workshops and so on. But it's voluntary, of course. We provide materials, we have documentation, we have collaboration to … for and so on. It is something we can just put out there and offer and hope that somebody's using it. We're not forcing our customers to use that. So, no, we're not in charge of that. It's the customers themselves can decide what they want...

LP: But the material is available?

JCF: The material is available, yes.

LP: Very good.

AN: Is there the possibility to have a trial experience of your service before making the official contract?

JCF: Absolutely, of course. Right now is a service pilot, so send us an email you get access to the cloud and if we're in talks with the universities then it's of course you give them trial accounts. We help you set your test environment and… yeah, absolutely.

LP: Do you have any idea since next year on the service is going to be payable, they're still gonna have a trial and stuff like that?

JCF: It depends. Traditionally our services have been sold directly to the university, to the IT department of the universities. So the university has opted in to a service, sometimes that's very simple opt-in. If you want network connectivity, you know, you have to buy our cable; sometimes it's an offering like SWITCHdrive, the synch'n'share, you can buy it for your university and your student but you don't have to. And with our cloud offering it becomes even more fragmented, if you will, because our customers are not the IT departments in the university. A priori it could be researchers, it could be research projects, it could be lecturers, it could be students, it could be many things. And while we're well equipped to deal with the IT departments and give them access to that, if a university says, "oh, it's fine, you can just go and talk to our researchers or whatever directly, then it depends if… We will help them with trial accounts and get them up and running, yes, but we don't have a formal process. Luckily we're small enough that we can handle all of that manually at the moment. But if things go as we envision them, then it becomes a total self-service. You sign up with maybe a credit card and you get a month free and then you get the invoices… It's not decided yet. We want to make it easy to people to come to us and making it easy also means lower the barrier, of course.

AN: How does the data hosting work? In which locations, city, canton, region is it hosted and why did you select these locations?

JCF: We have two data centers at the moment, one in Zürich, in the canton of Zürich, in the Zürich region, and the other one is in Lausanne, at the Université of Lausanne and the other at the ZHDK (Zuricher Hochshule der Kunste). So the data centers are in universities and we selected those regions because both of these universities have spare capacity in their data centers and they're willing to sell us that capacity. The ZHDK in Zürich is a new building, brand new, they just moved in and have tons of space and in Lausanne there's also enough amount of space. And we have traditionally, again, worked with the universities and can use their data centers and so on. And we wanted to have a geographic separation, also, of our two data centers and then there's the political aspect of having something in the Waadt land and one in the German speaking part of… If we had to open a third data center it will be in Ticino. These are the main reasons. And financials have, yes, one is more expensive than the other but in the end it was a matter of having access to enough room to grow into. We have spare capacity, we can fill that up as time goes by.

AN: When a customer cancels a subscription or terminates it, how does it go?

JCF: There are various implications to that, because what is a customer? If we're talking for example about the SWITCHdrive service, where the customer is the university but the end user is a staff member of a faculty member, if that faculty member leaves the university, whose data is it? Is it his data or is it the university's data? It's not a very simple question to answer. Same goes for infrastructure, if you have a research team in a university and they having data

analysis and one staff members leaves, his data, or is it the university's data? It's on a case by case basis that we do that. For SWITCHdrive, for the synch'n'share, the user has, it's his data, the data is on his local computer anyway, so there's nothing more stored on our servers than what he has on his data. For the Infrastructure as a service, basically he has full access to the storage or the virtual machines that he has, so he can take the data that he needs if and when he cancels. And other than that we have to work that out with the IT departments of the universities, on how specific cases should be handled.

LP: And if we presume that there is a university that wants to stop working with you, how does that work?

JCF: We don't want that.

LP: No, of course not! But just as an example. How long does it take for them to take all their data back?

JCF: Basically we would help them transfer that data immediately, effectively immediately and work with them to get the data out to them and then we delete it and remove it.

LP: So it's quite fast. It's a fast procedure.

JCF: Yeah, of course. What do you mean, cancelling a customer. We don't have. Nobody can cancel. And yes, we provide help to transfer the data. Absolutely.

AN: Does your company maintain client data exit? What do you plan, should your business unexpectedly fold?

JCF: I don't think we ever considered that option, to be honest. Because we don't expect to fold. We're not a privately owned company, so we are in a different situation, we really belong to the universities. We're not a for profit organisation. We're a foundation, we have, the board is made up of the universities and the government.

LP: That's an important point.

JCF: Exactly. So I don't think we will fold like a normal company would fold. So I don't think there is any contingency plans in that respect.

LP: That makes sense.

AN: How does the cloud computing service work along with the retention schedule of your clients' data?

JCF: Basically, it doesn't. Because we don't know what our clients are doing. We provide the infrastructure. If we now look at the Infrastructure as a service, we just provide the infrastructure and it's up to the client to handle data retention and so on. We will keep data safe, we will store it but we don't know what's in it. Same goes for shredding. If we go with the next question. It's up to the customer, we provide a virtual hard disk, it's up to him to shred that or delete that. At the end it goes up in the big bucket in the sky. There is no physical… There is a physical manifestation of it but we have no possibility of recreating that once the client has deleted his data. In that specific kind of service, I don't think there is an issue. We can't even help with data retention and lifecycle management.

LP: Not yet, at least.

JCF: Not yet. There are products on the way for the LCM (data lifecycle management), but so far nothing is ready for customers yet.

3. Economic aspects

AN: I think we can move to the economic aspects. Lucie, you agree? Which are the economic advantages for your clients in choosing the cloud computing services offered by SWITCH company?

JCF: Compared to their own services? Or compared to competitors?

LP: To competitors.

JCF: To competitors… I think the cloud marketing itself is extremely competitive. We have priced ourselves to be in line with the competing services like Amazon or Swiss providers. I'm not sure we can even provide an economic advantage, compared to somebody like Amazon or Microsoft or Google or whatever, with quasi unlimited funds and unlimited scale. There are other advantages by using our cloud, but those are more based on the location of the data, Swiss laws, regulations; that the cloud is connected to the same network that the university is connected to, so there is no data being handled outside of the university's network. And there's an advantage of us having worked with the universities for over 25 years, so we are often seen as a partner to the university and not as a…

LP: Sales or client...

JCF: Exactly, yes. Sales relationship. Those are the advantages that we have primarily. Plus we are able to work with the universities budget cycle and payment cycles and so on. We're quite flexible on how we structure the tariffs, we can kind of give the university a quote and they can redistribute the quote among research projects, we can keep track of which research project has accumulated how much computing capacity, and all of these things. We think that we can, by working that closely with universities and understanding how they work, we can make it easier for them, than if they have to handle their researchers with a credit card and buy resources on Amazon. So it's not economic arguments that we are using primarily, to answer the next question that's coming up, but the infrastructure and legal and closeness to their business arguments.

AN: What are the pricing mechanisms? (One time license, monthly plan, "pay-as-you-go"?

JCF: OK. It's pay-as-you-go. We charge two models. We will keep track of the usage and we will bill in a three months cycle. So every three months the customer will get a bill for the accumulated, accrued computing storage and so on. But, having said that, the university can also preorder capacity. They can say: "we know that we need so and so many CPO hours or whatever over the next year and we will preorder them and pay in advance", at which point we will discount the price. It's the same price, but it's a bit cheaper if they pay upfront than just use from their quota. So the advantage that we have here is that we have some kind of a better forecast of income. It's easier for them to budget and that makes it cheaper. That's the goodie we give them, we make it cheaper, and if they say "no, we don't want to pay upfront" it's fine, you can pay as you go, but no rebates in that case. They just pay the full price.

LP: But do you have any idea how much it will cost afterwards? The service?

JCF: That totally depends. If you have one server that means, a little web server, that will cost you maybe 250 francs for a year, if you do genome sequencing on 300 computers that will cost you, I don't know, 6000 francs in a month. It depends. It's totally flexible. It's very hard to predict.

AN: The last question. Except the university, do you have other customers?

JCF: Right now we're in pilot and we, just anybody that asks for an account will get one. Mainly universities but we have a couple of private start-ups and so on that are using our service. Some of them are spin-off from the universities that are starting up now, some others are start-ups that we know, people we know. It's a mix with probably 95% universities, lecturers, researchers, students, and 5% others. But none of them are customers yet. If you ask me in

an email I'll give you a voucher and you're a customer tomorrow. And it's swiss companies. Or swiss universities and swiss companies. Swiss organizations.

LP :Are you good with economic aspects?

AN:For me it's enough.

4. Legal aspects

LP: OK. So I continue with the legal ones. So you just said that the company is swiss?

JCF:Yes. We're regulated under swiss law. Swiss jurisdiction.

LP:If you know, how do they compare to other legal systems in other countries? Concerning the cloud?

JCF: I'm not a lawyer. I cannot answer that. I know that swiss data protection laws are better than certain other countries' data protection laws. I wouldn't venture into trying to answer that. Sorry about that.

LP: Are your policies, operations and all services around privacy and the protection of personal information different across countries and jurisdictions? But the thing is, you're only in Switzerland, is this correct?

JCF: Yes.

LP: Okay, concerning Swiss law on cloud computing, which procedures have been easier, and which more complex, in order for the company to operate, again, in comparison to other countries? Maybe from your personal knowledge, how is it handled differently in Switzerland, and how in other countries?

JCF: Sorry, I don't know. No. I can't tell you.

LP: What is required for national, cantonal and european legal compliance… again you don't know, it's okay.

JCF: I can give you contact with our lawyer if you're really interested in…

LP: It's just to understand what's the difference about this aspect. The thing is, since you still don't have this ISO 27001 or other norms, we just want to understand how it really works for you, about the legal aspects. How they are controlled...

JCF: We have company-wide legal documents that govern how our services are used, how the customers interact with them, our rights, their rights, and so on. And we also have that for the cloud, that is being created right now by our legal department. But I'm not… In the end, I get a document and I hand it over to the customers and, you know: “sign here, this us part of our agreement” I'm not into the details, I'm sorry.

LP: Okay, no problem... Okay, maybe five. Are clients made aware of all data that you collect on their usage?

JCF: Yeah. We have… what's the word… privacy policies, and those are public and we specify what data's being used, for what used, how long it is stored and so on and so on, yes.

LP: What guarantees of anonymity and security are in place surrounding these practices, and can the client opt out of data collection?

JCF: The guarantees on anonymity and security are that we will not use that data for anything else than the operationality of the service, whatever service we're talking about; that the people who are working on these services have signed, in their work contract, have signed agreements on how they have to treat customer data. And the breach of that contract will lead to human resources consequences. So basically it's a firing offense to misuse the data. We level out. If nothing bad happens of course. And no, the customer can not opt out of that data collection, because the system will just collect data, usage data and that cannot be opted out of.

5. Security aspects

LP: Okay we might overstep again on this. We go now to the security aspects. Okay, Aurèle? What measures or policies do you have for data security in your company?

JCF: We don't have any formal policies. Again, we're not yet ISO 27001 compliant. We have what I would call the industry best practices. We take security very… we value that a lot and we work on that. The normal measures of protecting the systems, having firewalls, having limited access to the data by those people that actually need it for operations, etc, all those are in place. But there is no formal guidelines and so on.

LP: Is data security an important point for your clients?

JCF: Absolutely, yeah. Based on the surveys that, as I said, earlier we are in talk with the "Datschutzbeauftragte" from the universities and work with them on defining what kind of security levels we assign to our services, when they use it. That is an ongoing discussion.

LP: So there are many levels of security?

JCF: Different universities handle that differently. Some universities say "the service offered by SWITCH, this is as good as if we would offer it ourselves, so our staff can put sensitive documents on SWITCH services", while other universities will say "no, it's outside of the campus, we're not allowed to use it for sensitive data." It's really university to university that decides that on their own. We offer the same level of service to everybody. There is no differentiation between… We do things differently between this university or that university.

LP: Did you have so far a university or another client that was scared and was hesitant about the security you offer?

JCF: No. Not in that regard, no. We have a pretty good track record of being a reliable partner so, no. Not that I'm aware of.

LP: Do some of your clients have special demands concerning data security?

JCF: No. It hasn't come to me yet. I'm sure there is a possibility of certain, I don't know, if we talk about medical research data or so on, that there will be special requirements, but so far, that hasn't surfaced yet.

LP: What kind of protection against malicious insiders and the misuse of client data by its employees and subcontractor does your company take? Example, if you do background checks, certifications, legal contracts…

JCF: Basically we have legal contracts, it's part of the employment contract, but we don't do any of the other. As far as I know there is no background checks for people being hired. Certifications is something I personally don't believe in, and session or click monitoring is not something we do.

LP: In the case of a security breach due to a malicious insider, is the client informed of the incident, the cause and the nature of the breach? And how public is this information made?

JCF: We haven't had that case. I can't really comment on what would happen when that happens. And that is something that would be decided on CEO level, I guess. I'm not even sure how we would react to that.

LP: So you don't know, you don't know what would happen in such a case… You don't know if there would be a compensation.

JCF: We just haven't have that case happen, luckily.

LP: All right. Do you use a back-up system?

JCF: This is a difficult question, because the amount of data that we're handling makes it very difficult to back it up For example we have two storage clusters, in Zürich and Lausanne, and they have like half a petabyte of storage each. It's impractical to backup half a petabyte of data, you just can't., basically, with normal measures. We cannot back up that amount of data. The second thing is, we don't know, when we talk about the infrastructure services, we don't know what the customers would consider valuable data. For example a research project that stores a couple of hundred of virtual machines that they do some computation, if one of them disappears or dies, then, there is nothing that needs to be backed up because the data is somewhere else and can be recreated or reinjected into this process. If you're talking about a service like SWITCHdrive, we have customer data, yes, we back that up, of course. If we know about what is being used as data, if it's our own service and it's user data we will back it up, but if we just provide the infrastructure we push that responsibility to the clients. We can offer help in doing backups but we will not just back-up everything that comes our way.

LP: How do you deal with data loss? Do you have some sort of insurance policy?

JCF: We. Lose. No. Data. (laughs) No, actually we have lost data in SWITCHdrive. We had a pretty serious upgrade that went very bad and we lost some data. We don't have insurance for that. We sent out chocolates to the users. And we were able to retrieve most of it. Some small amount of data was lost due to really bad timing, bad luck and so on. The data hadn't been backed up yet and disappeared during the day. We deal with it with a lot of stress.

LP: Of course. Since it's other people's property.

JCF: Yes, it's bad.

LP: We said before, different levels of security…

JCF: Well, yeah… We have a basic level, just one level of security but of course you can implement additional levels. If you run on our infrastructure you can for example encrypt your files system or take additional precautions. That's something that, again, is up to the individual customer, what he does with the infrastructure. We provide just one level of security.

LP: All right. Do you provide your clients with information about who is having access to their data in they request to know about it?

JCF: Yes. Absolutely.

LP: You give them details, names?

JCF: Yes. For example, again with the example of SWITCHdrive, we store, where you can sink data into our cloud. Of course our admins can look at the data that the client has stored, and we have had clients that ask, “by the way, who can see that data”?

LP: If your company has some subcontractors, do you require that your subcontractor have the same level of security and privacy policies as your own company?

JCF: If we have that, we have the contracts we sign with them includes that, so they would agree to our levels of security, yes.

LP: Who is in charge for your customers' data?

JCF: It depends. Our customers, basically. Our customers. In the case of the infrastructure we… In case of something like SWITCHdrive, the team that runs the operations, if you will, is in charge of the data and keeps them secure.

LP: Do your clients know where their records are hosted? In which data center?

JCF: Yes. They know that. Actually they can choose the data center themselves.

LP: And do they rather, again, this is…

JCF: They'd rather have them in Switzerland.

LP: Do you make random tests to make sure that the data assigned to you from your customers are still present in your system and in a good shape?

JCF: Basically the storage system we have does that automatically. It continuously checks for data corruption and will repair data that has become unreliable. The system takes care of that. And what could go wrong with that? (48:30)

6. Technology aspects

LP: We continue to technology?

AN: To technology aspects?

LP: If you want. If you're ready.

AN: Can we combine the cloud computing application with other tools used for record management?

JCF: Not sure I understand the question.

AN: The question is about if you propose other tools to the records management or the information management?

JCF: No, again, we're providing infrastructure at this level and there is nothing else.

AN: So I think the next question is useless because infrastructure. How have the existing privacy legislation and requirements been factored into the controls and architecture of the system at your company?

JCF: They haven't really been factored in a thoughtful process. We are kind of aware of what we have to do, but there hasn't been any formal, like: okay, because of this regulation we have to do this and this… It has happened, if you will. More of a general understanding than a decided full process.

AN: About multi-tenancy: do you offer your clients alternative to a multi-tenancy model, like multi-instance architecture?

JCF: Well... Currently, we only offer multi-tenancy, so we have one system that holds multiple tenants. We are looking at offering maybe multiple clouds, having one cloud for a specific

customer if he so demands. But so far this is not something that is anywhere near being rolled out into production. We only have multi-tenancy.

AN: Do you offer insurance or other forms of protection for business losses resulting from a lack of access of records due to server seizure, or other outages arising from a multi-tenant model?

JCF: No. We don't have that. We try not to. We have in our service level descriptions, we will limit the things that customers can do that would lead to seizure of data, so we don't allow the usual file sharing and so on and so on, things that have led to seizure of the hardware. But no, we don't offer anything specific.

AN:Do you provide clients with any information on who they share tenancy with?

JCF: No. Everybody is on the same system and they cannot see who else is there. We don't offer any information.

AN: One of the critics of multi-tenancy is that it can facilitate data mining by service providers, as client data is often held within a single database and/or application.

JCF: There are two answers to that. To the infrastructure part it does not apply, because there is no database. The only database is: this user has three virtual machines and the other user had twenty-five virtual machines. For SWITCHdrive, where we actually keep user data, there is no data mining being made. Potentially we can look at what kind of files are stored by the users. Our administrators have the capability to do that, but we're not allowed to do it. So we will not look at what kind of data we don't know what movies have been stored by students, etc. We just don't know. We don't look at those kind of things. Because the work contract we have prohibit that kind of access. We'll look at these things if the customer comes to us and says “can you help me find some piece of data or whatever, then we look at what he actually has stored, but other than that we have no idea, and no interest in knowing what has been stored.

In general, just as a side note, we try to limit the amount of information that we store and log and so on. Our legal department is very interested in us logging as little as possible and throwing away locked files as fast as possible. Just in order not to be able to produce logs when we requested. We don't want that information, if at all possible. We don't want to know what our customers are doing. We don't want to store that. Going back to the question about what kind of information is being stored: as little as possible. We don't track that at all.

AN: I think we can skip the next question, it's like legal aspects. So, the vendor lock-in. Why did you choose the open source solution?

JCF: Absolutely. We don't like vendor lock-in at all, so we use open source solutions. With the infrastructure it's very simple for a client to take his virtual machines and move them to another cloud provider. And that is the right thing to do. We don't want any lock-in. Although it would be interesting in terms of business perspective of course, but that's not what we think is the right way to do.

AN: How can you assure the integrity and the authenticity of data?

JCF: Again, two answers to that. For the infrastructure service, we will make sure that the basic storage has no integrity losses. Actually the software does that itself. Whatever the client puts in, it's up to them. For the SWITCHdrive product, it's a matter of… the software has mechanisms that authenticate the users and only allows a user to upload files into his directory and so on. We don't take any special precautions, but the product that we're using has mechanisms that help with that.

AN: Do you use a cryption or encryption method?

JCF: Cryption about strictly confidential data… We don't use any encryption per say. Our systems could use encryption. The basic storage level could be encrypted, so the data on the disk drives is unreadable if a drive should be stolen or whatever. We're not using that because of performance reasons. It costs too much performance. And for the products like SWITCHdrive, the user encryption doesn't really help. It provides no additional level of security. Because the keys are still on the server and the administrator could still use that additional access to get access to the data. So it's kind of… the only barrier is to those people who already have access anyway. It doesn't make sense. That being said, we would be interested in having a, for the drive, for the product, to have a system that provides end to end encryption, so that the customer can encrypt the data himself and we don't see that. This opens another can of worms in terms of support because if the user forgets his password, the data is unrecoverably lost. Unless you have kind of a master key, at which point we're back into why do we encrypt in the first place, if you have somebody who has a master key.

If a customer wants to use the infrastructure to encrypt data, they can of course do that. It's something that they can use by themselves, using encrypted files systems or encryption. That is encouraged, yes. But it's not something we can enforce or control.

7. Conclusion

AN: We can move to the conclusion. Lucie?

LP: Yes. First of all, because I think I didn't ask you earlier: how many different customers or universities are you working with?

JCF: Basically we're working with… We're at least talking with all of the universities, so it's about forty in Switzerland, and out of them, about ten of them, ten-fifteen of them are customers or have pilot… no, more, actually. Maybe half of them have been testing the system. And our interest is to get them all, of course.

LP: And the rest? The start-ups?

JCF: Oh, that's maybe five or six companies. It's very very small. It's not something we actively go out and pursue.

LP: Do you see an evolution in the kind of customers who request cloud services today?

JCF: Evolution in what direction?

LP: That they start to have different demands, they expect other things… they're evolving.

JCF: Yes. The first level is like "oh, let me have some virtual infrastructure, let me have a server". And then we see more evolved setups, we need some kind of special networking setup, we have special storage requirements and so on. Yes, there is a tendency to go more involved and more complex setups. There is a range of customers.

LP: So their demands changed over time?

JCF Yes, as we see more customers we see more specialized use cases

LP: This from your own experience now. Are there any best practices adopted by SWITCH company on hosting a cloud computing service in Switzerland, that you believe has been an important asset?

JCF: For our own product, you mean?

LP: Yes

JCF: Yeah, of course. Everything we learn feeds back into the product, into how the product is being operated, how it's being used. I'm not sure if you're familiar with the term "kaizen" from japanese production culture? Kaizen means continuous improvement. We're trying to continuously improve the product, and I think we're succeeding quite well so far. But there is not a single thing I could point and say "this is like a critical indicator or performance factor". It's the sum of everything that makes the product better and better and improves it. Our team is very diverse, has a lot of experience in a lot of different areas, so I think that helps in building a better product all the time. But I couldn't point to a single item and say "exactly, this is the critical secret ingredient that makes all of this possible.

LP: Aurèle, do you have any other question?

AN: No, I think it was a very interesting interview. Thank you very much.

JCF: You're welcome. I'm glad you found that.

LP: And you, would you have something else you think we didn't treat? That you would like to add?

JCF: Maybe just a comment on the interview itself. A lot of these questions are about cloud services that have customers records, and less of an infrastructure approach. That's why maybe some of the answers didn't quite match. But cloud is a very broad topic. I'm not sure who else you're interviewing and it might be totally the right questions to ask.

LP: The thing is, we made this questionnaire, we want to use the same for every kind of cloud provider. Some can answer more questions, some can less, but it doesn't matter for us because we still gather information and this is all that matters. We don't want to make different kind of questions.

JCF: Okay, fine. No, I do not… Issues that you didn't cover is maybe the whole concept of self-service. I think that's the important differentiator between cloud and other kind of IT services, is that you push a lot of responsibility to the customers of the service and have them use the system in a way that wouldn't have been possible before. If I'm talking infrastructure it's nothing fundamentally different than a virtualisation infrastructure that is in place in any kind of company. The difference is that the end user actually can provision infrastructure by himself and doesn't need to go to an IT department or somebody that keeps, is the gatekeeper for that. And I think that's a really important aspect of cloud computing, this self-service aspect. That's something I feel very strong about, that is important, if you talk about cloud, is that you push a lot of responsibility and a lot of power, also, to the customer. it goes both way, it's power and responsibility.

LP: But if you think about it, you answered almost everything, the only thing you didn't know about the legal aspects. But it's okay. So it was great. Thank you very much for your time. And do you think, if there is another question, can we contact you?

JCF: Please, call me again. Send me an email, or…

LP: Wonderful. Thank you very much.

Legal aspect

Answered by email from Ms Esther Zysset, legal department at Switch.

• Is SWITCH company subject to Swiss laws?

Yes.

• How do they compare to other legal systems in other countries?

I would say Switzerland has a decent data protection law which is however not the strictest and most effective. It is more stringent than that of the US but less so than for instance German data protection law.

• Are your policies, operations, and/or services around privacy and the protection of personal information different across countries and jurisdictions?

We are not active internationally, so this does not apply to us.

• Concerning Swiss law on cloud computing, which procedures have been easier and which more complex in order for the company to operate in comparison with other countries?

See above.

• What is required for national, cantonal and european legal compliance?

SWITCH is subject to the federal (national) data protection law which can be found here:https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html

The most important principles are listed in articles 4, 5, 6 and 7.

Currently, for European compliance each European country has to be looked at individually, as the current Directive is not self-executing. This is likely to change with the planned Regulation which will apply directly in all member states.

Cantonal compliance also varies from one canton to another, but they generally require each subject organisation (public institutions of cantonal law) to dispose of a legal basis for the processing of personal data. SWITCH is not itself subject to cantonal law but cantonal law may apply when SWITCH is outsourcing provider.

• What procedures have you put in place to insure that those legislations are respected?

As mentioned, we are not active internationally, so generally we do not have to take European law into account. As a general rule, we work with specific contractual provisions with our customers and suppliers. We also have an information security and a data protection officer within the firm, in order to answer questions and monitor compliance.

Filename: 3. Swisscom Eyup Koç

Date of interview: 13th November 2015

Place: Swisscom office, Genferstrasse 14, 3011 Bern

Duration: 1:24:41

Interviewers: Aurèle Nicolet, Lucie Petrelis

---

1. Introduction

LPP: This is the consent form. You agree that you are recorded

AN: And the questions.

LPP: So you can follow through.

AN: And sorry for my accent, my english accent.

LPP: We're gonna share the questions. All right, then we'll begin. Could you please tell me your name and your position in the company?

EK: Okay. My name is Eyup Koç and I am head of cloud enablement and consulting.

LPP: How long have you been in this position and if you could just say a few words on it.

EK: Since three years. Three years ago and what's the job… I'm talking with enterprise customers about cloud, what cloud is, what it is not, what does it mean. And not only about technological stuff, also about how to accelerate the development to be more agile and that means also you have to change processes, organisation, you need new skills. Things like that.

LPP: And how long have you been in Swisscom?

EK: Now, five years.

LPP: Five years, okay. So you were in another position and then you switched…

EK: Yes, I have been project manager for the first two cloud platforms. And then I switched to consulting, talk with customers then internal, organisational departments.

LPP: Yes. So now you are promoting one, the cloud.

EK: Yes. Yes, that's my job, promoting to… so, it's a mix between consulting, pre-sale activities, workshops, ehm, product development… it's quite a mix so I also have to talk with this internal part of Swisscom and to explain them what customers need. And also to the project team, to, perhaps to change priorities, or to replan roadmaps according to customer needs.

LPP: So, what kind of cloud computing services does Swisscom offer?

EK: Well, we have different… So, from IaaS, Platform as a service, PaaS, and… just these two. So, dynamic datacenter, dynamic server, we call them, so the product family is dynamic computing.

LPP: Can you tell us a little bit more about what you do for IaaS or…

EK: Okay. Okay, we have a… the existing product is a classical IaaS. A platform that means customers as a portal, self-service portal deploys his workflows, workloads in a, in a public

cloud, in the Swisscom public cloud, it's all in the Swisscom datacenters, all the stuff, and it's quite classic. So they are responsible for the workload, they are responsible for patching, monitoring of the VMs, of the virtual machines, it's really classic. But they can have also some options like managed operating system, managed OS or database services. So it's quite classic. All dynamic storage, cloud storage, something like… Amazon, Amazon storage… so. This is the IaaS. Then we have the existing PaaS service is managed OS only for customers, only for Swisscom customers, that means they already have some systems in Swisscom datacenters. It's not the PaaS in the mean of this definition, it's really managed, manages VM, managed OS, managed middleware… It's more outsourcing stuff with some self-service capabilities. Not really elastic PaaS. But since one month we have application cloud in place. It's now, it's public, available, now, and this is a classic PaaS. So, something like … from Amazon Heroku. You know Heroku? It's really, it's… it's a platform for developers.

AN: Okay.

EK: Software developpers, classic, for microservices based applications. This is available since one month.

LPP: Right.

EK: And then we are working on a new enterprise cloud, we call them enterprise cloud with self-development, technical orchestration, with, ehm, with more management capabilities than classical cloud platforms has in place. So if you look at the most clouds, public clouds, it is something for IT, IT people, they have not a lot of management capabilities. And what they really not have, and this is one of the problems, if you are in an enterprise environment you have dedicated systems in your data centers, you have perhaps a virtualized platform in your datacenters, and now you also want to use a cloud. How to monitor, manage these different environments platform is... it's difficult for enterprise customers. So the new enterprise cloud platform Swisscom, we will develop such functionalities, so that we also have something like a congregation management database for example, so every deployed workload is in a CMDB, we have interfaces to other monitoring instruments or IT service management tools, and brokerage capabilities, so the customer can also choose which cloud provider they want to have. If I have a classic Microsoft Windows workload, I can choose to deploy it to Swisscom cloud, to Amazon, whatever.

LPP: Is Swisscom a cloud computing provider, or does it collaborate with other cloud computing providers?

EK: Oof. In future, both. Because we are a cloud provider, but we will collaborate with others like Amazon, and this will be, in future this will be something like ecosystem. A cloud ecosystem. So I think this is one of the most important things to collaborate with others. Because we Swisscom will never be Amazon, we will never be Microsoft, we will never be Google. But we have some other advantages so we have to collaborate with them.

LPP: All right. And when did Swisscom begin offering cloud services?

EK: Oh, the first one we started five years ago. More or less five years, yes.

LPP: And how has it evolved over these five years?

EK: Well… I have to explain that we have… we had several cloud platforms, so we had a platform for SAP, subsystems, we had platforms for AIS, we had a platform for PaaS, and the problem is that you have no synergy effects. Because you have, for each service you have a platform, it doesn't make sense, so the huge change is that we are now developing one platform for different services. So that we are more scalable. This is the first point. The second point is from a customer point of view… not a lot of customers trusted enough to go to cloud. They sometimes didn't understand how to handle cloud. We also had to learn about what is a

cloud provider. For example: maintenance windows. Usually Swisscom has their maintenance window from Sunday to… in the night from Sunday to Monday, from midnight to three o'clock in the morning, and then once we had the phone call from a customer and they have been in Brazilia, so… we learned that there is no maintenance window. It's not possible in a cloud environment. We also learned that we… that… that the operations team, they have direct contact with customers. Because if they have problems, we have to talk together, where is the problem. Because normally we can say: "IaaS, that means if our platform is running, then the rest is your problem." Because they're responsible for that. But. In reality it doesn't work. We have to talk together. And that means we have operation teams who talk directly with customers, and you also learned in school as students in an ideal world, never have a customer talking with the engineering team, they are talking with the service desk, but it doesn't work in the cloud environment. So had to do some learning. And also the customers! Also customers they had to learn how to… when they create a VM in the cloud, they never changed the resources, compute resources, the storage, CPU, RAM… they always worked like some years before. They didn't use the capabilities to change resources. If I need more RAM than I give, I put more RAM to the VM. They always acted like normal in dedicated systems. They always built… the size, the size of a VM was always built after maximal resources needs. If you need in December more resources than you buy the computer for… even if you don't need the resource from January until November. But you have to buy it for… the server normally for the maximal size of what you need. And they also acted like that in the cloud. Doesn't make sense. Because it's easy to change. But normal systems in classic IT in client server based architectures, you have to stop the VM, the virtual machine, when you change the size. Of RAM, or CPU or something like that. And that's a problem. But that's… It's not about the cloud platform , it's about the application. The application is able to handle that. But it's ninety-nine percent of all business applications are working like that. They are not elastic. At the moment.

LPP: Tu veux continuer?

2. Managerial aspects

AN: Yes. The managerial aspects. Are your Service Level Agreements set in stone, or will Swisscom negotiate or renegotiate each requirement with its clients when determining contractual obligations?

EK: Laughs. It's not possible to negotiate different SLAs. Not possible.

AN: Okay.

EK: We have one SLA. And this is one of the problems because… customers want to have the same SLAs as in dedicated systems. In classic IT systems. And in cloud… does it really make sense? I'm not really sure. But it's not possible to negotiate them.

AN: Okay.

LPP: So what… how does it work?

EK: We… We have an SLA, we have an SLA, for example, for the AIS platform, we have an SLA for the platform, we can't give an SLA for the application, because we are not responsible for it. If a customer needs a managed OS then we give a SLA for that, but it's for every customer the same.

AN: Yes. Okay. It's the SLA for each type of service?

EK: Yeah. Each service, yes.

AN: But not for each client.

EK: Yes.

AN: Okay.

EK: But one of the problems is when… so let's say, Swisscom has an SLA for the platform. 99.5% of availability, for example. Then they have a partner, a smaller company, who is in reality a reseller of our cloud services, and built his own services as a value at. And if he sells his service for 99.9%, it's his problem, because it's not possible if the platform is at 99.5. But we realized such things...ehm… such mistake has been made. So for a customer, for an end customer it's always difficult if they don't know of which platform service is running, what is real, what is the real availability.

AN: How do you contribute to support client's information governance practices?

EK: Same as normal outsourcing. Governance is real important stuff.

LPP: Can you tell us a bit more? About Swisscom specifically, what do they...

AN: How do you do to help the clients' information governance?

EK: Well… Normally, in an enterprise environment they have… so… for example… a customer has the right for audits. We give them the rights for having an audit, we can give them logfiles, log information about their data. We can give that. We can handle that. We have certification ISAE 3402. This has been the form of SAS 70 report. We are certified according to ISO 27001 and ISO 20000. So. It's more or less the same stuff as in classic outsourcing.

AN: How long does it take to implement the service of the cloud within a company?

EK: So, now. If you are really in a big company… So let's talk about, example: Swiss television. Swiss television starts the journey to the cloud and they are now learning how to handle with the cloud and they plan to migrate all their systems into cloud. With the systems in Geneva and Ticino and things like that, within the next four years. And… another customer, we are talking about migration within three years because… you have to think about how to migrate, eh? And when do you migrate. Is it depending from life cycle of the application? Is it depending from, you have other pains, like you have a data center which is not sufficient enough, or do you have platform lifecycles, or… ehm… you have to wait until the supplier of the application is ready for cloud. So for example we have customers who have some systems with a physical dongle. The application developer says: "it needs a physical dongle. To run." A dongle is the stuff… yeah, for young people it's hard to explain. It's the stuff you put it into the computer, the software's not running with that piece. It's more something… like a key. Like a key for the application. It's a dongle. And how to put a physical dongle into cloud? Okay? So you have to wait. Or, you bought a business software. A business application. And if the business application is running on Spark, and not on X 86 architecture, not possible to migrate into the cloud. So. You have technical lifecycle, economical, different aspects. You have to handle. And for a smaller company it's… normally, for a small company, small, medium enterprises they have homogenous platforms… It's much easier to migrate into the cloud. In an enterprise, big enterprises, they have very heterogenous environments, they have different storage types, they have different hardware types, different software. There it's difficult.

AN: So… usually, a slow roll-out ?

EK: Not the big-band, it's slow. Slow roll-out, yes. Slow.

AN: Okay.

EK: All at once is nearly not possible.

AN: I see.

EK: If you have ten systems okay, no problem, but three hundred different applications: not possible.

AN: It's a jigsaw.

EK: Yeah.

AN: After the implementation, are you in charge for the adoption and the training of the staff?

EK: It depends from the customer. It depends. Because… Not after the deployment, it's before the deployment of their systems. It depends. We have customers with internal IT organisation which really knows how to handle with the cloud, who have experience with Amazon, they need no education. Sometimes they need… If you… You have also to think about, do you really need a portal, or do you use directly APIs? If you are not used how to handle with APIs, you have to learn it. So. Professional services, we explain them how it works.

AN: Okay. And if the company needs to help, you give this?

EK: Yes. Professional service, yes.

AN: Is there a possibility to have a trial experience of your service, before making the official contract?

EK: For… You have to see that for enterprise customers you normally make a proof of concept of the platform. So they have their request for information, request for proposal. And they you are… you have to make a proof of concept with them. That's normal in the contracting phase. So for Swiss television for example. And for small and medium enterprises, we give them the possibility to… how we handle it, there are two different models. The common model is that we say to them, for the first two months we give you… ehm… within 1000 francs per month are for free. If you use resources for one 1000 francs it's for free. If you need more in the month then you have to pay. But for a testing phase that's enough. And what we will do, beginning from next summer, for more bigger customers we say: we have proof of concept environment, we have standardized processes, you can try it for a fixed price and if go to our cloud then we give this price for free, if not you have to pay the price. Two, three, four, five thousands, it's not a big amount.

LPP: But it's for both kinds… For IaaS and for PaaS?

EK: Yes. Platform as a Service is much easier to test it, because it's not expensive. You don't need a lot of storage, you have… At the moment it's our… We give… In the first three months we give you reduction of the price of 1000 francs. So if you have a price under 1000 francs, it's for free. And this is absolutely enough for an applicational cloud.

AN: Okay.

EK: So they can try it three months for free.

AN: How does the data hosting works? In which location, city, canton, region, and why did you select these locations?

EK: That's clear. We selected because we have different datacenters, so Swisscom have different data centers, we have Tier 4 and Tier 3 data centers. Tier 4 is the max level of security and things like that. We have two in Bern. And we have colocation spaces in Geneva, in Zürich, in Olten, in Lugano. It's clear, Swisscom cloud is always in Swisscom data centers.

AN: The criteria, like financial, or law…

LPP: Why did you select these locations?

EK: These locations? Because we have them in place. We didn't build them for the cloud. We had them before. That's one. And you have to see that lots of our customers, they have not only cloud, they also have classical outsourcing stuff, so we need our data centers. And we have them in place.

AN: It's easier, yes. When a customer cancels or a subscription is terminated, how does it go off?

EK: Yes. Yeah, so, our responsibility is, if a customer cancels the contract, then we have to delete all his data after thirty days.

AN: After thirty days.

EK: Thirty days, yes. Thirty days so that customers have time to move their data, and we delete all data. So. And now it's depending on the storage type they have. How to delete data. If you have block store in a georythmic storage you can't delete the data, you can only revoke the key. But it's not possible without key, it's not possible to read the data.

AN: Do you provide any help for the transfer of data?

EK: Yes, of course. Professional services. And of course Swisscom is the company with the best network in Switzerland, and for transferring data you need network. So, we have these services in place. That's our business.

AN: Does Swisscom maintain a client data exit and recovery plan, should your business unexpectedly fold? I think it's a bit… hard. It's a catastrophic scenario.

EK: Yes, yes, yes. This is normally in SLA… So. In classic IT, you have for such... ehm... business continuity management, you have the storage stretched over two datacenters. Active are stretched. We also have cloud platform down, but… is it really necessary to have such functionality in a cloud? To be 99.99% available? Amazon is not. They are telling they are. Microsoft, they are also telling they are. But they are not. Because they only pay you a monthly fees back if there's a catastrophe or something, something's not running. But in contract with our customers we have penalties. So we have to be sure that it really works. But it's more or less met in a classic member. So. Stretched clusters of hardware over two datacenters… Yes.

AN: Okay.

EK: So, if Swiss television is not running, it's not good for us.

AN: How does the cloud computing service work along with the retention schedule of your clients' documents?

EK: The retention schedule? You have to see, it depends which service they have. If a customer has Infrastructure as a service, they are responsible for this, of course.

AN: Of course

EK: If it's PaaS, they are responsible for that, if it's software as a service we are responsible for it then. It depends of what kind of service is it. But… We have… We have all Swiss law regulation. We have to…. Well, we have an internal legal department, and they are looking that we are doing everything according to these laws. You have to see, we have banks. We have Swiss banks as customers, so… It's first normal stuff. But that's the difference between to… Amazon, for example. They are only a cloud provider. Use the service they have, or don't use it, but you have no chance to have more individual services. That's the difference.

AN: Has Swisscom ever conducted a transfer to client's records to an archival institution?

EK: … to an archival institution, what does it mean?

AN: Ehm, it's like… what's the world in english…

EK: Like a government institution, like police, or something…

AN: No, like archive of Switzerland, archive of Bern… the name of the institution, like each canton has an archive institution.

EK: Ah! Well, clients' records are always… Client is responsible for his records. So they are responsible. If they transfer the data to archiving it's their problem, not ours.

AN: And a client has never asked for the transfer?

EK: I don't know.

LPP: They just take their data. They never said take them from there and put them here.

EK: Normally they are doing that. If you have… In a… archival… Banks for example. It's archive to archive, the data is hard stuff. You always have to migrate the data from one hard disk or hard drive or to another technology, to tapes or something like that, or in another technology. So. If they want that, we do that and it's a project. We do it for the customer, so then we do that of course. Because we have a lot of banks in place, they outsource all their IT. But if they have their own people, then they do it. That is nothing to do with cloud. It's normal archival service.

3. Economic aspects

LPP: Okay. We'll pass now to economic aspects. Which are the economical advantages for your clients in choosing cloud computing solutions from Swisscom?

EK: Okay. Easy to say explain… You have a global market. You have competition. And the prices are more or less transparent. So it's not possible to be more expensive than Amazon, Google and things like that, if you don't have any special services. So if you have a classic IaaS service, it's not possible to get more money than Amazon. So it's more target pricing. Everybody's looking for the prices and if one of the global players decrees the price, everybody sticks to this price. And with IaaS, nobody's earning money. Nobody.

LPP: But why should we go on Swisscom? Financially, I mean?

EK: Financially?

LPP: Yes. That's my question. Why? Because it's… the economical advantages. Okay, you follow the market, and then you make best deals?

EK: … If you have Amazon, Swisscom, with more or less same price, more or less same services, then what is important for you? Where is the data stored? You have sometimes compliance issues. So compliance issues, or regulatory issues as one of the drivers. But it's not… it's not only a price, because the price is transparent. The difference is, you can talk with Eyup Koç of Swisscom. Try to get an interview with the boss of Amazon… Or a customer with whom he has to talk… We have our account managers, we have our people here you can talk with them… Try to discuss this with Microsoft. It's not possible. And important decisions for the product development… they are made here in Switzerland. And not in US or Germany or in other countries. We are more local than the other ones. And if you compare Swisscom with smaller cloud providers, which are also in Switzerland, then it's the fact that Swisscom is more stable and that we have a better… Everybody knows Swisscom is earning money. The chance for bankruptcy is not really high.

LPP: I think you replied also to… it's okay to talk about the return on investment?

EK: From a customer perspective or from a provider perspective?

AN: What do you think? Customers?

LPP: Yes, customers.

EK: I can't calculate the return on investment for a customer perspective. It's not possible for me and from all point of view, as a provider… Actually, prices are made by CPU, RAM, storage. And this is more or less old fashioned model. So I'm quite sure that within the next years we will have new pricing models in place and it will be more end service prices. You don't pay, perhaps, for the CPU, RAM, storage of a virtual machine, you will pay for monitoring service, you will pay for that you have all information CMDB, you will pay for that you have a dashboard, you will pay for report, you will not pay computer resources. But… No cloud provider is really sure in which direction he goes but every company is sure the actual pricing model is not the right one. But we will see what's coming next. Within the next one, two years, that's the future.

LPP: Yes. About the pricing mechanisms…

EK: Yes, it goes with more or less the model. And now we have pay-as-you-go. We started with monthly prices and now we are going to hourly prices. If a virtual machine is running for one hour, you pay one hour. In the model before, if you started you pay one month, and now it's one hour. And I'm quite sure within the next two years you will pay per minute.¨

LPP: Okay. Now about your clients: how many do you have at the moment? On cloud computing?

EK: On IaaS it's more than 300, about 300 customers. And on the PaaS, we started one month ago, more than 60 independent software vendor, so more than 60 customers.

LPP: And mainly, are they in the public sector, public companies, NGOs, international organisations…?

EK: Private companies. Most of them.

LPP: Small, medium…

EK: We have small and medium, but also big enterprises, it's…

LPP: Variety.

EK: Yeah. But the most of them are private companies.

LPP: And they're mainly swiss, or international?

EK: Mainly… Mainly swiss but we also have some… Mainly swiss, yes. About 90% Swiss companies, or Swiss-based companies. And 10% are…

LPP: International, but within Switzerland?

EK: We have international in Switzerland, we have international from outside of Switzerland. Brazilian companies for example. Brazilian companies are very interested to have their financial systems in swiss cloud and not in a brazilian cloud. Or italian companies, they have their financial systems in Switzerland. Holding. In a holding structure. The holding is more or less in Switzerland, the companies are in Italy but the holding is in Switzerland and the financial stuff is in Switzerland.

LPP: So you said you have banks, and something else, other fields.

EK: Yes. Swisscom, we have all. Everything. Small and medium companies, banks, insurance…

LPP: Which kind of sectors? Banking, and insurance, and…?

EK: All. All. Everything. All.

LPP: Right. So we said in which countries are the companies' infrastructure, you said about Brazil…

EK: Yes, but… Infrastructure, IT infrastructure?

LPP: Ah, sorry, sorry. Yes. In which country is the infrastructure.

EK: IT infrastructure? Okay. Actually, our infrastructure is only in Switzerland. IT. But for swiss-based multinational companies we are also going outside of Switzerland. So we decided with one customer that we will build an infrastructure, a platform in Singapore, because Singapore is very regulated, highly regulated. If you do business there you have to be sure that the data is there in Singapore. And one in New Jersey, US. But it's only for swiss-based multinational companies. Other companies, we will always have a service in our datacenters. Not in Germany, Austria, US, UK or whatever.

4. Legal aspects

LPP: All right. Now we go to legal aspects. If your company's international, are you subject to Swiss laws?

AN: I think Swisscom is not international.

LPP: No, I mean… sure, but… Okay. If you are subject, can you tell us about Swiss laws?

EK: (laughs) Yeah, you have to have all Swiss law regulations in place. For example, for the banks, we also have the financial market regulations from Switzerland, we have in place, it's clear. Swiss law is the most important law for us. We are a Swiss company in Switzerland…

LPP: And how do they compare to other legal systems in other countries? If you know. The Swiss law, how does it compare with other legal systems, on cloud computing?

EK: On cloud computing? It's more or less the same. In the European Union it's more or less the same stuff, also with data protection. They are not really different. They are not. And if you look to the american law, everybody heard about privacy, privacy is something different in the US. But within Europe it's more or less the same.

LPP: Okay. So you just said it's the same. Are your policies operation services around privacy and the protection of personal information different across countries and jurisdictions?

EK: Well, Swiss people always think that swiss data privacy is the hardest, or the strictest in Europe. It's not correct. German are more. My wife is working in the swiss… she's responsible for the data privacy at the government. So. Switzerland has not the hardest law. It's not.

LPP: Concerning swiss law and cloud computing, which procedures have been easier, and which more complex, in order for the company to operate in comparison to other countries?

EK: I don't know the english name… Prüfungs… the law for all providers, all providers need to give access to swiss police for monitoring telephone, internet, things like that. And we have to

do it too. We have to do that. And we have to archive data for six months. But according to swiss laws. And this is expensive. Lots of data.

LPP: What is required for national, cantonal and european legal compliance? On cloud computing.

EK: It's depending on the business. So normal compliance, legal compliance, it's more or less… between different industries you have different regulations. So if you are swiss retail banking, for a swiss retail bank, the data must be in Switzerland. But if you are UBS, or Credit Suisse and you have your mergers and acquisition company or your investment banking they are in UK, or you are in US, it's important to have the US regulations, or the UK regulations, in place. As a cloud provider, at the end, it's more or less the service, an outsourcing, a sourcing service. It's not really different from that. And we have to be careful that we have all regulations of Switzerland in place. If another company, from Brazil, they are in our cloud and they have financial systems, for example, in the cloud, and it's forbidden by brazilian law, it's not our problem. It's the problem of the customer. Okay? You have always to look, which perspective is the important one?

LPP: Which procedures have you put in place to insure that those legislations are respected?

EK: We have our legal department, our audit department, we have internal and external audit… Classic stuff.

LPP: Are clients made aware of all data that your collect on their usage? What guarantees of anonymity and security are in place regarding these practices? And can the client opt out of the data collection?

EK: We have to log all data according to client services. Client systems. For example, if we are responsible for the operating system, we manage it and we log who is entering on this VM, who makes changes, things like that. We have audits trails. If everything is managed by the customer, then we only, okay… they have different VMs, but we don't see into the VM. Cause we don't have the right, the permission, to get into the VM. We don't have the root admin rights for that. But normally you have to log all access, identity access changes. You have to log security instances, you have to log patching, you have to log monitoring, you have to log a lot of different stuff. This is logged, and all data which are for customers we give them, if they want to have the logs they can have it. But we don't give log-in information where we are responsible. We don't give them to the customer. If it's helpful for the customer for their infrastructure, that's okay. We give them. Of course.

5. Security aspects

LPP: Now we go to the security aspects. What measures or policies do you have for data security in your company?

EK: Lots. We are certified according to ISO 27001, and we have the ISAE 3402 regulations. We have… the regulations of no firma don't have a security regulations specific for cloud or IT they don't have. We also can say…. Oh! For the banks, PCI DSS, yes, of course. For transfer. Transfer of money. Transaction. All policies which are needed. Well, we have banks, so… But we have no special cloud certifications, at the moment. No. Because they are not really helpful. At the moment they are not good. Eurostar, for example. Doesn't make sense.

LPP: Is data security an important point for your clients?

EK: Yes. Yes. One of the most importants.

LPP: And how do you manage your clients' fears or hesitations about data security?

EK: For every big customer, they are taking their security department is talking with our security department about what we are doing. For every big company. It's normal.

LPP: Do some of your clients have special demands concerning data security?

EK: Yes. Sometimes they have that but then we have to talk together what is really helpful, what makes sense, what not. Because one of the problems is, we are in the cloud, and cloud means service. And if you have a classic outsourcing, if this is your server, and it's outsourced to the provider, then you are the owner. You, you are the customer, you are the owner of this hardware. So you have a lot of rights to see that, to do some stuff. But if you have a cloud service, you are not the owner of the service, we are the owner, you use it. That means that we have a shift into… of the level of… what makes sense, which information we give, what doesn't make sense. If you are in a public cloud, a hypervisor, we never, never give the customer rights of the hypervisor. Not possible. If it's a private cloud, we can discuss about that. We can discuss because it's only for them. If they do any mistakes, it's their problem. But in a public, not possible. And normally we don't give, also in a private cloud not the possibility to have admin rights on a hypervisor level. Doesn't make sense. Because we are responsible for the… for the service. At the service… Also, IaaS means hypervisor is included from the provider.

LPP: What kind of protection against malicious insiders and the misuse of client data by your employees and subcontractors does your company take?

EK: Background checks… ehm… What's the english name… In German it's the Strafregister Aufstrug, en français je ne sais pas. It's the records of legal… of justice, records of justice… something like that. The normal stuff. Normally, each employee has to give some records. Not compliance records, it's… juristic… Ah, I don't know what the name is. We check some records, and we also have a part of Swiss police in the data center in Switzerland, and all employees they have to check, to give the records all three months.

LPP: Okay. In the case of a security breach due to a malicious insider, is the client informed of the incident?

EK: Yes.

LPP: So it has happened already?

EK: Yes, of course. Yes. If I say no, then I am lying. That's quite normal. You have to say then what has really gone wrong and what you are doing against that. And normally they also, the customer is… bigger customers, they normally make tests, security tests themselves. With hacking tools, things like that.

AN: And how public is this information made? In the newspapers, or...

EK: It depends. If it's only a small security breach or it's only for one customer, then we inform the customer. It it's something bigger… and we didn't have that, for different customers. It has not been… you don't tell that in a newspaper, eh? The banks are also not doing that. Because if you read it in the newspaper, then another company or another guy will try to do the same stuff. So we don't tell that, but we tell it to the customer, of course. They have the right to get this information.

LPP: Yes. And what steps would your company take in such a case? Has there ever been criminal proceedings brought against an employee or subcontractor?

EK: Yes. Yes, you have read it in the newspapers, more than two years ago, with archival data. An employee of Swisscom didn't destroy tapes. And these tapes' informations have been sent to Neue Züricher Zeitung. So you can google it. Two years ago, yes.

LPP: What rights and/or compensations are awarded to a client in a case where you are at fault for data exposure, if any?

EK: Yes, that's in the contract. Always. With big customers you always have penalties defined before that.

LPP: What kind of penalties are there?

EK: Money.

LPP: I guess it's important amounts?

EK: Yeah. It hurts. *(laughs*) If not, it doesn't make sense.

LPP: Do you use a backup system, do you make a replication of the records, or a printed version?

EK: Yes, of course, but… If we have a… It's a service, yeah? If I have Infrastructure as a Service, computing resources, then I have the option that we have backups. Automatic backups. If not, it is the customers, who is to install backup capabilities, backup services, in their datacenter, in their own custom environment. Yes, of course. But this is always one of the services every customer has. But if they don't use our service, they have to build their service on their own. It's always customer decision.

LPP: But the backup system, it's something included in the package, or it's extra?

EK: It's extra. It's always an option, yes.

LPP: How do you deal with data loss? Do you have some sort of insurance policy?

EK: Yeah. The legal department and so… We have processes in place because we need that for banks. And banking systems are in a banking zone. And in the banking zone we have services in place where we can see if we have a problem with data loss, with… who has access to the data, is it usual, is it normal, is it a normal case, or if there are any curious actions.

LPP: Are there different levels of security?

EK: Yeah. For each company. In the cloud… In the cloud, not possible, if they have IaaS because you don't know what they are doing, we have no information. Then we can't do that. The banking's a community cloud. Only for banks. It's something different. All customers there are banks.

LPP: Do you provide your clients with information about who's having access to their data, if they request to know about it?

EK: Yes. Yes, that's normal, yes. We have to say that. Yes. For banks it's normal. You have to name the persons. In a classic public cloud, not. In a private cloud, when we have managed services, yes. If they need information we give it. So, no problem.

LPP: If your company has some subcontractors, do you require that…

EK: Yes.

LPP: The same.

EK: It's the same.

LPP: Who is in charge for your customer's data?

EK: Customer's… The customers.

LPP: Do your clients know where their records are hosted?

EK: Yes.

LPP: Or do you know if they'd rather have them in Switzerland?

EK: Only in Switzerland. Swisscom data are always in Switzerland.

LPP: Do you make random tests to assure that the data assigned to you from your customers are still present in your system, and in a good shape?

EK: It's getting… It depends, now, from the service. In a classic IaaS service, we don't know. We only see the amount of data which are stored. What we can control is if the backups are okay, or not okay. Our backups. If we do it on ourselves. If the customer is responsible for the backup, we don't have the chance to have a process. Or to make some random tests. But for all services we are responsible, we have to test it. So. One example. If we make backups from the storage pool, then we say to the customer : "we do it once a day". That's not correct, we do it three times a day. And we store one. One of these three. We do it three times a day, not one time. We do it more often than necessary.

6. Technology aspects

AN: Okay. The technology aspects. Can we combine the cloud computing applications with other tools used for the records management?

EK: Yes, this is one of our… ehm… USPs, because we are not only a cloud provider, we are also an outsourcing company. So… It's clear that our cloud systems will… must be able to interact with dedicated systems. With dedicated data.

AN: How much control do your clients have over the data? In IaaS I think all?

EK: All. They are responsible for that. Can they visualize the state of the records? It's depending of that that they have in place. I can't say, it's depending of their systems. It's not in our hands. And the second point: "can they make modifications on the metadata of the records on their own?" … Metadata you normally have in your communication systems, document systems, archiving systems. And the metadata, they are important, and in IaaS, they will do that with their own documentation system, or they can have it. If it's a service, it doesn't make sense without metadata. It doesn't work. It doesn't make sense. The records belong to the customer. So, the metadata too.

AN: How have the existing privacy legislations and requirements been factored into the controls and architecture of the system at your company?

EK: In different ways. But from beginning of the project, security and privacy responsible persons have been in place, they work also in the project.

Multitenancy?

AN: Yes, multitenancy. Do you offer your clients alternative to a multitenancy model? Like multi instance architecture or something else?

EK: One of the services we have, the dynamic source is a multi instance model. Because you always have, you have instance of a server. You don't have a tenant. But for company, if I don't have only a server, normally we have a multitenancy model. In a shared environment, in

a shared cloud, you need the multitenancy model. But the multitenancy is based… is more or less a security boundary. It's not multitenancy in data records, it's a security boundary for the systems.

AN: Do you offer insurance, or other forms of protection, for business losses resulting from lack of access to records due to server seizure or other outages arising from a multi-tenant model?

EK: No. Normally not, only in the banking zone it's clear that we have to say okay, they are different banks in different tenants. But normal is not. We always say, it's a shared environment, but it doesn't matter which customers are in this shared environment, because the security must be as strong that it doesn't matters.

AN: Okay. So. One of the critiques of multi-tenancy is that it can facilitate data mining by service providers, as client data is often held within a single database and/or application. For clients worried about privacy, how would you respond to these concerns?

EK: Hm. No, you have to… Okay. When I look at that, then you talk about what a database with multi tenant, that means mandatory multi mandants, multiple companies in one database. Completely different from multi tenant cloud structure. Or they mean that… No. It's really difficult to understand what is really meant by this question. Yes, of course, if I have a multi tenant, or shared cloud environment, I have a cloud management zone. This cloud management zone is the zone only for the cloud provider. In this example for Swisscom. And then of course we hate datas… we have information about each customer. Who will pay our bill, for example. Or which roles they have, and which is the contact person and things like that. Of course we need that. But. This has nothing to do with multi mandatory databases. Multitenancy is more in the customer environment. Then we know which customer belongs to which tenant. But we need to know that, if not we can't manage it. But… databases or applications… privacy, that's nothing to do with privacy. I don't understand this question. Because multitenancy in a cloud environment means something different as that in a database, it's… in a multi tenancy it's a security boundary. It's not a network boundary. Of course always, also with network but not with classic… security boundary even by network is more.

AN: Yes, I think it's… we're not technology experts, and I think we didn't understand the multitenancy.

Okay. The question five I think, yes. It's always national swiss law… What do you think about vendor lock-in? Do you try to propose or suggest an open source solution?

EK: We have different hypervisors. We have open source hypervisors and we have proprietary hypervisors. OpenStack, different... But in a cloud, we believe that proprietary systems, or proprietary APIs are not the right way in the cloud. So we expose and we describe all APIs. It's public. You have, how to say… Of course, if you have a system running on VMware… And now, you have also a multi providers strategy, eh? Sometimes, provider A has a cloud based on VMware, while provider B is based on OpenStack, for example. They are different. You have, of course, some technical lock-in possibilities. You have, but it's more technical stuff. For us, it's important that… We don't see a chance to have a lock-in situation for the customer. Doesn't make sense. And if one cloud provider starts with them, he will lose all customers. Doesn't make sense. Cloud is, from my perspective, against lock-in. If you have a classic outsourcing, it's much more difficult to change the provider. If you are in a cloud it's easier to change the cloud provider.

AN: How can you assure the integrity and the authenticity of data?

EK: We can't. It's not our problem.

AN: Yes, it's the customer's problem.

EK: Yeah.

AN: Yes. I think question seven is the same, the customer's…

EK: All data is encrypted.

AN: Okay.

7. Conclusion

LPP: Now we go to the last part, the conclusion. Do you see an evolution in the kind of customers who request cloud services today?

EK: Yes. The first customers are learning that it's more than virtualization. It's more than virtualization, it's much more. They are thinking about how to change the application, that they can use the computer resources in an elastic way, and how to be more agile. And you are only more agile and more cost effective if you change the application architecture. So a lot of the customers are… Not a lot. The first customers are aware of that. And of course all younger ISV, independent software vendors, they know it, so. But they don't have the history from heterogenous IT, so it's much easier for them. That's one point. The second point is that they start thinking, if I go to cloud, which new rote skills I need, as a customer, and how to change the organisation, their own organisation. Because it's hard. If they have… you have an IT infrastructure department, eh? You have your own IT. And you are the head of IT infrastructure. And the CIO says, now we go to the cloud. That means that your staff is new in the cloud and that you are not more responsible for the infrastructure. How to handle that? They know that… Most of the CIOs, or managers of an IT, they have accepted that cloud is the right way. That's the biggest change within the last five years. Because five years ago, it doesn't make sense, cloud. Nowadays it's really changing. It's gone to the cloud, it's more or less a question of time. When you go to the cloud. But it's not a question cloud or not. That's the point, yeah.

LPP: So, have their demands changed over time?

EK: Yes. It's increasing.

LPP: Are there any best practices gained from your experience and adopted by your company on hosting a cloud computing service in Switzerland that you believe has been an important asset?

EK: Yes, in the application cloud, this is the new cloud platform. We are the first company in Europe with a Cloud Foundry based PaaS model. Yes. We are the first one and we are the first company which is… ehm… yes, in a public environment, we are the first one in Europe. And we are also member… it's open source, we are member in the community, we are working with the community. So quite a lot of things. You have to see that we have… some people which are working together, or within a community. And the most innovative tools are open source. They have much more power than IBM, HP, Dells and whatever. They are more innovative, and if you want to use that you also have to work together with the community. That's something that we have to learn. Before, we had a supplier, we had a contract. But now, how to have a contract with a community? Not possible. It's more or less a problem for the… a main change for the managers and for legal departments.

LPP: So. Do you have anything to add, or is there any issue you believe we didn't treat?

EK: I'm quite sure that with the cloud operation model, IT is changing. And so continue the integration, continue deployments. These are very interesting models, and this will change a lot in operating and IT. But we think it's the right way. And we are still at the beginning of the

cloud world. Not at the end. We will see a lot of different business models, and everybody knows Airbnb, Netflix, things like that, but there are much more different business models incoming. It will be very interesting. Problem, for a lot of companies, is that they still think to… how to say… they are not agile. They are not really customer oriented. If they don't change their mind they will have problems, because a lot of smaller companies are coming with new business models, with lot of drive. And that's interesting, that you can start your own business with no money. That's the point. That's interesting.

LPP: And are you willing to answer…

EK: Yeah, no problem. No problem.

LPP: Thank you very much.

AN: Thank you very much.

Filename: 4. DFi Thierry Blanc ENG

Date of interview: 16th October 2015

Place: DFi office, 18, chemin des Aulx , 1228 Plan-les-Ouates Genève

Duration: 47:42

Interviewers: Marion Destraz, Arina Grazhenskaya

---

1. Introduction

AG: Could we discuss the language question?

MD: Do you prefer french or english?

TB: If we could do this in french… If that's okay with you.

MD: It's perfectly fine.

TB: You would have preferred french. (Laugh). I can see that.

AR: No it's fine. It's just that it's additional work to do the english translation, but we can do that. Thank you very much.

MD: Could you begin by reminding us of your name and your position in this company?

TB: My name is Thierry Blanc and I am director of governance at DFi Services, I arrived here about two years ago. If I go back on my past, I spent twenty years in a big watchmaking international company at different IT positions. I did system, development and finally network. And after twenty years, DFi offered me to join them, among other things for an ISO 27001 certification. I don't know if you've heard of it, it's a certification in information security, which was updated in 2013. We will talk about it later. DFi is a hosting service, historically, that had telecommunication lines. Little by little they started doing cloud hosting then we added the security layer, so that today we have a coherent whole.

MD: Can you tell us, in large strokes, what kind of cloud services you offer?

TB: DFi, historical telecom operator, we offered internet lines a long time ago, and little by little it evolved. Physical hosting for clients who ask for it, people who still have machines to put into rooms, we still do it. There are demands, probably less and less, and there is cloud hosting. Today, we offer Infrastructure as a Service. I don't know if you know the different parts. There is Platform as a Service, where we simply offer the minimum. We deliver infrastructure, and above us there is Software as a Service. So, we offer more or less services to the clients depending on their competences, the time they have to spend on it, the budget, etc. We adapt but globally, what we try to offer is infrastructure. The client drops his applications and from there, he manages his services or not. Business applications it's not for us to manage, the clients knows them well, it's his job to take care of it. If he drops an ERP (entreprise ressource planning), his HR management… He knows how it works and operates them. Mainly, that's how we work.

2. Managerial aspects

MD: We will talk about the managerial aspect of what you offer. Are your SLA set in stone, or can the client negotiate?

TB: When you offer cloud services, there are SLA, which are, I'll resume very fast but we propose a document which says: it's 99.999, it means eight hours of interrupted services a year. It means we make it so there are never more than eight hours of interruptions or there are penalties for our clients. We set in place redundant architectures and we know we can hold this promise. There are contracts we make our clients sign, we are asked to do this, SLA are requested by clients.

MD: Do you contribute to information governance of your clients, the way they manage their data?

TB: Governance for our clients, we can't say we do, no. We can manage our information today. With the clients, depending on the level of maturity, they don't know those terms, either because they don't think in that direction, it's governance, I'll say, everyone is free to manage their data. If they ask us for help we can offer it, but it's very rare.

MD: When a new client ask for your services, how much time does it take, more or less, to start implementing a cloud system in their company?

TB: DFi has more than 3000 clients today. It means small ones, 5-10 persons, companies, SMEs, the core business of DFi, that's between 20 and 200 persons, and some very big clients. So it's hard to answer the question, because for small clients it can go very fast, for the big ones there is a whole study phase. They have chosen several partners and they look at several criteria, among them security, more and more, and once they have all those informations they look at how we work, where our data centers are… Usually we answer, for the biggest ones, to RFQ (request for quotation), and from there we explain our way of doing things and they chose afterwards. But the processes, for big businesses, can take up to three to six months. For the small ones, there is less information, less things to take care of, we close the deal more quickly.

MD: And how does it happen? Do you do the big bang or a slow rollout?

TB: It's for the client to decide. The client chose to host all of part of its service and we answer their needs. We're pretty flexible but for clients who want to deploy a complex architecture, they say we don't… Generally, the big ones, it's not that they can't afford it, it's that they don't want to spend time and money to manage basic things. We will host the infrastructure but we will also do their service maintenance.

MD: Are you in charge of the entire deployment mechanism?

TB: In general, yes, it's what the client asks for. Most of the time we do soft transitions. We migrate. First, there are what we call "proof of concept", which means we build a test infrastructure so we can tell them: that's what it would look like, do we all agree? And little by little, we build a complete infrastructure and we migrate part of the services until the transition happens naturally, so that it's not too brutal.

MD: One the implementation is done, are you in charge of training the staff so that they can use the services?

TB: I would say there are the two cases I was talking about previously. Either they are services we call "managed", in which case we take charge of everything. The client manages his applications but we guarantee that the platform are working, that the discs aren't full, that there are no security trouble, that we do the updates… Then we do our job as host and maintenance, and the client only does the operational part and can concentrate on his job. It's what we hear more and more. "IT is not our core business, so take care of the servers, of all that, do what you must, we agree on a service and then we concentrate on our real job." Which can be insurance, which can be banking, which can be industry, which can be a whole lot of different trades.

MD: So you do everything.

TB: Mostly it's like that, it's what makes it interesting. Because to drop some IT someplace, what is the point, if it was in their data center, in the machine room or at our place… There isn't one. Then there is the whole maintenance part which comes on top of this.

MD: Talking about hosting, your servers are all in Switzerland, I think?

TB: Yes.

MD: And you have several sites?

TB: Today we have four data centers. Data is not hosted in our offices but in those four data centers. We have two for telecommunication, so already there's some redundancy at that level. We have links coming from two different data centers. And two data centers for all clients data. We have a network that's totally redundant, that has been entirely remade in 2013 so that it guarantees redundancy and security to the client. We can't afford to lose data. Even if there are problems in one data center, normally, the client can't even see it.

MD: And geographically, where are they?

TB: In Switzerland. Exclusively in Switzerland.

MD: Is there a reason they are exclusively in Switzerland, or is it just more practical?

TB: The reason is not the cost, because I think it would be much cheaper to do it somewhere else. No, the reason is so we can control the data. Today we can guarantee that the data remains in Switzerland. That, too, is something that is requested more and more. OK, we put the data in the cloud, but where are they? That's the real question. We can tell them: "we can guarantee that they are here." They remain on the territory. In particular for questions of data protection, law, regulations. The clients who are constrained to that are mostly the banks, the insurance companies and people who are sensitive to where their data is stocked. But we see that it's something that comes up more and more.

MD: If a client decides to cancel a subscription, how does it go? Do you have ways to give them their data back? Is there a process? How much time does it takes?

TB: It's all in our general conditions. The client remains the owner. So if a client wishes to leave, we give him his data back, it's his. There is no reason for us to keep them. Then we agree on the destruction of tapes… Clients are generally very faithful, some have been here for twenty years. But sometimes a few clients make other strategic choices and decide to quit DFi. From then on we ask them what to do of the tapes. When can we destroy them? OK, you got your data back but you may realize you need one month, two months, so we make an agreement with the client, but contractually, in our general conditions, the client know - and that, too, is a question the clients ask us. We call it reversibility. It means: we decided to leave, what's the process? It's detailed in our general conditions and it reassures the clients.

MD: If DFi had a problem and you were forced to close down, do you have a way to give clients their data back. Is there a process?

TB: If DFi were to close for financial reasons? Or for other reasons?

MD: For example.

TB: We have the same constraints. We tell the clients, and we've been certified on these things too, so we will give the data back. The data doesn't belong to us. That, the client has to understand it. Sometimes demands happen like that. It seems logical to me, just logical. But it's contractualized, we agree with the clients, reversibility in written in the SLA and in the general conditions and we say who owns the data. It's relatively clear.

MD: Is your architecture maintained in proprietary code?

TB: What do you mean by architecture?

MD: The cloud architecture, the whole system.

TB: No. We are based on commercial offers. However, there is a whole lot of tools that we use based on what we call open source. In general, the world of telecom and the world of hosting work with open source a lot, there are solutions that are sold to our clients that are proprietary, but cloud solutions, no. It's based on a commercial solution.

MD: Do you have a way, in your system, in the services you offer, to work with the retention schedule of your clients' data? If they have data that needs to be destroyed after a while, do you have ways to guarantee it has been done?

TB: Yes. We have processes. In our ISO 27001 certification it's asked of us. We work with third party businesses whose job it is to destroy hard drives. If we need to go up to physical destruction they come, they crush, they give us a certificate that the disks, or the tapes, have been physically destroyed.

MD: Could customers audit those measures?

TB: We have certificates, we have tapes, we even have disks numbers… Either they come with us to witness the destruction of the disks, which rarely happens, but sometimes they ask us for the certificates that confirms their data has been destroyed.

MD: Did you ever have to transfer a client's data to an archival institution?

TB: Not to my knowledge. Which means not for the past two years. I haven't heard of it, either. Generally the data is stocked here and we adapt disks sizes according to the client's demands.

MD: You don't usually do transfers?

TB: No.

3. Economic aspects

MD: Let's talk about economic aspects. Are there economical advantages for your clients in choosing a cloud computing solution instead of something else?

TB: In terms of costs, I think it's interesting, here too depending on the size of the clients, on the number of servers, on the number of persons who work on it… But I would say, if the clients has decided to outsource his solution, he doesn't have material costs anymore, nor licence costs, all this is part of a global service. Everyone is a particular case, if the people want to take care of it, want to manage… But all the work that is done, finally, it frees up some time for them, frees up some budget… Knowing that we propose 24/7 services, so night surveillance of their infrastructure of needed. We have teams that keep watch days and nights, holidays included, their on their infrastructures. There are alarms, we take care of things, or we warn the client if there are different needs.

MD: Can we talk about ROI?

TB: We don't calculate that; I think clients calculate it. But we aren't asked that, it shows through the offer, they will look at the direct cost, but I believe what they calculate, too, is the indirect cost. I don't need to pay people during nights, I don't need to pay people to go work on the machines physically. That's what we do. All these things, the client takes them into account. We don't make those additions for them. We're not asked to, at any rate.

MD: Do you use economic arguments to convince your clients?

TB: Economics, so, we hear talking more and more about "green IT", and this, it can be an argument for the clients. It's true that to mutualize instead of having machine rooms spread over all of Switzerland, if we only had a few data centers, it would cause less pollution. Economically speaking, it's for the client to see, we talk about certain aspects now it's for him to decide if it's interesting for him. But globally, I believe the clients gains from it.

MD: You said you have more than 3000 clients, we talked about them a little already. Can you talk about them a little more? Are they more public or private sector, international organisations, are they more Swiss?

TB: We can talk about activity sectors. I told you insurance companies, banks, industry, what do I forget… people who work in the travel business, people whose business is based on the internet, people whose job is security. Mostly Swiss clients, a few international clients who want their data kept in Switzerland. They want some guarantees regarding this. So American companies, from everywhere, who say: "We want our data to be here."

MD: Is there an evolution on this side? Are there more and more of them or has it always been the case?

TB: I think there's an interest in Swiss law on data protection. There are some guarantees given in Switzerland that don't exist abroad. Today, we see this change, I wouldn't say it's a total upheaval but we still see… people are more conscious of the value of their data. For political reasons, too, Switzerland is relatively stable, data protection law is quite restrictive, so people have an interest in putting their data in Switzerland. So if we can guarantee them they will stay here… all the better!

4. Legal aspects

MD: Do you know how Swiss law compares to international laws in regard to data protection? Do you know what happens in the rest of the world?

TB: Typically, there has been a voting. The Americans rejected Safe Harbor, I don't know if you know what that is. So that American businesses could put their data in Europe, they wanted that the data could go back out. There has been some conflicts of interest between Swiss law and American law and there was a votation on the 6th of this month [October 2015] and Americans have put this procedure into question. I don't know if it will change things drastically but they are trying to say, if you have American clients, the data must be provided to the United States. It's a political debate. Until today, what is in Switzerland remains in Switzerland. I don't know if it will change in the future. Something might happen in the months to come.

MD: You have American clients who have their data here?

TB: We have American clients, yes, who want their data to remain on Swiss territory. Today we can guarantee that to them, tomorrow, I'm not sure.

MD: To be in accordance with the law about data protection, are there any particular processes that have been created?

TB: I told you earlier, we've been certified in information security by ISO 27001. We completed this certification by another called OCPD, which is the Swiss norm for data protection, and which respects this information security law. And we've been certified Good Privacy, too, it's the international equivalent of this OCPD norm. So it means we have one certification in information security and one certification in data protection. When we've been audited two years ago, there were jurists, a jurist who came, technical people, and they audited every

process: how we manage our clients' data, where is it stocked, how are they kept, do they leave the company, the territory, all these things have been analyzed. Then they put their OK stamp, certified OCPD. This certification is renewed, we underwent it a short time ago. Every year, all these things are looked at again, with the evolution of the company. No nonconformity, they call it major nonconformity, minor nonconformity, we haven't had any on these two certifications.

MD: No major and no minor.

TB: That's it. It means we respect the law on data protection as we promised we would, and information security in the same way.

MD: Do you collect data on your clients?

TB: No. Clients' data belong to the clients and we don't treat them. We treat the part… We don't touch confidential data, we only treat those linked to facturation, which we need, but no, no statistics, no stocks, no selling it back to anyone. We're very thorough on this point and this certification imposes it upon us, too. It was the will if the company so it wasn't a big effort, it's more a question of ethics than anything else.

5. Security aspects

MD: We can talk about the security aspect in more details. What measures do you have that guarantee data protection, concretely?

TB: Are we talking about technical measures? The ISO 27001 norm talks about human resources, physical security, location, data centers, talks about the whole technological part around the data to protect them. An example: we correlate all data in terms of security and we look, rather than treating them independently, we put into place mechanisms to centralize the information and to correlate, on a security point of view. When there is an alarm, because I mean, to watch over 3000 clients, routers spread over four data centers, I men digital attacks come by different ways, it's not humanly possible to check. We can't have someone reading a router's log, a firewall's log, an active directory's log and who says: "Ah, I saw something that correlate there", no, it's not possible. So we put in place those mechanisms and from there, when attacks are detected, these malicious IPs, we ban them from all our infrastructure. So that's just an example, but we have a lot of mechanisms that allow us to protect those datas with different technological means. ISO 27001, it's 133 control points that we've all gone through one after the other, I told you, on theses various aspects. On every control point, auditors validated that what we've told has been put into place and that our data are well secured.

MD: Security is an important point for your clients, I take it?

TB: It's very important to us and I think it's very important to the clients. Not everyone is conscious of this today. I think that, as long as people haven't been through a security incident, it's hard to conceive but the day it happens, security becomes a priority.

MD: Are they not all aware that it's important? Are they worried about security?

TB: No. I think that some companies put production first, if you will. It means that for them, the operational part is very important, but that their data is kept on the other side of the world, they aren't aware of it. People who use Dropbox, today, don't realize their data aren't there, they're abroad, that's the first thing, that the software is absolutely not secure, that anyone can access their data. People who use Gmail as their professional emails… That's a whole series of reflexes that people don't necessarily have today and we, we make them aware of this. Know that if you have confidential data, it might not be the best place to put them. That's some

reflexions to have with the clients but I think that, today, we're far from having educated everyone.

MD: Are some of them worried anyway? Do you have ways to reassure them?

TB: Banks are very rigorous about this, because they're watched by FINMA, because they, too, are subject to many norms, which can be ISAE 34.02, and so on. Insurance companies, too. So they are very, very rigorous and very fussy. I told you we hosted people whose job is security. They came to us for those very reasons. Then we have clients who are less security conscious who come here, we talk to them about security services, but they don't quite understand what it means.

MD: Do some of them have special demands concerning security, in addition to what you provide usually?

TB: Special demands no, but some ask us a very large number of details. I'm thinking about those people whose job is security. Their website is a shop window and they absolutely can't afford for those sites to go down, or that other content is published on them. Those people have asked us very, very precisely how we do things, and when they saw how we managed data they said: "OK, we can lean on you as a service provider." Granularity depends on the interest of the client. But we can go very, very far in the details, that's for sure.

MD: Do you have processes in place in case someone, in your company, had malicious intentions and made bade use of the data? Can you be sure of your employees?

TB: We can't be sure. However, we can take certain precautions. We made our employees sign what we call a, "Acceptable usage regulation" [RUA, "règlement d'usage acceptable"] in which we state "those are your rights, your obligations". If there is a negligence in security, that's a professional misconduct, it's a grave misconduct. That's written in this document. If you use confidential client data, if you don't use adequate ways to transfer them, it's a professional misconduct. People have been sensitized. We do sensitizations, even for us, whose trade is IT, in matters of security. Every new hire is sensitized and we explain to them, and for us too, employees review the process at least twice a year. We look at security incident that happened in the world, we explain to them. And we, we can't be judge and jury, we get audited as well by an external company and we say, I don't want to say trap our users but to see how they react. This year we had a process, last year we had a different one, next year we'll use something else again. We agree with this external society which works in security, we say "try to send us something and we will see how our employees react". That we get caught or not, that's not the question. It's how they reacted, in what time, did we take the right measures? We overlook this and we don't tell anyone.

MD: If there was a problem because of an employee, would you tell the client?

TB: It never happened. We're a small structure, 44 persons so we know our employees, there are no other locations… Malicious intents, it can always happen but it would take a really good reason, someone would have to be very, very motivated to do this. The other reason I would give is that it's a small world and someone who had been branded like that, it would be very hard to find a new job afterwards. I don't think so. I think in companies which are much bigger, where employees are distributed across the world, it might be more complex. We have this advantage to be at human size, it's easier to deal with the situation.

MD: If there was a problem, would there be a compensation for the clients?

TB: We have insurances. Insurances called RC Pro, who would compensate the client. You'd have to look at the global conditions, there is a maximum level which is indicated, but the client can turn against us, and in this case, the insurances would compensate him.

MD: You said all data was redundant?

TB: Yes. We do saves. Of course, we save the data of our clients depending on their needs. Up to them to give us the periodicity. We want to keep them 30 days, 60 days, the offer will change accordingly because we will need different disk sizes. The more information retention they do, the more the service will cost. But that's on demand. We're able to stock data for 6 months, 10 years if there are legal constraints for them. Up to them to tell us, after that, we don't want them on disks, we want them on tapes, we will transfer them.

MD: Are there different security level to access the data?

TB: Yes. There are clients - I told you about some certifications, we have another, PCI, which is the norm for credit card payments. I mean we have a client whose business is travel, which makes sales over the internet, so there are credit card numbers transiting. This client must answer to the PCI norm. So we have auditors coming to us, as we are one of their subcontractors, who say: "show us how you manage data." We've been audited by them too. We aren't certified, however we take note of the needs of the clients and we make it work. This very precise environment, not everyone internally has access to it. We agreed with the client, only a few defined persons can access this environment. Despite all the various client environments there can also be partitioning. There are different security levels according to different needs.

MD: Do the client know who has access to their data?

TB: If the clients ask for it, we precise it to them. I take the case of this one client who says: "I want to know the names of the people taking care of my data, and no one else, I want you to guarantee this to me, to send me the logs of who accesses it…" Demands can be very precise. We are able to answer them. And the partition the client's data in a very specific environment with specific access rights. We do this.

MD: Do you work with subcontractors?

TB: The subcontractors we use, actually, are the telecom providers, the data centers… Except for that we do everything here. We're obliged to have the Swisscom, others I won't name… and the data center providers, who host the data in the physical sense, guarantee that there is security, that there are guards, that they are redundant in matters of energy, that they are redundant in matters of electricity. We're obliged to lean on these providers. All the rest, we provide it ourselves.

I wanted to say, too, it was a strategic choice not to substitute ourselves to them. We could have built our own data center, we didn't do it. It's not our job to manage climatisation, to manage all these things. So we told ourselves, rather than do this in a cellar or somewhere, let's make use of people whose reputation is international and serious, and we will rent spaces that belong to us in these structures. It's like we had a dedicated machine room.

MD: So it's all secured and the subcontractors don't have access…

TB: We ask the data centers for accountability. Tell us, I want, every month, a log of all people who entered the data center. We gave an authorized list. We did the same for us. Some people have permanent access. For others, we give access on demand. We need to pick up a tape or something in a data center, it's someone who hasn't a permanent right, I give them temporary access, that's validated by the data center. There are processes in place. We will let that person access at a certain time because I signed a document, because the data center called me back to tell me: "who did you gave this authorization to, what's their date of birth?" There are some very precise processes with them.

MD: Do you do tests to make sure the data are still where they are supposed to be?

TB: Tests to know if the data is whole, yes. Everyday, with backup tests, we have what we call restore tests. What we do is, we put a file, whose content we know, and we see if we can take

it back. We assure consistency this way and the confidentiality of data is respected. Now, where the data is, we know it. It's in our four data center. They aren't with Amazon, they aren't with Google… We know where they are localized.

6. Technology aspects

MD: Let's talk about the technological aspects. Do the cloud applications you offer interact with other records management tools?

TB: Yes. Typically, the monitoring tools we use. We guarantee functional platforms, that we don't reach the disk limits, the CPU's, the RAM's… All these things we keep an eye on. The client's services we keep an eye on. We have our own monitoring tools, we monitor our network of course, to be sure it's still in good shape, we monitor our DNS, our servers, we monitor the whole infrastructure. It ads up to the services we offer but we are obliged to be sure everything is functional.

MD: To what point do clients control their own data? For example, can they see what they have put on your system at any time, from an device?

TB: Either the client imposed restrictions, I'm thinking of those in the security business, who say: "we want our data accessed from our office only, so that our employees can't access them from home." So the constraints chance, too. But I would say the client has access to the data and can at any time check that he has access to everything. He can copy, he can extract… We guarantee the functionality, the security. He's free to check if he'd like.

MD: Can they modify the metadata?

TB: It's their data.

MD: So they do whatever they want?

TB: They do whatever they want.

MD: Do you have a multi-tenancy model?

TB: Not in the cloud part but it's a model we used to offer. We call this "mutualized data". There are dedicated locations for the clients. A client who says: "Me, I don't want to share my server with someone else", and clients who say "me, in terms of cost, it doesn't interest me, so if I'm on a mutualized server, I don't have any confidential data, that's perfectly fine with me." You can chose as we offer both options.

MD: We already talked about insurance… And if they do share their server with someone else, do you tell them with whom?

TB: No, we won't tell them with whom.

MD: But you know it?

TB: We know and we communicate about it. We will tell them: "you're on a shared server". Those are points we bring up with the client at the very start. Because it impacts the cost, it impacts the security, so it's normal that the client be informed. Even if he doesn't come with this demand, saying: "I want to be in a dedicated environment", we ask him. He's free to chose.

MD: Do you know if there are laws, be they european, national or cantonal, that concern multi-tenancy?

TB: Not to my knowledge. No generic laws. But if clients have constraints on data protection, it will influence the environment they will chose. I think that they would know. Generally, we

know that banks and insurance companies have a number of obligations. Companies in the industry, not necessarily. We have some very secure environments; if people come in those environments and don't have any obligations, we will still offer them all the guarantees that go with it. We explain this to them. They take it into account or not but they know they are in a partitioned environment and that they are rather well protected.

MD: Are some of them worried about the possibilities of data mining coming from you? You have access to all your clients' data, you could take advantage of that… Are they worried about this?

TB: We haven't had any fears expressed about this. Are they reassured by the certifications? Are they… I don't know. We guarantee we won't sell their data, that we won't use them except for facturation needs, all that's linked to the client himself. But no, we won't mine data. And we won't sell them, either.

MD: They know this and they trust you?

TB: They know this. But they haven't expressed any fear about that. The fear is more about data security but I don't think they're already at the stage where they think, "hey, they would mine…" They don't talk about it, at any rate.

MD: Could you tell us about lock-in? You have open source solutions…

TB: Solutions… ?

MD: If your clients decide to see another provider, they wouldn't have any problem transferring the data?

TB: No, because we told them we'd give them their data back. It's contractual.

MD: And they manage their data the way they see fit.

TB: Exactly.

MD: Do you have any way to guarantee the integrity and the authenticity of the data? Can you prove it hasn't been modified?

TB: Information security covers three themes: confidentiality, integrity and availability. Those are the three themes we cover with the ISO 27001 norm, globally. On all kinds of different aspects but it's true that data integrity is vital, that they aren't modified and that no one can alter them because that's much worse than losing them. We will discover afterwards that they have been modified. Our job is to secure those data and not only do we say it, but we can prove it through the certification.

MD: Do you have any encryption methods for data that is really sensible?

TB: In some cases, the clients impose it to us. So there are some encrypted environments. For our own data, we have encrypted some of them, that are confidential. And the third vector, it's all that concerns communication with federal organisations, with the police… They impose us encrypted communication. There's a process as well, actually there are several processes with the DETEC, with the police… To transfer data to them and so that they are transmitted in an encrypted way.

MD: So you make data transfer with them.

TB: There are legal demands, if there are complains about clients… We are subject to this through telecom law so we answer to it.

7. Conclusion

MD: We're getting close to the end. We'll just conclude. Do you see an evolution in the kind of clients who ask for cloud services, since you've been there?

TB: Me, I see two evolutions. What we talked about earlier, I mean that people, now, want to know where their data is located. If we can tell them it's in Switzerland, it reassures them. The second aspect, which is becoming more and more important, is security. How is my data protected. It's a question, I think, that wasn't asked a few years ago, which may seem aberrant. But today, with all we read in the press, it's not only small businesses that get hacked, there are very big groups, that have used big means, or medias, TV5 Monde… It can have dramatic impacts. I think that today the public has become conscious of this and asks questions. Where in my opinion the people still haven't understood is, what is my data worth? I think there are a lot of people who take advantage of this. I'm thinking about fidelity cards in department stores, where people give away their data freely. Do they understand the impact of this and how their data is used, I'm not sure. I believe it's something that will come little by little.

MD: You think it will happen in the future?

TB: It will happen. I'm convinced of this. People will understand that we use their data and that finally they are providing the material that is used against them in the end. Which is detrimental.

MD: Do you have any idea of good practices, that you have put into place, that could be useful for another company that would like to install a cloud computing service in Switzerland?

TB: I think that good practices, for us, are mainly axed on the two terms we talked about: to have control over the data, physically, geographically, and to protect it. Today those two points seem crucial to me. You can't say anymore: "we're hosts, you can stock your data here, and that's all." I think that's over. And then, the geographical consideration, I think, are taken into account.

MD: Is there anything we didn't talk about you'd like to broach?

TB: We talked about legal aspects, we talked about security aspects, we talked about physical security… No, I believe we've seen everything.

MD: If we have further question, can we recontact you in the future?

TB: Of course.

Filename: 5. Innofield Bojan Jovanovic

Date of interview: 19th November 2015

Place: Innofield office, Brandschenkestrasse 150, 8002 Zurich

Duration: 1:34:06

Interviewers: Lucie Petrelis, Aurèle Nicolet (on Skype)

---

1. Introduction

LP: I just started to record.

BJ: Yes, so everybody knows it!

LP: Yes! and you just sign the consent letter. I'm going to give you the question. Here is an explanation of our project

LP: Could you tell me your name and your position in the company?

BJ: My name is Bojan Jovanovic. My position is, since we are a small team, I will say that "I'm almost everything". I will call me managing partner because we are CEO and CTO everything in one. But actually my responsibility is more to build the cloud architecture, to maintain the systems and keep them up in running. I'm more a technical guy than just the manager.

LP: How long have you been in this position?

BJ: It's actually my company, we started it in 2009, so almost 6 years.

LP: How long have you been in this company?

BJ: Six years.

LP: What kind of cloud computing services does your company offer?

BJ: We offer different services. The most well-known one is called XCloud, it's a very special service. Which is actually "Infrastructure as a Service" but mainly based on OS X machines. So many companies or many providers out there they have VPS services, for windows, linux, Unix and so on and we started with the same but OS X. It was, ammm nobody did it in the past and we were the only ones there, so that one of them. I know it's not used by typical companies but there is still a big demand for it. For example, on Spotify, all apps that you have on your tablets or smart phones or computers are built on top of our platform with XCloud. For example, if you want to build apps, for Apple devices, they have to be running on top of OS X so you cannot use any Linux or Windows machines to do it, you have to do it on OS X. That's one of the use cases for example. The other one is called Flow app engine. This one is actually a "Platform as a Service" category, it enables developers and companies to actually very quickly deploy their apps into the cloud without having to care about the system, the system landscape, the infrastructure tasks, and so on. And that's the one we are pushing now. So at the moment we have two serious products. There are others really small ones but at the moment they are not published and we are having some beta testers but more is coming in 2016. But for now we have these two services.

LP: Is your company a cloud computing provider or does it collaborate with other cloud computing providers?

BJ: I would say, at the moment we are a kind of independent cloud provider but more and more we are using for example Flow app engine this one is based on a software called Jelastic and this software can be used by any provider out there or any enterprise and this software is bringing us features like federation. So that means assuming we are up to date we just release and other hosters maybe for example some from the UK or Australia or whatever, if they also enable the federation feature we could actually offer our customers to have part of the system, part of the data in Switzerland. And if they have some clients for example in Australia and they need to have the data replicated there so low latency and so on can use these federation feature. But they will be built by us. For the moment we are like on an island with all these features on these tools we will be kind of collaborating with other cloud providers. So it's yes and no.

LP: When did your company begin offering cloud services, and how has this evolved?

BJ: Well, in the beginning it was of course not that easy, we even though it wouldn't work out because there is much competition in this area as you know. But as I mentioned initially, we started with that service called XCloud, it was unique, there was no competition at all in this area so it took as around half a year to really, start to earn money with it. At the beginning it was some friends we knew that recommended us and so on. But I will say that after half a year it started to get serious, and one and a half year later we could pay our salaries and so on. The evolving was hard at the beginning but after a while it was easy to manage and our focus has grown and improved and so on. I think thanks to being unique in this area with this unique service it helped us to involve faster and smoother. Just offering Windows and Linux machines to the rest of the world it would be nothing special so the way with this would be much harder.

2. Managerial aspects

BJ: I would like to mention one last thing. Of course the Swiss part, having the data in Switzerland, and that is something we guaranty in our contract, is a big benefit. Not only for Swiss customers since many of them are crazy about the fact that the data should not leave the borders. Looking around to what is happening, it makes senses to sometimes have it in your country, it doesn't mean it has to be Switzerland but just not anywhere and even foreign customers, Russia, many of them are from Russia and using the benefit of having their data to Switzerland due to good data protection law and so on. So this is also a big benefit for us that is just included since we are here. It's a very important thing cause many request: are your data centers just located in Switzerland? And when we say "yes", than we continue to talk. So, often this is the initial question.

LP: They feel safer…

BJ: Yes, They feel safer. I think when you think about it, many of them they send email that go to many servers worldwide and at the end of the day everything is going to different countries but I think it's a psychological topic. And of course it has some benefits but if someone wants to hack you, they will do it. It's a matter of money. Even governments get hacked so I think its relative. More or less it's a psychological thing but it's a benefit for Swiss companies and for Swiss cloud providers. It's an integrated included benefit that you don't have to pay for it.

LP: it's just there!

BJ: It's just there, exactly! So I hope it will stay like this. Ok, sorry, I thought it was an important thing.

AN: No problem! Are all your SLA's (Service Level Agreement) set in stone, or will the company negotiate or renegotiate each requirement with its clients when determining contractual obligations?

BJ: Well, by default it's set in stone because we are not ready and we cannot manage having different SLA with every single customer because they might have a small instance, let's say 70 CHF per month and if you have to talk to them about special SLA's it will be a nightmare. But for other companies like PWC, it's not a secret I can say that, they take our SLA and they know that we are not going to do that for them and that they have to do the work and we just need to sign it and check it. So they just take our SLA as the bases and then they add just a few points that are important to them. And then if there is, you know, nothing unusual, if it's something logical we agree to that and we sign it. That is maybe the thing, we are small and we are flexible so we can manage that. So I would say yes, but it depends on the deal size and the complexity of the project. We also are open there to have special SLA's per customers but we always used our basis because our most important things are covered there and so on.

AN: How do you contribute to support clients' information governance practices?

BJ: I don't understand the question.

AN: How do you help the clients to govern information.

LP: It has more to do with archival aspect.

BJ: Do you mean if we cover some regular, some laws for example to keep the data for 6 months or 6 years? That's what you mean?

AN: Laws, Tools for the record management.

BJ :Aha, well this is something which is always individual. You know we have the platform, the infrastructure to serve the software, the solution that is running on top, so that's up to the customer. We don't have at the particular time any special software for archiving. We have some SLA there that says ok this will be saved just for a year, or whatever. If the customer comes to us and they have archives software they can decide how long they are going to keep it. They can decide to keep it forever, it's good for us (!!!), but we are not limiting anything here. We just take care that the infrastructure is up and running and we take care of back-up and recovery. But how long the customer will take or keep the data it's up to them.

AN: How long does it take to implement the service of the cloud within a company?

BJ: Well the most correct answer will be, it depends, right? All depends on the complexity of the implementation. It could be a very simple one that would take a couple of minutes. Or it could need months. I cannot answer it in more details if I don't have more details on what kind of service, there are different options. And often it depends on how the opposite side is able to manage it. Sometimes some customers don't really know what is going on, on the background. They hear the term "Cloud" and then they think that everything is going to be on our side, without their input we cannot set up anything, so it depends. There is no clear answer to that. Sorry.

AN: Which method do you usually use, the bing-bang – all at once- or a slow roll-out?

BJ: Also here it depends, for example, we are moving now our full data center infrastructure to a new data center, this is why you can see here all our staff around and this is just a part of. Our office is full of hardware and so on, so we have for example one specific customer and they have a full rack with their own firewall and with our own storage systems, servers and so on. Let's say there going to be a new customer that we need to migrate them to us, this can be managed also as a "big bang". Because we have one firewall, one set of public IP's for example and everything is within this specific rack. So you can schedule a down time, for example Sunday, migrate the hardware, implement it on our site, bring it online, maybe you have to re-address the IP addresses and that's it. So we just did that two weeks ago with one of our client. So it was a migration at the moment but this could also be a new customer. But most of them are mostly slow roll-out. Nobody wants to risk any down time and especially if it's

our business critical applications often they ran test import and then they see if everything is well and then they schedule a productive migration. So I would say 20 percent big bang and 80 percent slow roll-out.

AN: Are you in charge for the entire deployment mechanism?

BJ: Yes, in most cases. Because in our experience, in many cases the knowledge, the IT know-how inside the company which is migrating the cloud is not that good otherwise they will not do it, right? It's my opinion! Because even having cloud providers, if you have the knowledge and the know-how inside, you could build your own cloud. It's a technology that anybody could do it. You can do it at home actually. But in most times they don't have the know-how. We even cover the deployment mechanism for them. So yes, we are in charge for the entire deployment.

AN: After the implementation, are you in charge for the adoption and the training of the staff?

BJ: You mean on the customer's side? No. But it happens not that often that we get for example many stupid question from one particular user on the other side or an admin not just a normal user, and after a while we saw that the basic knowledge is missing there, so we recommend them or his boss to send him to do a training. But it's not our job to tell them what to do and to send them into training, but sometimes it's necessary. Because it's a benefit for them as well if he gets good in a specific area. But not in a daily basis. So this is not our part.

AN: Do you offer the possibility of a lifelong learning process or you make educational seminars at the beginning without further teaching sessions?

BJ: There are some webinars we do sometimes for one of our product and it's going to increase in the long term as we will have some more products, but I can say that many customers today are used to have internet connection so the self-learner approach is very high. Often they come with just specific questions and if we are able to answer we do that. So maybe in the past, they had the IT department and they would go out for training. But today with the internet and all these technologies around us, I think this is decreasing. Because everything is available and there is no need to get a physical book in your hand to learn to operate a server and so on, I think this is decreasing. But we do some kind of webinars.

AN: Is there the possibility to have a trial experience of your service before making the official contract?

BJ: Yes, absolutely. That is very important to us. When you look at cloud service providers, I would say especially in Switzerland or in Europe in general, many of them when you go on the website, probably you have seen many of them while doing your research to find people for the interview, all of them are cloud providers. Everybody is a cloud provider. But when you want to try it out, often there is a "contact us". No click on a button, or free trial, or just enter you email address even without credit card and you get a welcoming email with log in credentials that you can start without contacting anybody. That was very important to us, from day one. And many customers in Switzerland they say that we are finally a serious cloud provider because we are really modern because many providers or products that come from the USA they are a step further than Europe. It's normal that you have a free trial and that you can try a product without having to contact a sales guy. At least this is happening in many cases. That is the opposite in Europe. Everybody is a cloud provider, but when you want to get in details, it says "please contact us" and then you have to talk to a sales guy and then blablabla. The new generation of people who are adopting the cloud computing is a consumer and they don't want that. They want to try it without any contact to the sales guy. So yes, we do that for sure.

AN: How does the data hosting works, in which locations (city, canton, region) is it hosted and why did you select these locations? (With which criteria, financial matters? law concerns?)

BJ: That's a good question. How does the data hosting works, it's actually very simple if you know how to manage it of course. We are not for example a data center provider. We are Cloud service provider. So that means we don't own our own data centers, it's not our business, but we rent Rackspace there. We get the power, the energy and the air condition, USP devices in our contract. So our part starts from physical hardware, storage service, network device, switches, and so on. It's actually nothing magical, you have to have the know-how to manage the systems that are running 24/7, if possible (!) and that's actually how it works. We don't own a data center, we just rent a Rackspace and build up our infrastructure on top of that. In which locations? Currently we are in 2 locations, one is in Zurich and one is in Basel. But just at the moment we are moving to new facilities which will also be in the Zurich area, in an even better one, and the second one which will be replacing Basel, will be in a former military banker. So it will be a very unique data center. Probably you have heard about it in some IT newspapers or in some blogs, there are few data centers inside the Swiss mountains and one of those will be also rented by us. More or less as a back-up destination. So we say to our customers that even if we disappear of a nuclear attack, our data will stay. We are also thinking of renting a room there, so if something happens we can stay with our data!!! So everything is in Switzerland, the new will be in the Swiss Alpes in Canton Uri. This new one we'll be rented in a different way to the current locations. There is a big difference. The current one's they are also not just offering Rackspace, they are also cloud service provider so they have their own cloud services, so there is a kind of competition. So it was important to us when we'll move away from them, we'll find another data center company with a provider that is not doing Cloud business. They focus on data centers and we focus on cloud services. Also in terms of competition and interest conflicts, and so on, it's a small team but many important. Many of them or many customers out there they are not aware of this, it is not their problem but it's a problem for us. For example, we also had some bad experiences, not very tragic but they could do it better this way so we decided to go away so that was one of the criteria for the new data center. So your question is very actual for us. Financial criteria? No this is more or less the same pricing, some of them are more expensive but, plus, minus, it's the same. On law concerns, in Switzerland it's more or less the same, there is no difference.

AN: When a customer cancels a subscription or terminates it, how does it go (off)?

BJ: They cancel it. One of our products you can cancel it automatically, they can just switch of and won't be charged any more or with your credit card. Even then you don't really have to talk to us. For the first product you just have to cancel it with one ticket by sending an email and that will automatically create a ticket. And then we terminate the service at the end of the billing period. Very simple. This is no rocket science.

AN: How long does the customer have to wait in order to get his data back? So you don't have the problem of the data back because you are rack and not data center?

BJ: Normally I never had the case where the customers asked us to export the data to a USP disk, or something like that, normally if they need the data they do that before, they copy it from the internet and that's it. So I think they are smart enough to think about this before canceling. I never had an experience that after the termination they asked me, where is my data?

AN: Do you provide any help for the transfer of data?

BJ: Yes, we do. As mentioned we never had a case, but we do. We also have that in our contract but of course they will have to pay for it if we need to buy any special hard disk or whatever, for the shipping and for all the effort we'll be charging extra.

AN: Does your company maintain a client data exit and recovery plan, should your business unexpectedly fold?

BJ: Yes, that's a very good question. Some customers are also asking this. If we will go out of business, actually it's not going to be stopped from one day to the other. It takes some time. We will just inform our customers to migrate their data and maybe give them recommendations. So that is how we will manage it, so there is no real plan for that. As everything is digital it can be transferred anytime so there is no restriction. But this is definitely a good question. We even had ideas to even talk to some partner companies to do it like: if we go out of business can you take over and we will do the same for them. But… I hope this will never happen! But that would be maybe one approach.

AN: If the cloud architecture is maintained in proprietary code, what extraction tools or strategies does your company provide or guarantee in the case of sudden closure?

BJ: The good thing is that we take care about this, so everything that is hosted with us, you have an option, even without contacting us, to be able to export it. So no proprietary code (go to 33:19!!!), so lock-in, that is the term in Cloud. No vendor lock-in. So this is also very important to us when we launch new services. Nobody likes that, and if we don't like that we will also not sell it. It's an approach.

AN: Would your company release source code to clients in the event of an unforeseen closure?

BJ: The company release because we are not developing our own software. The software we are using they are in many cases based in open-source and if not everything is based on open-source, you have not export feature. So this question actually doesn't apply to us. Because we don't have our own software.

AN: How does the cloud computing service works along with the retention schedule of your client's documents?

BJ: I think this one is more specific as a special solution for example for archiving, I think it's similar to the question before. We don't have any limits so it's up to the customer to decide what retention policy they want to apply to their software and the software they want to apply is up to them. Maybe there are some cloud providers that provide special solutions for archiving but they are probably specialized in this, but we are not. We are the general cloud service provider.

AN: If your clients have some data that, according to the retention schedule, needs to be destroyed, do you have policies to make sure that the data have been "shredded"?

BJ: We use shared storage and our default back-up policy and retention is 7 days. Actually customers need to maintain their long term backups but we do it for just disaster recovery reasons, we keep it for 7 days. So it will be automatically shredded after 7 days that they end the contract, at the end of the contract period. I think this questions applies more if a customer which is consuming cloud services have a dedicated environment and they really want to have these disks destroyed after the end of the contract period. So this question applies just in specific scenarios. So we don't have any policy with shredding any data, it happens automatically.

AN: Could the clients check and audit those measures?

BJ: I cannot answer to that.

AN: Has your company ever conducted a transfer of a client's records to an archival institution?

BJ: No. It's actually not our business to be honest!

AN: What issues, if any, were encountered in this process?

3. Economic aspects

AN: Which are the economic advantages, for your clients, in choosing the cloud computing solutions offered by your company?

BJ: There are a thousand things I can say! But I will say it's also a selling term that they have more time and automatically more money to spend on focusing on their own business and on what they do best and we take care about the infrastructure. For example, many of some smaller customers today they have maybe some servers in their basement somewhere or on a special office with some small air-condition system or even without any and this is 38 degrees inside and they have some old paper and the printer there… and you know what I want to say! But its in-house and its super safe. So having it in a professional data center where it will have everything organized in case of fire or explosion whatever, are some of the benefits and they are faster. Let's say they need more storage in one day to another because they have projects and new customers and they need to enable that with a start quickly without having experts in-house to take you weeks or days if they have time. It's enabling to do quicker business, faster business. There are thousands explanations. They can focus on their stuff and we can focus on our stuff. We don't do for example, archiving, you know. We do infrastructure, and take care that it's up and running 24/7 and back-ups and even in case of disaster that the data is replicated in another data center and so on.

AN: Do you use economic arguments to try and convince your clients of using your services?

BJ: Yes, of course, a little bit, on our website. But if we have any person face to face here and we are talking about benefits, most of the time we are not talking about this "bullshit" - sorry for the term-! We are more focused on enabling them and helping them with the features and functions we can offer. I think that most of them they know what are the economic benefits for them. But of course we do it on our website in the prospects, it's part of the game!

AN: Can we talk about a Return On Investment? If yes, how do you calculate it?

BJ: We try to give the best to do it and what we are trying, for example, is to be independent of specific vendors because we also have to buy hardware, we are also depending on other companies so we try to be independent and be able to order any parts from any distributor and this allows us to be competitive and also to calculate really the prices. So we are able of course to make our pricing calculation on top of this pricing which is more or less stable. And this is how we calculate it. We calculate our salaries, everything around it, rent, company cars and everything around it, including hardware and then on top we make a pricing calculation and we try to make the return on investment as soon as possible. But of course we cannot make the prices the double as competition. We are trying to fit somewhere there. And it works! It's a lot of work and I hate this kind of work, everybody here hates it, but we have to do it once. So how do we calculate it, all the costs we have and how much we charge the customer, per CPU, per RAM, per storage GB, per traffic, and so on. And then on top there are these catalogue prices actually.

AN: What are the pricing mechanisms? (One time license, monthly plan, "pay-as-you-go"?)

BJ: The pricing mechanisms at the moment with one of our products is on a monthly basis with a monthly plan and the other one you can pay it on a monthly basis or even hourly basis. The one on the hourly works like this, you have to fill your balance, your kind of account with us

and let's say you pay 1.000 francs and according to the usage of your service which is calculated in hourly basis it's using the money on this. So if your application is not doing something or you stopped it because you don't need it anymore or because the project has stopped you will not be charged. This is actually a very modern way in charging customers in an hourly basis. There are different approaches and since we are not selling any software we don't have a onetime license. So more monthly or hourly plans.

AN: How many clients do you have at the moment?

BJ: I think last time I looked it was 400 and plus but of course not all of them are huge. Some of them are smaller and others are bigger.

AN: Are they in the public sector, private companies, NGO's, international organizations?

BJ: Everything, a mix of everything.

AN: Mainly Swiss companies or international?

BJ: It's interesting but my stomach feeling I will say that there are 70 percent International and 30 percent Swiss.

AN: Which field are they in?

BJ: Also, different fields, not really a rule, I would say most of them are in software business maybe creating apps or having software that needs a server in the cloud to offer their services. I will say more software industry.

AN: What size of business?

BJ: Also a big mix, from very small to very big. But doesn't mean that the biggest company has the biggest contract with us, you know. The question here is more on the size of the business.

AN: In which countries are the companies' infrastructures?

BJ: The same answer here, from Australia, India, US, Russia, everywhere! I think we have customers in every continent. That's cloud computing!

4. Legal aspects

LP: If your company is international, are you subject to Swiss laws?

BJ: No, we are a Swiss company so we are subject to Swiss laws.

LP: How do they compare to other legal systems in other countries?

BJ: Good question, I think in terms of how the business works, Swiss laws have one of the strongest data protection laws and then that's compared to other countries, especially to the US. It's much better and especially better for the end users. In the US for example with the patriot act, the government or the NSA they can go directly to the provider like us, and ask for the data of a specific customer without informing the customer. If they have the paper, they can do it. And in Switzerland you must have a special document from the government and from the court, so it's not like we can do it just like that. It's more complicated and it doesn't happen usually. We never had a request like this, maybe other providers in Switzerland, for sure, but we didn't have any yet. I hope my answer was good enough for that question.

LP: Are your policies, operations, and/or services around privacy and the protection of personal information different across countries and jurisdictions?

BJ: No. Our contracts are based on Swiss laws, so the customer who uses our services is mapped to these laws.

LP: Concerning Swiss law on cloud computing, which procedures have been easier and which more complex in order for the company to operate in comparison with other countries?

BJ: I cannot answer that question because we never had this case. I think this questions are more for cloud providers for example Cloud Sigma, they have data centers in the US and in Switzerland. So of course if they have data centers there the data location they have to manage has this challenge. But it's not in our case.

LP: What is required for national, cantonal and European legal compliance?

BJ: They are many of them. Every country has some legal compliances and every second month there is a new standard or whatever, but there is one standard certification which is the most popular one and the most stable on, and Thank God, this one is accepted by 99.9 percent of customers and this is the ISO 27001. This one is good and this is something that we have. It's actually a data center certification. So this is one of the requirement when we select the data center and that is the case we do it. The current one and the new one. This is the standard, absolutely. There are many others, some European, and blablabla and some SAS 70. But ISO is a standard.

LP: What procedures have you put in place to insure that those legislations are respected?

BJ: Well, the most of the biggest part of this certification gives the possibility to choose the data center provider so we automatically profit of those things they do. So we have to make sure that the systems are up and running and protect the data of the customers and physical protection is covered by data center providers so it's not in our responsibility. We have to trust them, it's an eco-system. I think the only cloud service provider in Switzerland that has its own data centers is Swisscom, all others are renting data center Rackspace.

LP: Are clients made aware of all data that you collect on their usage?

BJ: This question doesn't really apply to our business, it would be more for a company like, software as a service like a new Facebook or whatever, and they run it in Switzerland and then they have to collect the user's usage. If the customers is with us than his with us, they know that their data are with us so we are not pushing them to do it. So, the collections is their responsibility and what is on the server. So it doesn't apply to our business.

LP: What guarantees of anonymity and security are in place surrounding these practices, and can the client opt out of the data collection?

BJ: It's the same as before.

5. Security aspects

LP: What measures or policies do you have for data security in your company?

BJ: There are no real policies, what we guarantee is based on our SLA is that we save the data within Swiss borders and Swiss data centers and that we protect the data from any disaster and so on. So there is no special policy or measure. It's something in the contract and we do it on a daily basis. The key point of our job is to guarantee that. But no measures or policies in detail.

LP: Is data security an important point for your clients?

BJ: Oh yes! Definitely! For every customer that is important.

LP: How do you manage client's fear or hesitation about data security?

BJ: Most customers that decide to go with us they like our approach about having integrated backup and even disaster recovery. So that, and don't know how many interviews you did in the past, but it doesn't matter what service they are using with us, everything is integrated with the backup, even customers can do their own backup but we do it on another level, independently if they take care of that or not because many of them are expecting that from Cloud providers. They don't want to deal with that and that is something that we do and it's how it should be. And we also replicate these data from one data center to the other. So in terms of data protection, data security, we try the best to cover all aspects. Not just the security with the firewall and so own, that is easy, it can be done from everybody, but also at a data protection level. With many competitors out there, many customers are responsible for their data. Or if it's included then it doesn't have to replicate in other data center which is 50-60 km away. And that is included in all our services. There is no difference between if you pay the lowest plan that you are not included in the disaster's recovery, everything is included. And that's what people like about us. If they have data with us, they are covered. This is the good answer to the question on how we manage clients fear.

LP: Do some of your clients have special demands concerning data security?

BJ: Special demands… Yes, this is more specific on the firewall level because on the deeper level having the data replicated, it's something we cover as mentioned, and if they have some special requirements, it's something that can be handled on a firewall level which is the entry point from internet to their data and we have a nice firewall solution so we can cover all their requirements. They are some that have some special demands but everything is possible with these tools. We never had any customer which had some special requirements that we couldn't handle.

LP: What kind of protection against malicious insiders and the misuse of client data by your employees and subcontractors does your company take? (E.g. Background checks? Certification? Legal contracts? Session and/or click monitoring?)

BJ: Yes, for example what we do is we have, I won't talk about this in detail, but we have a very special approach on how we block access to the data of the customers, there are several levels which you have to enter and from there you have to hack another one and there are three hard levels. It's a little bit a secret on how we manage that. For example what we do with our email account and access our data because many documents from us have some critical data from the customers, we use 2 factor authentification for example. So even if you have an email address and password you need to have 2 factor authentification and so on. We are doing everything that is possible to protect the data. There are no certification for that, it's just our effort based on our experience and our knowledge.

LP: In the case of a security breach due to a malicious insider, is the client informed of the incident, the cause and the nature of the breach? How public is this information made?

BJ: Yes, Thank God we never had that, but you know that today everything is possible and dangerous. Internet is a big mess, maybe you are reading in the newspapers, for example the company from Geneva, Proton-mail, they encrypted email service and they've been attacked the last few weeks for several days. They've been online and it was a big damage to them. Thank God, today we didn't have this issue or this case, but if that happens of course we have to make it public and inform the customers because you need to manage it.

LP: What steps would your company take in such a case?

BJ: First of all try to make sure that these guys are not inside anymore and then try to make it more secure to find out what was the hole (the leak). As soon as everything is clear, we inform the customer.

LP: Have there ever been criminal proceedings brought against an employee or subcontractor? What rights and/or compensations are awarded to a client in a case where you are at fault for data exposure or exploitation, if any?

BJ: No, it's something that is not in the contract of the SLA. This is not covered. To be honest with you no customers has ever requested something like this. Maybe if that happens on a monthly bases then they will come and change all contracts with that, but I hope it will stay like this!

LP: Do you use a back-up system? Do you make duplications of the records or a printed version?

BJ: Yes for back-up system. Since we have all digital, we have the backup system and the replication in other data center so really in case of a logical issue and physical damage, we have it on a totally other location, so no need to print it.

LP: How do you deal with data loss? Do you have some sort of insurance policy?

BJ: No, we don't have any insurance for that. Also here, we based on our infrastructure and our approach on how we deal with the data, and something is on our contract and on our website, one of our benefits we try if best there won't be any data loss at all, Thank God also here, we never had any data lose at all. Me and also the other co-founder, we both are from the storage area, storage system and so on, so this is our key domain. So that's our focus and priority on this.

LP: Are there different levels of security?

BJ: This question is too general. Which specific area?

LP: On protecting the data.

BJ: Oh yes, that's something I mentioned before, yes you can call it different levels, you have to brake 3 doors until you are reaching the customers data and that's something we are managing on our side. We have three different levels.

LP: Do you provide your clients with information about who is having access to their data if they request to know about it?

BJ: This is also in the contract that our employees have access to their, not to their data directly, but to their systems. There are tools and software solutions that you can encrypt your server and that is even included in OS X or Windows or Linux, so if the customer enables this kind of encryption, even us, as providers, we cannot access these data. So they have the choice also to secure their very last level of data. But they are aware, that is also in our terms of services, that our employees have access to their systems. But not to the data.

LP: If your company has some subcontractor, do you require that your subcontractor have the same level of security and privacy policies as your own company?

BJ: Yes, we actually don't have subcontractors because we are trying to focus on our services and if something is there… we receive many other requests asking us if we do this and this, and then of course we are small team and we want to focus on our business, maybe technically we have the know-how to manage it, but we say no. And in this case you will have to work with a subcontractor but we don't want to deal with that because then we would need project managers and then this and this… There are many companies out there, then you have the

choice. We are infrastructure provider and if you need a specialized know-how in this particular area go look for that. We can give recommendations in some areas but we don't have subcontractors and we say yes you need this, this one is for you. So that doesn't apply to us. But if we would do it, probably yes, we would require the same policies.

LP: Who is in charge for your customers data?

BJ: Who is in charge. What's the meaning of this question, can you maybe described it in a different way?

AN: If you are subcontractor, when you are one who is in charge of the data.

BJ: I guess I have no answer for this.

LP: Do your clients know where their records are hosted?

BJ: Yes they exactly know it.

LP: Do they rather have them in Switzerland, or abroad, or they don't wander/ don't mind?

BJ: Most of them they care and they want to have them is Switzerland. Not all of them but many of them.

LP: Do you make random tests to make sure that the data assigned to you from your customers are still present in your system and in a good shape?

BJ: Yes, we have an automatic test which is using the backups we create and it's doing a clone of it and restore it to see if the data is consistent and so on. We do that on a weekly basis.

6. Technology aspects

AN: Can we combine the cloud computing application with other tools used for record management?

BJ: Yes of course. I think especially for record management, you mean here solutions for having big archives, you mean of big amount of data. I think 2 pieces are here important, that's the infrastructure part, that you can actually rent it in demand with cloud with transparent pricing you know if you grow how much it will cost you, and then on top you have the choice as customer to decide which software, which solution should be used for managing your records. So we are independent, you can… there are… oracle has this open text, I don't know if you know this one and there are many archiving solution and this combination of two of them, yes you can combine and have a final complete solution for that.

AN: How much control do your clients have over their data?

BJ: This is something probably also relevant to the archiving tool or archiving solution, this is the job of this tool, to show them where it is and how much, and so on. Probably all serious archival tools have this.

AN: Can they visualize the state of their records using applications or software while using different devices? (PC, tablet, smartphone)

BJ: It depends also on the solution which is used. I can't answer that! This are specific questions for the archiving solution.

AN: Can they make modifications on the metadata of the records on their own?

BJ: Yes I think this is the same story here. I can't answer it, but normally I would say yes!

AN: How have the existing privacy legislation and requirements been factored into the controls and architecture of the system at your company?

BJ: I think this question is the same related to the consumer or the user of the cloud computing in combination with the archive solution. I mean the existing privacy legislation, you mean the company that is using the service, right?

AN: It's about the legal questions, about the privacy and how you built in your architecture.

BJ: Oh yes, I think this is a kind of harmony you have to follow this rules or else you are not compliant in the services you are offering. You have to follow the rules for these requirements and adopt your solutions in architecture that follows these rules. That's how we do it.

AN: What do you think about multi-tenancy?

BJ: It's great because, it's not great for every use case, but for many it's good enough and especially you benefit from much better and attractive prices in multi-tenancy environment. So that's the main benefit. And automatically if new features came up, this multi-tenancy system gets updates to new releases and new features and automatically profit of new features and so on. But also there are disadvantages, if you have multi-tenancy system and something goes wrong, everything is affected as well. But in general, I think that many cloud services are built up on a multi-tenant environment. It's part of the game, I would say, in cloud computing.

AN: Do you offer your clients alternatives to a multi-tenancy model? (e.g. services based on a multi-instance architecture, etc.?)

BJ: Yes we do. We have this, I talked about that at the beginning, it's called Flow App engine, it's a Platform as a Service, and it's a solution which is built on a multi-tenant model and if they are customers that have really super special requirements, I would say 95 percent are covered with that solution, but if there are they can go with dedicated servers. But then they have to manage it or let as manage it, extra for them. But all this costs extra. So it's a question of money and of how much time intensive it is. But it's possible we offer both alternatives.

AN: Do you offer insurance or other forms of protection for business losses resulting from a lack of access to records due to server seizure or other outages arising from a multi-tenant model?

BJ: Yes, we do. Our SLA is based on an availability percentage, right, and if you have more outages that guaranteed in this SLA's than you get based on an hourly basis you get a 5 percent of a monthly charge and so on. There are some rules, described in the website. And don't know all the details. Thank God, we never had the case to pay but you never know. To answer your question, yes we have something in place. And its transparent for every customer, we don't hide it.

AN: Do you provide clients with any information on who they share tenancy with?

BJ: No, some of the customers on the website, as reference customers, so they can guess ok, that these customers are as well on the same platform but not in detail.

AN: Do you know at any given time with whom your clients share tenancy?

BJ: No, that's the interesting thing, that many of our customers using a multi-tenant landscape or platform and if you think about it in the background, we are also using a multi-tenant data center, right. A data center using a multi-tenant energy consumption and even our customers, some of them, which have built their applications, their web applications on top of our multi-tenant platform they have their own multi-tenant solution for their customers. So everything is

multi-tenant. This world is multi-tenant! But we don't know from our customers what kind of customers they have on top. Maybe if we knew them personally but not in general.

AN: One of the critiques of multi-tenancy is that it can facilitate data mining by service providers, as client data is often held within a single database and/or application. For clients worried about privacy, how would you respond to these concerns?

BJ: The multitenant system I just talked about, it's in terms of data they store, it's not multi-tenant, it's isolated. So that's one of the benefits of this system so if such a question pop up we can answer quite easily and also in the technical basis many knows what is running in the background, so every customer has his own container, maybe you've heard the term "docker containers" (1'19'30), I don't know how you are in the text stuff, So everything is actually isolated but it's running on a multi-tenant platform. So data is not shared between tenants. So that's how I would respond to these concerns.

AN: What does European, national and cantonal legislation require for multi-tenancy issues?

BJ: There is nothing in details, nothing in formal details about this.

AN: What do you think about vendor lock-in?

BJ: What I think… I think no customer really likes that, because there are many many cases where you probably will like to switch to another provider or maybe the provider is going out of business and you will have to do something and if you have the vendor lock in especially if you have a big project or a big solution on top of a cloud provider than it could be very expensive thing. So as mentioned before, we are also trying to offer just products and services that don't have any vendor lock-in. And the general trend today is that almost all servers and popular solution out there, which we are also using are based purely on open source basis. Maybe 10 years ago, Windows and Microsoft, have been the standard in enterprises but this is changing right now. Linux is growing and it's more popular even in enterprises, it's going into them so that's a good development.

AN: Do you try to propose / suggest an open-source solution?

BJ: Yes, always if possible, yes we do it.

AN: What has your company done to ensure that the clients feel in control of their data/records at all times, including the ability to terminate the service without data loss?

BJ: As they have access 24/7 to their data, they even have an option to sink it somewhere else, for example some customers they know that we do all the back-up but they say, we love you and we trust you, but we still export our data on a daily basis to their office or to another provider, so they are super sure. But we are not limiting our customers in any way that they won't have any access to their data. It's called transparency. And they have route rights to their systems (1'23'23) so there is no reason to worry about this. With typical, with maybe old school providers, in the past you called them hosting providers, now you call them cloud providers but it's the same, that the technology has changed more things, more automation and more self-service approaches. In the past it was like a black box, on the provider's side you didn't really have the feeling of what is going on and how it is build up and so on, but today you have a very transparent connection to your data and then you have many options to export it at any time. Even without letting us know, and that's a good thing for customers.

AN: How can you assure the integrity and the authenticity of data?

BJ: That's actually the job of our file system in our storage boxes, this is something which the software, the technology is covering for us, so you cannot check that on a daily basis, it's the

part of the job of the system. And if something is not ok we need to check it, but normally this is very stable.

AN: If there are data which are strictly confidential, do you use an encryption/decryption method?

BJ: Yes, and this is actually open to every customer to enable it, it's not abled by default because it means lower performance for the data especially if they are in high performance business. Encrypting and decrypting every single block every time will be an impact on the speed and performance but for them, who they really need it, they are free to do it.

7. Conclusion

LP: Do you see an evolution in the kind of customers who request cloud services today?

BJ: I will say that… give me a minute. I think, I will not call it evolution but I will say that all the young guys that are leaving now the university or finishing the school in IT area, like developers and so on, for them it's just normal to use Cloud services, You know, it's part of the game! And maybe with older people that are used to have the servers in the office or somewhere else, it's still a big challenge for them. Think about not having the data in-house. Even it's more secure to have it with the provider. It doesn't mean that it's better but I will say in most cases. So I will say for the new generations cloud services are just normal. It's like having the energy coming out of the wall. Maybe we can put it in evolution phase because in 10-15 years, nobody will buy a server anymore to put it in an office. Just providers will take care about that. Even in enterprises, because today even if the enterprises don't deal with IT, you heard it about moving all the services to the cloud or to external companies to manage it, so that's actually my opinion and that is something we see on a daily basis and what the point with the classic customers, maybe older guy, is what we see there is that many of them don' have enough knowledge about these topics or are maybe scared with this and there is a big challenge for them to make the switch because with us for example we are a provider offering an infrastructure service, but they still have to manage it for that. We give them the computing resources but they still have to manage it and they don't have the skills to do that. And for this they will need an additional company that will do the managing services part. And then when they hear about that then they become confused and then they hate cloud computing. But this is just a matter of having the skills that's the point. So to be honest with you we are focusing on the new generation of customers and we are not going out to say that ok company X with 5 employees that are selling bread we want to have their data in the cloud. No. it's too difficult and complicated to talk about them about this. There are other IT consultants which are doing that very well and they should keep on do that, but we don't.

LP. Have their demands changed over time? In these 6 years.

BJ: Yes I think that the situation is getting better because more and more customers are used to cloud computing eco-system so it's not a question of should we move and what is the benefit of cloud computing, we are already in the first step talking about implementation and features. So I think this has changed dramatically. Even at the beginning they said: "where is the data" and "how you do it?" And so on, even if it's on the webpage. I will say 6 years later they are like "how this and this work", "how can we implement this?" and so on. It's changing and it's good! It's great for us!

LP: Are there any best practices gained from your experience and adopted by your company on hosting a cloud computing service in Switzerland that you believe have been important assets?

BJ: Yes, best practices… I will say that you should just focus to serve the customer with everything and not just to say we are the cloud provider but we don't take care of the back-up for example, and many of them they maybe write it and they do back-ups if you additionally pay for it and check it on the order box. So our experience is just, serve it, with the food, salt and pepper! It should be there without them asking for it, don't ask additional money for it. Serve it! Like energy from the wall.

LP: Do you have anything to add? Is there any issue you believe we didn't treat/cover?

BJ: (Thinking for some time) At the moment nothing pops up to my mind. Many questions were general so maybe I was a bit confusing but I think I covered everything.

LP: Are you willing to answer further questions at another time, should we need additional information?

BJ: Yes if it's short and simple.

LP: Yes of course just if we didn't understand some details.

BJ: Yes of course!

Filename: 6. Infomaniak Siméon Gourlin ENG

Date of interview: 7th December 2015

Place: Infomaniak office, 26 avenue de la Praille, 1227 Carouge

Duration: 48:44

Interviewers: Marion Destraz, Arina Grazhenskaya

---

1. Introduction

MD: Before everything else, can you remind us, just for the record, who you are and what your position in this company is?

SG: My name is Siméon Gourlin, I am a system engineer. I deal with… I'm part of the production team here, at Infomaniak Network. So everything that's operational… and a bit of research and development too, mainly on Infomaniak products.

MD: OK. And how long have you been at this post?

SG: Five years.

MD: And how long have you been at Infomaniak?

SG: Five years, too.

MD: You started at this post right away.

SG: Yes, we have a first level support here and the third level upstairs.

MD: OK. And what interests us in particular are the cloud computing services you offer here. Can you tell us a little more about the kind of product you offer, of services?

SG: Yes. Mainly managed servers, or not managed, in cloud version. Historically, we already did virtual machines on… it wasn't called cloud back then, but here. We have done this for a good few years, virtual machines for clients who had small needs or medium needs for a physical server. Then we migrated two years ago, more or less, to cloud solutions. So we exploit this mostly inside, we don't give access to all functionalities to the clients.

MD: OK.

SG: But this allows us, in any case, to propose new things, to be… how to say… a bit more competitive, a bit more reactive too on some functionalities by integrating these machines directly into a cloud.

MD: OK. Do you collaborate with other cloud providers?

SG: No… I mean…

MD: It stays inside.

SG: It stays internally and we develop almost all we do internally, too. So we don't have any outside needs for that.

2. Managerial aspects

MD: OK. So, for the next part, do you have SLAs? Are they fixed, or is it negotiable, when a client signs a contract with you? Can we discuss terms beforehand?

SG: So that's more of a political question and… I don't know much about that. I know we have a SLA that's applied by default to the client. Particular contracts, there are some, but I don't know the terms, or the number.

MD: But it exists?

SG: Yes, with privileged clients, we have slightly different agreements.

MD: OK

SG: But it's really case by case.

MD: OK. And then, do you have any way to help clients manage their data, or do you let them do it on their own?

SG: It depends. We have two kinds of offers in what we do in cloud. We have managed type server, it's us who create the machine, who leave just an interface to the client so that he can manage his sites and so on. And then we have non managed machines where the client has total access to his machine and do whatever he wants. We use the cloud only for the server part, we don't do any file storage for now, object storage, all this we don't do. It's in project, but…

MD: Ah, it's in project.

SG: A lot of little things to take care of, and stability, all that.

MD: And this project, do you know when it will be implemented?

SG: It's scheduled for 2016, but…

MD: So you don't know for sure, but it's close anyway.

SG: Yes, it's pretty close.We're doing tests right now. But it's not yet open.

MD: OK. So, when you have a new client, how much time does it take to put it all in place?

SG: It's very quick. In a few minutes the client can have his machine.

MD: And are you in charge of the whole deployment mechanism?

SG: It's all automatized but yes, we take charge of deployment.

MD: And once the deployment is over, do you help the client use the service? Do you propose formations?

SG: Yes, through our support, we have FAQs, documentations which help you start. And regularly, clients call us for the first few steps to take. Our support helps them with that.

MD: So it's always here if you need it.

SG: We also have some offers to install more or less in their place and configure it afterwards.

MD: OK, but it's all remotely. Don't you do, for example, seminars, or lessons?

SG: No, it's always remotely, either through the web or by phone and support.

MD: Is there a possibility to test the service before signing?

SG: It depends who, but we had in some periods offers with a month free or something like that for clients who wanted it. And in general, if a client sees that it doesn't work for him, we pay him back and he chooses another product or tries somewhere else. But there's always a possibility to discuss about this. I know at a certain point it was more or less, for partners at any rate, we had free months of test. Now I don't know if it still exists, but we regularly have this kind of operations.

MD: Then you told us you don't do data storage…

SG: No. There are two parts in the cloud: either we stock files if clients want to do backups of their pictures, for example. A little like Amazon with S3, services like that. We, we didn't have the time to develop this part already. For now, it's really virtual machines to stay in our business of websites and all this. So clients who want to put a site online, or several sites, on a single machine to be more isolated, have their own resource, have a lot of resource if they need it, we're more in that kind of market. So they have the data of their site with us, a bit like they have mutualized service or other things with us. We manage it more or less in the same way.

MD: And talking about physical hosting, where are the servers?

SG: We have several data centers. We have one at the Route du Bois-de-Bay and one in Vernier. That's it for now.

MD: Both are in Geneva, right?

SG: Yes, both are in the canton of Geneva. We have a historical one upstairs.

MD: But it doesn't work anymore?

SG: Yes, it works, it's currently migrating.

MD: Ah, OK. Do you know why you chose to have those data centers in Geneva?

SG: Hmmm… Why… No. It was a management decision, but no it's so that we have something close and mostly in Switzerland. It's important to keep things here. And then there's another fact, it's that since we do everything ourselves. When we need to move a machine, after it breaks or something like that, ideally it has to be as close as possible.

MD: Better not go to India or something like that.

SG: Exactly.

MD: If a client decides to cancel the contract, how does it go? Is it automatic, does it take place at once or is there some time…

SG: No, no, it takes place at once. There's an admin interface for our clients. They can chose to cancel a product. So I don't know if, accounting wise, we wait until the end of the month or something like that. At the technical level, as soon as the cancellation is signaled, we destroy the data and that's it.

MD: OK. So you destroy them.

SG: Yes. In the cloud, at any rate, I mean even with the rest, we destroy machines and that's it. Then we have back-ups of a few days, but it's kept for maximum one week after the client cancelled.

MD: And if they ask for help to recuperate the data before canceling?

SG: We can do that, too. It's to be checked with support, but it happens that… At any rate, we put at disposition of our clients all their data and the archives of the last seven days. So they can recuperate in case there is a problem, for example their archives of two or three days ago.

So if they need it before they cancel, they can also have those data, of course. And it happens that a client cancels but hasn't done his data back-up yet. In the limits of what we have available, that short week, we can help him.

MD: And do you have plans in case of problems? Not right now, but if your business were to fold suddenly, do you have a way to give the clients their data back, in such a case?

SG: So… Well, we have plans in case of breakdown, at any rate. Now, folding, I hope not.

MD: I don't think it will happen tomorrow, but…

SG: But when we have machine breakdown. Absolutely, we have plans to recuperate the data. We also have those back-ups which we use from time to time, when we have to, to put the client's data back online in a minimal amount of time.

MD: I see.

SG: Sometimes it's a few minutes. Sometimes, a few hours. But we try to stay in reasonable limits.

MD: OK. So, moving on… About the architecture, is it proprietary code?

SG: No. We use OpenStack a lot, it's a free cloud software, one of the first and the best.

MD: Yes, we've heard of it.

SG: So, our architecture is based on that. Then we have a few homemade scripts to go around that. We use those a lot internally. We don't give access to all functionalities to our clients, but we have small shortcuts to create a VM automatically from our admin.

MD: OK And for them there's no problem with recuperating it later.

SG: No, no. We try to do as much as possible with what OpenStack allows. There are APIs. So we use these APIs, and that's it, in the hope of having those functions made public someday, of course. That's the idea we have now, at any rate.

MD: OK. How do you do with the data and information management, I mean if they have data that needs to be destroyed at a certain time, can you do this for them?

SG: Yes. Absolutely, when a client cancels, he knows those data will be destroyed.

MD: Yes, but if he doesn't cancel and there are only a few things on a server he wants to erase.

SG: That's for him to manage. As long as the client is with us, we won't destroy those data for him. However, we will give him tools to destroy his data. The day he wants to destroy them, he removes them and that's it. But we don't do that automatically.

MD: OK, they do it themselves. Can you prove to them that it's been destroyed?

SG: Often, they ask us to restore them. And we don't have them anymore because they just erased them.

MD: That's a problem.

SG: It's the inverse problem.

MD: And do they sometimes ask you to prove that it's been canceled?

SG: No. Then, we have several offers of non managed servers, we don't have any control over the machine, so we don't even do any back-ups for the client. So when they destroy the machine, the data are destroyed at the same time. And… We also have other offers, synologic servers, for example, which are backup servers for enterprises, on which we can't act. So, same, there are no archives with us or anywhere else. The client has his data on this. When he decides he doesn't want them anymore, he destroys them or cancels the product and all is deleted. We really only keep the data relating to the offers in which we say we keep the data, because it's more or less managed by us. In any other case, the client takes care of it.

MD: Has there ever been a case in which you had to transfer data from a client to an archival institution?

SG: Archives, no. We sometimes have demands from the law.

MD: And how does it goes, in cases like these?

SG: Most of the time, we answer if it comes from Switzerland. Since we're subject to Swiss law. Now, we have several which come from other places, which we don't answer, because quite simply we don't have to. We try to collaborate with Swiss authorities, transparently when we can. When we have the data they ask for, which is not always the case. Now, most of the time it's not log data, it's the content of an email for example. For this we have nothing and they don't ask for it, either. So we give them the logs we have. The metadata, so to speak. Mainly, I mean only when it comes from Switzerland. When it comes from someplace else, we don't have to.

3. Economic aspects

MD: OK. We will come back to that eventually. But first, the economic aspect of the question. For your clients, is there an economic advantage in choosing your services instead of another?

SG: So… No… I'm not sure about the concurrence at this time, but it's true that the… if you take, typically, the product, a virtual server with that much resource, in Switzerland, I think it's pretty competitive but compared to something in France no, or in the world. So, what the client pays for is more quality of service and a geographic emplacement, rather than… pure resource. Clearly, you can find cheaper for equal resources in other countries. Now, in Switzerland, French speaking Switzerland at any rate, we are well placed. So yes, for Swiss people in Switzerland, it's advantageous.

MD: And is that an argument you use, the economic argument?

SG: Yes. I mean, it's true that… it all depends what you compare it with.

MD: Yes, of course.

SG: We have clients who come from other providers in Switzerland who pay more for the same service and who are happy to come with us. We have others, too, who are mainly French clients, who paid less before and decided to have a little more quality or a little more functions and to pay a more with us. Then you have to compare, in terms of resources, on the paper we tell you, you have that many processors, that much memory, disk space, and there is the quality of service too, a support level that you have to take in account in regard to us.

MD: Is there a return on investment for the client?

SG: In most cases I hope so, yes. Otherwise they wouldn't stay.

MD: But they calculate it themselves? You don't offer…

SG: No, no. We don't do any calculations, saying: you used to pay that much, now you will pay more, but… It's for each client to make his own little calculation. Then we work a lot with partners, big web agencies in Switzerland which do the calculation for their clients. But it's not our… Well, we don't do it systematically, at any rate.

MD: OK. For paying, how does it go? Is it by month?

SG: That depends. We offer by month, by term or by year. So the client chooses for how long he pays and that's it.

MD: OK. So it's payable in advance?

SG: Ehh… I don't know anymore. By year, in advance yes, but by month, I don't know if it's the month in progress. In any case, if the client is late paying, we keep the service and warn him for a few days, and warn him in advance when needed.

MD: I'm sure you do. Do you know how many clients you have, more or less?

SG: No, hard to say.

MD: Do you know what kind of clients they are? More public or private? NGOs, or international? National?

SG: It's pretty hard to answer. We have quite a few SMEs and private sectors. We also have public contracts, but… We're currently doing a few ISO norms to have more of them, actually. But the "historical" target is more PMEs.

MD: OK. So that's what it is.

SG: We have several associations too, in fact. NGOs and all that. I don't know in what measure, actually.

MD: So you have them, but don't know how many. Are there more Swiss companies, or international?

SG: A lot of Swiss ones, thankfully. Then we have quite a lot of French clients, I know. International, but a lot of french speaking clients. And from African countries, things like that.

MD: OK.

SG: We have one big Belgian client, as well.

MD: French speaking, then. And more… No, that's okay. We can move on to legal aspects.

SG: Then it depends on the offer, too. On cloud offers, it's more key in hand. We have radio offers, it's a different public altogether.

MD: We're more interested in cloud. But it's interesting as well, radio, television…

SG: Yes, radio, television. Often it's other services. Then we have a few clients who take all of them. Who have a radio, a website. It's interesting for them because they have everything in the same place.

4. Legal aspects

MD: So we told that you were Swiss, and are subject to Swiss law. Do you know, if you know, how it compares to other laws in other countries? Do you have any idea?

SG: No, not really. I'm more technical than legal.

MD: Do you know what Swiss law says in matter of cloud?

SG: In matters of cloud, specifically, no. We have laws on log retention, for example, or things like that. We try to respect them. Then it's more general laws on information and all that.

MD: Data protection?

SG: Yes, that's it. More than specific laws on cloud offers. Cloud is just a word for several technologies, in fact.

MD: The technical aspect will come, but not right now. Do you have any special procedures to make sure you respect the norm?

SG: Yes. Well, in any case, we have a lot of markers that tell us when we… if we have, how to say… we have services for our log archiving, backups, all that. We also have alarms when these things stop working, which allows us to make sure we keep what we have to. Simply put.

MD: Do your client know what data you have about them?

SG: that's a good question. We ask them for some data when they sign up with us through the admin interface, which is up to date: email, telephone, all that.

MD: That's clear. They know it.

SG: They know, of course. Then, in regard to their website, we keep some of the logs. It's standard in the business, for providers, as the law asks for it. Web agencies know it, because they are more technical. The average client, I couldn't say if they know it. Those who are interested in this, probably. Then we don't keep any more information than the law ask us to. It's still a lot in terms of disk space. So there, we don't want to put too many resources in something we don't use.

MD: Of course. And you make sure it's anonymous, don't you?

SG: No, that's for sure. We guarantee it, naturally. Datas are used internally. We don't use them for partners. They can ask, same, through the admin interface, to have an offer for another website, but in that case we tell them we transfer their demand to our partners so that our partners can contact them. But they give their consent for that.

MD: OK. So they always know who has their data.

SG: Yes, that's it, or when they ask for a special offer we ask them if we should ask our partners or not at any rate, for these kind of things.

5. Security aspects

MD: OK. Let's move on to the security aspect. Do you have any measures to assure data security?

SG: Yes. Well, we take care to keep our programs updated, to detect viruses, intrusions, things like that. We offer, for our web hosting, to mutualize the cloud that we manage. We have an antivirus, and things that scan files before the clients put them on their space. Which allows, if their password to an FTP account gets stolen, or a pirate tries to put a virus, he will be blocked. We have a few protections like that in place.

MD: Is security an important issue for your clients? Do they worry about that?

SG: Yes, a bit. It depends, of course, but a lot of our clients, today, use CMS, things ready for use like Wordpress, to make their website, and who don't keep them updated. And then, how to say, in a mutualized offer, for example we have several websites on the same machine, we have to be very careful if a site gets infected, that it can't contaminate other sites. We have all kinds of securities linked to that and we communicate on them, too, in regards to the antivirus for example, so that our clients are reassured and know that we do what needs to be done so as not to be had at this level.

MD: Perfect, this answers my next question. So we can directly go to… Do you have protection against malicious insiders, people inside your enterprise? Are your collaborators watched in any way? Do you do background checks?

SG: That depends on access rights.

MD: Yes, I suppose it's not the same for everyone.

SG. Our support service doesn't have access. We only have a small production team which has access to everything. That's changing, too. We try to put more and more things through versioning systems and so on so that, we can, not trace, but go back to the source if there is a problem. Not only in case of malicious intent, but it happens to make a mistake sometimes, and not notice until several days later, and then we can know, "yes, that was why", and that's it.

MD: If there was someone malicious anyway, would you inform the clients of what happened, or not?

SG: Yes, so… Well, if we made a mistake on our side, at any rate, we inform the client of what happens. A malicious insider, it never happened, but a mistake, that's happened in the past. Then we are honest, we try to do what we can. It can happen that mistakes are made, we communicate it to the client, we patch it up and that's it.

MD: OK. Until now, there hasn't been any major problem?

SG: No, no. The production team is really only a few people and there are a few months while the persons are integrated with different tools, before they can have access to everything. So the problem never really happened.

MD: OK. So, you said you used back-ups. Are all data backed up or does it depend of what clients ask for?

SG: All data which… From our managed offers, actually. All we're supposed to manage for our clients. So a managed offer, we say to our clients: "you have a website, you don't have to worry about server configuration, we do this, you just put your website somewhere and it works."

MD: OK, so you do copies of that?

SG: Of that, we always do copies. Now if a client takes something or says, I want to manage myself, we don't do any back-up. They know we don't do any back-up.

MD: They can do it themselves.

SG: They can do it themselves, if they want. We have clients that take several machines with us to make back-ups of one on the other one, for example, but it's pretty rare. Well, for some we know, but we don't know what happens inside, at any rate.

MD: OK. And what happens if you were to lose those data? Do you have insurance, or things like that?

SG: So, same, for now, as far as I know, it hasn't happened either.

MD: Good for you. But if it were to happen…

SG: If it were to happen, yes, we have… We have general conditions with service levels that are more or less by default. If a client, for example… we have a mail that we lost… in that case, we tell him, we don't necessarily have penalties. Now, we have more important clients where if it were to happen, we might have penalty systems or something like that. Most of the time, we discuss, so to say. We tell them: "we offer you a gratuity in compensation for the breakdown," and that's it.

MD: So it's case by case, or are there rules?

SG: It's case by case. It depends of the duration of the breakdown, it also depends of what data has been lost and the duration of data loss, since we have back-ups, you can always go back the previous day, but it's true that the last one we don't have. It has to be negotiated. Now, when we don't have it, we can't make it appear.

MD: Indeed.

SG: We do the best we can, but…

MD: Do you have several security levels in the services you offer?

SG: No… Not particularly… We try to offer maximum security to all clients. And then, we have two or three special clients who have more specific offers, because of special things, and… specific demands, too. In those cases, it's bigger projects and it's rarely… Well, it's not in the cloud offers or anything like that. And if we are asked, we provide more specific things that we manage ourselves with more advanced security.

MD: Does it happen a lot?

SG: No. It's for historical clients, identified, with whom we make business. No, we have, from time to time, demands where clients tell us "we would like back-ups for thirty days instead of only seven". We can do that as well, but it's more that kind of demands we have, about security.

MD: So it's not standard, but you do it if asked to.

SG: Yes, that's it. It's things like that, on duration, on things like that. We can do it, no problem. Then, if a client is really paranoiac, and wants to take care of security himself, he can take a non-managed offer, so that he can manage it from end to end.

MD: If your clients want to know who has access to their data, do you give them the names of the person who have access or not?

SG: They know there are teams here that have access, at any rate, and it stays inside. It can happen that we communicate, I think, on names or persons. They can see it on our website anyway, the teams and the composition with the names of the teams. They can easily know who has access to their data that way. We have a small production team.

MD: They can know without problem… Do you have subcontractors?

SG: No, except for the partnership, with this thing about building a website. But no subcontractors, no. We have softwares we pay for of course, with enterprises, antispams for example, antivirus… A bit like everybody, but no, we don't subcontract. All is one internally.

MD: And the data about clients, do they know where it is, physically?

SG: Ehh… I don't know if we tell them either. It's on our datacenters, on our machines.

MD: I believe that. Is it something that clients ask for, that data remains in Switzerland?

SG: Some, yes. Some are interested in the matter at any rate, they like to know, to be sure that all is in Switzerland.

MD: Do they tell you why?

SG: Some do, too. We have had a lot of questions recently concerning the last laws in France… Laws on ITs, and so we know that some clients came to us because of these laws.

MD: So it's because of laws, essentially.

SG: Yes, that's it. Then… Those who are interested in this and who want to be sure their data are not seen by the government, at any rate. But it's still laws in brackets… I don't know in what measure they are applied. It's more theoretical as long as no one asks for them to be applied. We can't check what happens in France, but we know that some clients feel more secure because in Switzerland some laws don't exist and they are not, potentially, subject to that here.

MD: Yes. You said earlier that you had legal demands from other countries, right?

SG: It happens, yes. We sometimes have demands for example for copyright images, coming from the US or somewhere else. Most of the time, we notify the client by telling them we have such a demand and then we manage, but it's not for us to delete the link, the content of something like that instead of our client, it's not our problem.

MD: Do you do random tests, to be sure data is where it's supposed to be?

SG: Yes. So we have a whole part of our monitoring in general, for our infrastructure, and in this monitoring part things that make sure that backups are done correctly, that data is still accessible and so on.

6. Technology aspects

MD: OK. So we can move to the next point. In the cloud services you offer, is it compatible with other records management, data management tools the client may have?

SG: Eh… No, because we only use this internally. Theoretically yes, but we don't give access to them to our clients. Our offer is really virtual machines, so if the clients do things like data analysis on them, we don't necessarily know what they do. The machine we manage ourselves, it's really websites and VMs.

MD: OK. And those machines you manage yourselves, in what measure do clients control the data? Can they control everything?

SG: When we manage ourselves? They put their data through FTP and they have access at any time to their data. Us, we take care of the display of the data, but yes, they have control on everything we do, we have the available backups visible. They can't modify them of course, but in case of need they can still see that those backups exist and are here. Then the rest, we keep a few logs we use to do their stats afterwards. They don't have access to the brute data, but they know they can see it because we generate their stats from that.

MD: And can they see it from any device? From a smartphone for example?

SG: Yeah, our admin interface, it's still better on a computer. For now, smartphone isn't quite… but we're working on it. Then yes, they can generate their website through our admin interface from wherever they want. And then, clients who have non managed servers have access to

the server console, so really like they had a screen in front of them, with what the server would say if it crashed, they can reboot the machine remotely, have their history.

MD: OK. And can they modify the metadata on their data?

SG: Well… In the limits that we generate the machines and all that. They can't modify them, because those are internal data. So, for metadata,we have to keep them for legal reasons, for example traces of logs, all that. They can't modify them either. There isn't anything much from metadata we keep. If the client wants to change the name of his product or the name of his site, in his admin he has access in any case. The rest, it's for internal things. So in terms of metadata we don't keep a lot either, because there aren't a lot of data that are interesting to us at this level.

MD: OK. Do you know the law about privacy and data protection, since it can influence the technical side and the architecture of what you offer?

SG: What do you mean? I didn't understand the question.

MD: You respect the law on data protection, of course.

SG: Yes

MD: Does it have an influence on the technical side?

SG: Yes, so we take care to… we have a small team which has access to the data and we take care, simply, to respect the client. We won't go and see his data if no one asked us to. Because there's no reason to. But we also have a certain number of websites, so that we don't have the time to see and investigate everything. If the clients asks us to look into his data to find, I don't know, a string of code that provokes something on his side and he doesn't know where it comes from, sometimes we will look for him. For example, if a pirate got into his code or part of his website, to see this file was put at that time on that day, it's malicious, do you want us to delete it or do something with it? We have an environment that protects us from that, it happens from time to time. If the clients ask it we can go see his data of course it's not systematic.

MD: OK. So… You have a multi-tenancy mode, with several clients on the same server.

SG: Yes.

MD: Do you offer an alternative? If people ask for it.

SG: As far as cloud offers go, no. We have several virtual machines on the same server and a server farm, it moves from server to available server when the client creates his machine at any rate. Then we have one client who asked to have his own project so that his machines could communicate with each other in his own environment, but we could, later, set dedicated machines so that clients could have a private cloud, but that's not for now. Now, since it's us who manage the interface and… how to say, manage Open Stack, there is no risk that clients step on each other's toes since they only have access through their admin interface. The number of actions is limited so that they can't go just anywhere even if the rights exist for that, but you never know.

MD: We already talked about what happens in case of problem… So, what do you tell your clients, do you tell them who else share the server with them?

SG: No, rarely, most of the time the client wants a virtual machine so we give him that much resources and we guarantee that much resources on the server. Now he doesn't necessarily know what machines are next to his on the same server. We don't do over commit. It means, if we are asked for… I mean, we have a machine with fifty physical processors on it, we rented fifty, not fifty-two!

MD: OK, so you're sure you can give.

SG: That way, we're guaranteed not to have performance problems where someone says, I paid for ten, but I feel like I have two, what's happening? In any case he has his disks and that's it.

MD: OK.

SG: It's more expensive for us but it's also why we're more expensive that our concurrents. It frees us from having to manage this side. That's not bad!

MD: So you always know who has access to which server, which clients are stocked where?

SG: We can find out quickly. In case of problem we know which client is affected. If a client asks us something about his machine, we know where it is. We have the tools for that.

MD: A critic that happens a lot on multi-tenancy is that it facilitates data mining on the data that's on the server. Are your clients worried about that?

SG: No.. So data mining are people testing links, or…

MD: For example, you could mine a lot of data on your clients easily.

SG: Ah, in that sense, no.

MD: They don't worry about it?

SG: No. We don't do it because we don't go watch what they do in the back anyway. When it's not managed you have to know that even the production team doesn't have access to the machines so we really can't know what they do. It happened once or twice that organisms alert us, watch out, something not kosher is happening on this machine, it's fishing or something like that. Then we have to react so we cut the machine entirely. We can't go and see on the machine what needs to be cut or not. We cut the network access of the machine. It's all we can do.

MD: You can't look at the details.

SG: No, you can't look at the details. When it's managed, the clients give us mandate to say "manage my website" do we can see what happens but on non managed cloud servers, no, no idea. And part of the data is here so when the client cancels, since it's given to another client, we make sure to wipe the data before reattributing the disk space to another client. So that a client who asks for a server will always have a shredded space and finds nothing there.

MD: What do you think of lock-in? You told us you used OpenStack which is more open source.

SG: Yes, absolutely. In all projects we use, even outside of the cloud, we try to do open source. It's a matter of philosophy. As much as we can, at any rate, there are some products where we can't, because they are not as good as conventional products but it's very rare. All that we can, we do in open source, yes.

MD: And how do you do so that clients can feel they have control over their data?

SG: It's mostly a matter of trust and then… they know they have access at any time, that they can delete or put new ones at any time.

MD: Do you communicate on this or do you let them discover it by themselves?

SG: No, they know that when they do something with us, we offer a certain number of services a bit beyond.

MD: OK.

SG: So their data… when they cancel the service, we remove the data and that's all… We don't keep it… and we don't use it for something else either. We have no advantage nor enough time to do it in any case.

MD: Do you have a way to assure them you don't modify the data? Are they worried about that?

SG: Same, it's a question of trust. They know that no one but Infomaniak has access to their data in any case. Then we have from time to time some clients who tell us, " this file has been modified on that day, it's not me!" In those cases we go and check. And here, every time we discover it's either one of his colleagues or a hacker that went into his site through a security flaw that modified such or such file. In most cases we can go back to the source and tell the client exactly what happened.

MD: And do you have data that is strictly confidential and that are encrypted?

SG: Yes, we have clients who [interference] then the client will chose an offer that will ensure the security of his data.

MD: You have different offers, then?

SG: If they want, typically something we don't have access to he chose a non managed cloud server, then he's sure, he can encrypt his file system if he wants to. We won't go and see what he does. And we don't have access in any case. Dedicated synologic offers that we don't manage, same, we have no way to go and check. It's his responsibility. Then we have a housing part where the clients can rent a rack to put their own gear, so that's even… they come physically in the data center with their server and plug it in, themselves, to they know that only they have access and put a code or something. It depends, we have clients that have the security level they want, they chose the offer according to that.

MD: OK. So it's a but modulable.

SG: Yes, that's it, we have offer that allow to make sure we can answer practically any demand.

7. Conclusion

MD: That's wonderful, we're close to the end. Just a few general questions. Do you see an evolution in the kind of clients who request cloud services, since you've been here?

SG: Yes, yes. There's a lot of people now who do cloud so we have more demands like, do you do such or such particular cloud thing… Sometimes we can't say yes so they go somewhere else. But it's true that there are a lot of clients who ask for new services or things we don't do yet. Cloud, now, allows to… how to say, we use it to make virtual machines and the clients then have to install their own applications in a non managed offer, for example, and there are other services who offer to have only a database, or to only have a database access to their thing knowing its redundant or things that are much more complicated, proxy, cache servers… We don't propose these kind of high level integration yet. We do it for clients we manage if they need a cache we install it for them. But we don't offer already formatted virtual machines so that the clients can directly have only database or things like that, not without managing it ourselves.

MD: That's things they ask for more and more?

SG: Sometimes, but it's more frequent these kind of demands to do "log js", modern stuff so to say, with a more container mode on cloud offers.

MD: OK. Are there any best practices you might recommend to someone who would do cloud today?

SG: It depends on what you want to offer as a service. As the word "cloud" says, we do a lot of things with it, it remains very technical in the background, a lot of technologies put end to end and we propose the virtual machine and clients will use the cloud to propose just file storage, services who will use the cloud to propose to developers to integrate their soft rapidly and so on. It depends on the final goal, of what you want to do with it. Now, we have had a few surprises in the beginning with stability troubles, you need to know what you want to do and what resources you need and to size the platform carefully. It's at that level. That's what we can say about it. It won't be magical because it's called cloud and because we have unlimited resources! You need to carefully size the base that wants to know the techniques and technologies underlying the cloud before you can offer cloud services yourself.

MD: Do you have anything to add, a point we haven't talked about yet?

SG: No, nothing special.

MD: If we have other questions later, can we send them to you by email?

SG: Yes, of course. Gladly.

MD: In that case, it's good for us, thank you very much for taking the time to answer to us!

SG: You're welcome, with pleasure!

Annex 4: Poster

RECORDS IN THE CLOUD - SWITZERLAND

CONTEXT

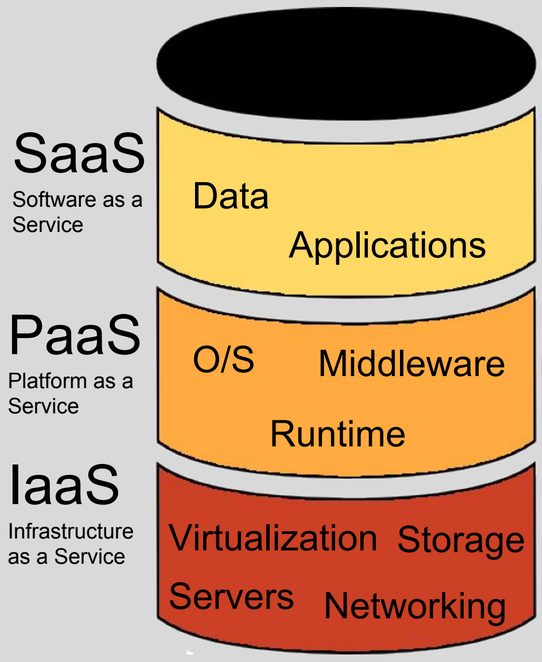
Records in the cloud is an InterPARES project. It's a 4-year collaboration between the University of British Columbia (UBC) and several European and North American universities, aiming to study management, operational, legal, technical issues on cloud computing, as well as clarifing policies and procedures in order for a provider to implement cloud services while understanding risks and benefits.

RiC Switzerland is a research project analysing 5 aspects of cloud computing in order to understand what it requires to implement "Records in the Cloud" in Switzerland. It is focused on the German and French parts of Switzerland which account for 85% of the Swiss population. The main purpose of this study is to suggest a set of good practices related to the use of cloud computing in the Swiss context.

Master IS: Department of Information Sciences, Geneva School of Business Administration. University of Applied Sciences Western Switzerland
M8 - Research project by:
Marion Destraz, Arina Grazhenskaya, Aurèle Nicolet, Lucie Petrelis
Supervised by Dr. **Basma Makhlouf Shabou**

WHAT IS THE CLOUD?

Levels of services*



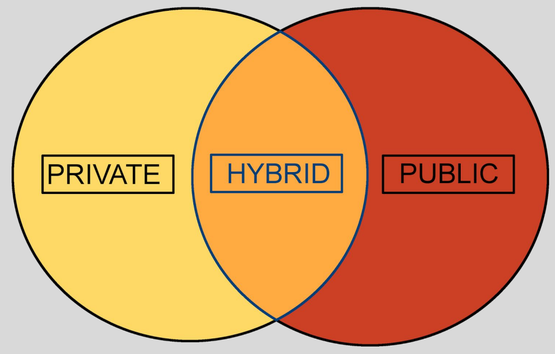
Google Drive

amazon web services™

IBM

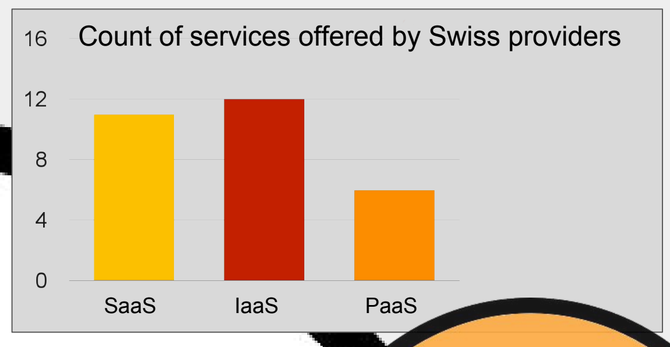
Main types of cloud models**

- **Public cloud:** Made for general public and owned by a third-party.
- **Private cloud:** Specially made for one organization, it is in principle more secure.
- **Hybrid cloud:** Combination of at least one public and one private cloud.



METHODOLOGY

State of the art → 21 cloud providers contacted → 6 providers interviewed → 5 aspects analyzed



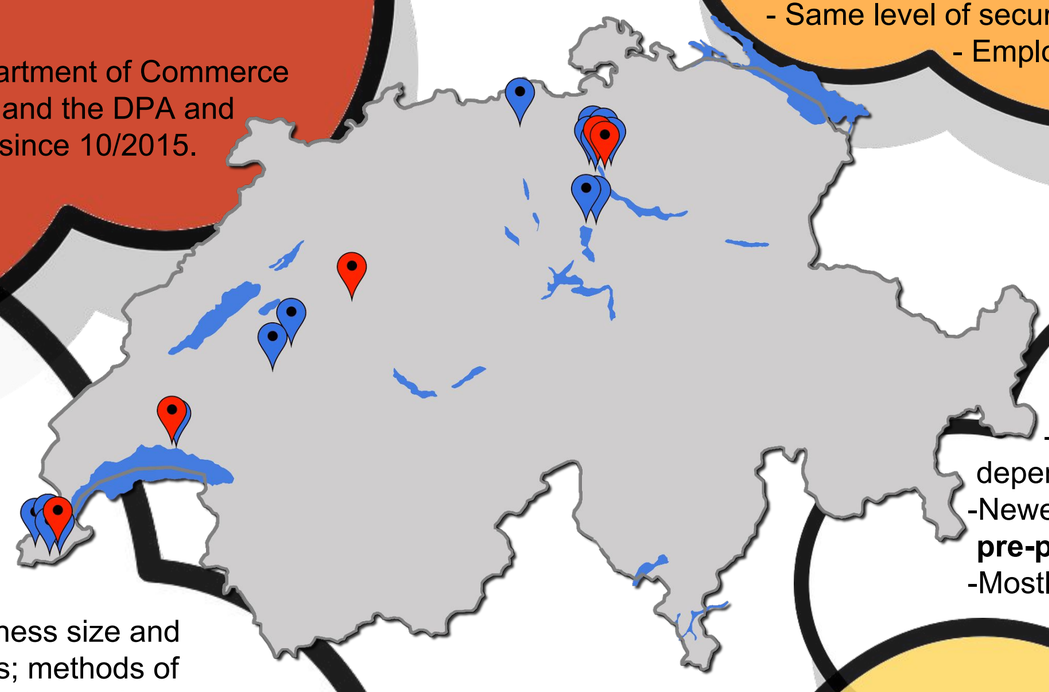
CLOUD COMPUTING IN SWITZERLAND: Main results

Concerned legislation

- **Swiss Federal Data Protection Act**
- **Swiss Federal Ordinance on Data Protection Certification** (DPCO): Guidelines on the minimum requirements for a data protection management system. Based on the DPA.
- **ISO/IEC 27001: 2013** formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks.
- **Cloud Security Alliance Certification**. CSA: world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.
- **Legal contracts** when no certification acquired.
- **International Safe Harbor Privacy Principles**: The US Department of Commerce developed privacy frameworks in conjunction with both the EU and the DPA and the Information Commissioner of Switzerland. Decision invalid since 10/2015.
- **EU legislation** not applicable in Switzerland.

Main security issues

- **Firewall** solutions.
- **Back-up** systems "so no data will ever be lost".
- **Disaster recovery** plans.
- Multiple **authentification levels** to prevent hacking.
- **Replications** of the data in other data centers.
- **Encryption** method available if the customers require it.
- **Insurance** policies and **compensations** in SLA contracts.
- **Automatic tests** and **data cloning** for control of data integrtity.
- Customers know exactly in which **data center in Switzerland** their data are hosted and who have access to it.
- Same level of security when having **subcontractors.**
- Employee **background checks.**



Managerial aspects

- **Hosting**: Datacenters are located exclusively in Switzerland.
- **Trial experience** is usually available.
- **Contracting:** Increasing demand for standardisation (SLAs)
- **Implementation:** Timeframes depend of the customer's business size and internal management cycle - from 30 seconds to 3-6-12 months; methods of **technical implementation** (big-bang - all at once or slow roll-out) are also selected by customers; only SaaS providers participate in deployment mechanism.
- **Information governance practices:** Cloud providers don't contribute yet. They are ready to provide support on customer's request,
- **Adoption** and staff training might be a part of the provided support or to be offered at the customer's request.
- **The cancellation and termination of subscriptions** are regulated by terms of conditions.The data may be transferred back with cloud provider's assistance.
- Most providers don't have a concrete recovery plan in case their business unexpectedly fold.
- Cloud computing services work independently of data retention schedule and lifecycle management.
- "There is no cooperation with archival institutions".

Economic situation

- The cloud has **advantageous pricing** compared to traditional IT, but the Swiss cloud is not the cheapest.
- From **pay by the hour** to **monthly plans**, depending on the service.
- Newest providers offer easier modes of payment, **pre-pay**, etc.
- Mostly **swiss customers**, but a good number of **international** ones, too.

Technological options

- **Open-source vs vendor lock-in:** "Open-source is the standard in the world of telecom and hosting"
- **Multi-tenant:** The multi-tenancy model is the preferred way, because "it is easy to update and to offer price benefits". Sometimes, the cloud provider can offer an alternative, but it is rare.
- **Encryption:** "Not all data are systematically encrypted due to performance reasons, only the most confidential ones".
- **Archiving and governance tools:** The providers haven't specially thought about the compatibility with archiving or governance tools in their cloud computing services. In most cases, it is because they provide IaaS.
- **Integrity and authenticity of data:** Often, the providers refer to ISO 27001 about confidentiality, integrity and avaibility of data. But they don't have particular considerations about authenticity of data.

Presentation date:
17th of December 2015

*LAU, Wely, 2011. A Comprehensive introduction to cloud computing. *simple talk* [online]. 16 December 2011. [consulted on 8 December 2015]. Available at: https://www.simple-talk.com/cloud/development/a-comprehensive-introduction-to-cloud-computing

**GOYAL, Sumit, 2014. Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review. *IJCNIS.* February 2014. Vol.6, No. 3, pp 20-29

Hes·so GENÈVE Haute Ecole Spécialisée de Suisse occidentale

InterPARES Project International Research on Permanent Authentic Records in Electronic Systems

Records in the Cloud

heg Haute école de gestion de Genève Geneva School of Business Administration