Project on Cybercrime
www.coe.int/cybercrime

Strasbourg, 5 March 2010
Draft

Discussion paper

Cloud computing and its implications on data protection

Prepared by
Research Centre on IT and Law (CRID)

Yves Poullet, Jean-Marc Van Gyseghem, Jacques Gérard,
Claire Gayrel and Jean-Philippe Moiny

Namur, Belgium

Project funded by Romania, Monaco, Estonia, Microsoft, McAfee and the Council of Europe

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Contents

1 Introduction

1. The Council of Europe requested the CRID to prepare a preliminary report identifying the main privacy issues related to cloud computing and the questions to be addressed in the future, in particular in the light of Council of Europe data protection standards.

As set by the contract, the work is to identify and underline the main cloud computing privacy issues. This first draft is definitively to be further elaborated and to be completed. It does not aim at giving answers which would have to be elaborated in the context of another mandate.

2. This report is structured as follows. It starts with a brief technical introduction illustrating the variety of services covered by the concept of "Cloud computing". As defined by NIST[1], "*cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*."

3. Cloud computing services include a large diversity of services going from those offered at the benefit of individuals as the services offered by social networks to those proposed at the benefit of companies in sharing a common software or by using shared information infrastructures. To establish a typology of cloud computing services is quite important since legal problems raised by each kind of computer *services* might be different to a certain extent. The second point is dedicated to the analysis of the adequacy of the CoE Convention 108 (referred hereinafter as ETS 108) definitions with the cloud computing reality. In particular, the status of the actors involved into the operations will be analyzed. Thereinafter, our report analyses the duties of the persons subscribing to the cloud computing services or offering these services. The crucial question of the security is then addressed. Finally, the report envisages the delicate questions of transborder data flows and international private law, which are inherent to most of the cloud computing services.

Obviously cloud computing raises several issues at many levels. Currently, cloud computing seems closer to fog than cloud and it might constitute a real danger for the users and data subjects whoever they are (legal entities, individuals).

1.1 Some technical aspects and specific risks linked with cloud computing services

1.1.1 The frame (or quick history)

4. "In the world of the computers, there are two classes of people". The first and main class is made of the users. All internet surfers are part of this class. The second class is made of the professionals of the computer world.

Users exploit applications with a lot of functionalities which help them in their work or in their other activities. They reasonably expect that their data be stored in protected spaces in order to retrieve these data when needed. That constitutes the standard way.

5. Since the beginning of the computers area and regularly, new concepts appear.

[1] P. Meil and T.Grance, The NIST Definition of Cloud Computing, Version 15, 10-07-09, available on NIST (National Institute of Standards and Technology) web site.

But some constants remain and it is useful to remember us these fundamental concepts.

In the sixties, the only way to do that was to use mainframes for the software. The data were stored on tapes, with no direct access for users.

Everything was "online". The users did not know where and which specific support their data were on. They only knew that the data were in one splendid and large room in one specific building. Everybody has already seen these ranks of tape machines on TV.

The data access was controlled by the operators of the mainframe. And no external access was possible.

Rapidly, an external access was created with a modem and controlled (for the rare persons that could try to it) by one simple password.

With the advent of the personal computer, everyone could have programs and data on his own computer. Users became responsible for the access control to their data.

Nowadays, with Internet, users can access the data owned by one computer everywhere in the world. Users become responsible for the physical protection of the data they get to others.

6. Thus, simple users can access data on "mainframes" located anywhere. They can also access the data they manage on their own system (that is to say their local network). Finally, they can access data stored in computers from where they have access when connecting themselves on Internet.

In these 3 cases, users can access to applications on the "mainframe", on their own computers or on other ones elsewhere on Internet.

In conclusion, four main components are needed in computing field:

- Hardware (processing, storage and memory)
- Operating system
- Applications
- Data

7. These objects of computer science can be used on a local computer (such as the user's personal computer) or on another one located anywhere else while users access to it by any means like Internet. The use of external Information systems might bring certain advantages since it implies the possibility for your computer or information systems to get rid of running programs or to support itself large communications facilities. Another benefit might be found in the fact that all the expenses and efforts concerning the maintenance, upgrades and security of the information system shared between the cloud computing services are supported financially by their different users and technically by the company offering the cloud computing services. Definitively it might be asserted that cloud computing services do represent for companies particularly small and medium-sized enterprises (SMEs) major scale economics. At that point it should be underlined that this kind of benefit might be also offered in the context of a GRID. The main difference between the GRID and the Cloud computing services lays down mainly in the difference of nature of the relationships between the users. GRID services concern users linked by a common professional interest and using the same information system (for instance, hospitals using the same datacenter or peculiar

software in order to diminish their expenses). In the case of Cloud computing services, it is not a question of sharing on equal footing the use of the same services on the basis of an individual agreement but rather the selling by certain specialized (or not) companies of certain remote services, that we could describe as a commodity which presents the following characteristics described by the NIST paper:

- *"On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.*

- *Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).*

- *Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.*

- *Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.*

- *Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service."*

This commodity can be offered through different deployment models. So, NIST paper already quoted distinguishes:

- "Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

- Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

- Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)."

1.1.2 Cloud computing

8. With cloud computing, the model implies that there is a simple computer that runs one browser. Although simple, this model is sufficient to work.

Users can use one application of the "cloud" and stock their data in one folder in the cloud. The most important question is the identification process of access to these data.

The three situations of infrastructure described above in the frame, are translated in the model of cloud computing by three models of development. The three platforms are the "software as a service", the "platform as a service" and the "infrastructure as a service".

The "software as a service" (SaaS) is easy to understand: users access to applications on the Web, for example, a text writer, a spreadsheet or more used one email software (see http://gmail.google.com). The services offered by Google are part of this kind of service. The data are also stored on their servers. Google is technically responsible for the application services and for the data of the users (secure conservation and secure access).

The "platform as a service" (PaaS) offers an operating system where users can install their own applications. However, the data are stored according to the "applications' decisions".[2]

The "infrastructure as a service" (IaaS) offers one "logical hardware" infrastructure. Users have to install one operating system; the applications they need and can finally decide where to store data[3].

At high level, these three services are carried out through two kinds of elements in the cloud: datacenters and clusters.

The datacenters are specialized hardware where data are stored. They generally provide security for access and recovery services.

The clusters offer the execution of programs with a high level of speed.

For simple cases, customers can use simple infrastructures. We can consider, for example, that virtual servers are also examples of IaaS. The virtual computer you installed can be moved from one location to one another when needed. The case of a Web server is current.

In this simple case, we can understand that the segmentation of the infrastructure must be serious, because, if not, one instance ca read or write in one other instance or virtual machine. Hacking or destruction is then possible.

More generally, in the 3 great kind of cloud computing, the same problem can appear.

In the case of the SaaS, only data are separate. Each user starts one instance of one unique application (text writer for example). The identification of the user is the only way to attribute data to the correct user. The system must be sure and secure at the level of identification.

---

[2] *See* https://www.dropbox.com/ for one simple example or http://msdn.microsoft.com/en-us/azure/default.aspx for one more complex example.

[3] *See* for example http://aws.amazon.com/ec2/.

In the two other cases, the problem is more complex, but the aspect of security must not be ignored or misestimate.

In conclusion, the technical problem of the cloud computing is only one kind of generalization of existing systems.

1.2 Specific risks linked with the cloud computing:

9. This section describes some risks related to or accentuated by the use cloud computing services which justify a possible intervention of the C. of E.: such as the opacity of their existence and their functioning, the constant mobility as regards the location of the processing operated throughout the world, the possible radical dependency of the subscriber towards the cloud computing services, etc.

The legal issues may be different whether we deal with services directed to individuals or services for companies or public administration.

10. So, as regards services to individuals like those linked with social networks or other large public available web 2.0 platforms, we have to pay attention to the following risks:

- The opportunity – for a third party or the cloud computing service provider itself – to **profile data subjects** by crossing several databases/information related to a person existing in the structure of the cloud computing itself. This risk is increasing when consumers will be invited to use gratuitously cloud computing services if they accept to receive one to one targeted advertising. It is quite clear that they will be happy to sell their privacy in exchange of this gratuitousness.

- The concept of **consent**: Beyond the risk already mentioned it might be considered that information circulating in a cloud computing system may be linked to people who are not aware about that.

- The problem of "**ownership**": Consumers once they have released their data in the cloud might have difficulties not only to maintain the access to these data (we might think for instance to a sort of denial of access in case of non-payment of the service) but more fundamentally to recover their full control of the data released when they terminate their contractual relationship with the cloud computing service provider. According to the general terms of the service, the provider could contractually keep the option open to keep the data at stake even after such a termination (e.g. social networking sites).

- The lot of the data **after death**. When the subscriber of a service dies while his or her data are circulating/stocked in a cloud computing system, certain questions have to be solved: Who is empowered to get access to these data? The heirs of the *de cujus*? The cloud computing provider?

11. As regards now the case of a *company as subscriber* of cloud computing services, additional questions might raise:

- The obvious need to distinguish clearly the concepts of **user, subscriber and data subject,** which each of them refers to clearly different people involved into Cloud computing services and subject to different problems. So, the employee who is using the information system provided by his or her company might not be

aware of the recourse made by his or employer, the subscriber, to cloud computing services. As regards the data located within the datacenters provided by the cloud computing services, some are relating to customers, furnishers and so one who are not necessarily aware of this fact. So to what extent can we consider that these persons must be aware of the use of cloud computing services and is this recourse subject to possibilities of refusal or even of acceptance? Other specific questions relate to the distinction between users (employees) and subscribers (employers). In case of death of an employee, who will have access to the data stored in the datacenter? The death of the user. This is linked with what we saw above. May the cloud computing provider erase the identifier and password of the user? Is he empowered to do so? In the negative, who has the authority to do so? Beyond that question, is that conceivable, to the benefit of the employees using the companies' information system, to make a difference between private and professional, excluding the former from the use of cloud computing services?

- The **protection of legal persons** and their know-how, industrial secrets, etc. On that point, we envisage two different problems. Firstly, the company might locate on the cloud servers trade secrets concerning itself or third parties which might be compromised by lack of security of the cloud computing service. Secondly, the cloud provider might record certain transactional data generated by the use of the services offered, which will reveal substantive activities of the company. For instance, the storage and analysis of communication of financial data between the subscribing company and a bank might reveal risks of bankruptcy. We will comeback to these issues (infra n° 12).

- The **exclusion or subjection to strict conditions of the use of cloud computing services for some types of data or activities** (like the activities submitted to a professional secrecy). Certain legislations (see the US HIPPA[4] on Health data) regulate the disclosure of data to third parties. Insofar as the cloud provider might be considered a third party, he will be submitted to such regulations. In some cases, it could be deemed, due to the sensitive nature of the data and the risks inherent to Cloud computing services, that the processing of these data is incompatible with the concept of cloud computing which involves the dispersion of data and to a certain extent the loss of control by the data controller on the data stored within the clouds. Therefore, should the use of cloud computing services be banned in some circumstances or for some matters? Indeed, one can consider that some matters as health, Justice, administration are so sensitive that they cannot be reconcilable with the use of cloud computing which could imply the spreading of information on the Internet with a major risk of disclosure.

- For the same reasons, should the use of cloud computing be forbidden or subject to certain restrictions when specific processing of data by **public administration or authorities** are concerned, since the sovereignty could exclude the transfer of data to countries where risks of attempts to the confidentiality or more broadly to the security of data might jeopardize the State's sovereignty? The use of hybrid clouds operating only within the national borders might be imposed as a solution.

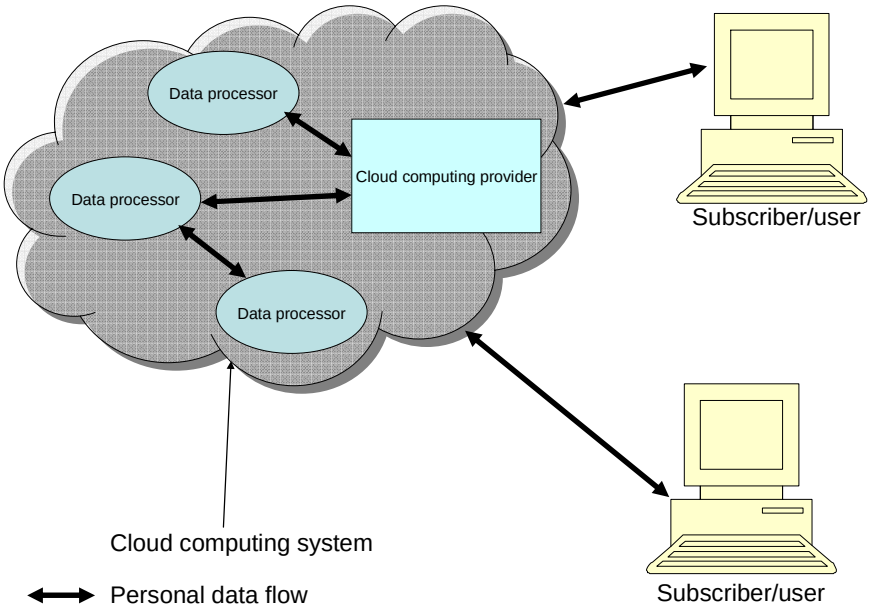
[4] Health Insurance Portability and Accountability Act. About that example and others, *see* B. Gellman, Privacy in the clouds: Risks to Privacy and confidentiality from Cloud Computing, Report prepared for the World Privacy Forum, Feb. 23, 2009.

2 Personal data flows within any cloud computing system

12. Different personal data flows can be identified within any cloud computing system which involves several actors.

We can identify four major ones as data controller, data processor, subscriber, user and data subject.

The cloud computing pattern can quickly be drawn as:



3 Thoughts about actors

13. ETS 108 provides basic and useful definitions for the processing of personal data. However, this list shall be completed taking into account the peculiarities of cloud computing.

Providing additional definitions should clarify the understanding of the functions and duties of all the actors intervening in the Cloud computing system.

Therefore, any text dealing with Cloud computing seems to refer to certain concepts known or unknown by the existing Convention 108:

- **Cloud computing provider**: The natural or legal person providing a service (SaaS, PaaS and IaaS) in a Cloud computing pattern.

- **Subscriber**: The natural or legal person contracting with the Cloud computing provider. The function and duties of this actor will be explained below. It might be an individual (see social networks), a company or a public administration

- **User**: The natural or legal person actually using, in the context of their tasks, the services of the Cloud computing system. It can be the same person than the subscriber, as it cannot be. In the latter case, an employee working in a company could be involved. He would be the user while the company would be the subscriber to the service (SaaS, PaaS and IaaS). Definitively the users might be data subjects of the processing operated by the subscriber or by the cloud computing provider. ? Should the cloud computing service provider be subjected to specific obligations in favor of the user – only acting as a user? And which would be such obligations (e.g. information)?

- **Data subject**: If ETS 108 already deals with the concept of "data subject", it doesn't give any complete definition. It appears important to define precisely this main actor in the personal data processing, whether in a Cloud computing system or not.

- **Data processor**: The distinction between data controller and data processor is at first glance quite clear according to the definition given by Directive 95/46/EC but this actor is not defined in the ETS 108. The Data controller processes the data for his own purpose and defines the means to achieve his purpose; the data processor operates data exclusively at the request of the data controller and does not pursue any own purpose. In the context of cloud computing, the provider might be considered in certain cases as a data controller and in other cases as a data processor. The qualification might be in other cases quite difficult « since the cloud computing service provider could define means that, due to the characteristics of the service at stake, would justify some processing operations not directly requested by the subscriber – as the case may be, data controller ». As an example, the provider of an IaaS, caring about the efficiency of its service, could automatically allocate processing and stocking capabilities between various facilities located worldwide. For instance, at a time "t", the most efficient could be to use a data center and processing capabilities located in Germany. But, due to the increasingly use of these facilities at a time "t+1", it could be more effective to have recourse to facilities located elsewhere in the world, for instance in India, in providing the service – which could involve a duplication of data, etc. In this respect, the technology at stake would automatically imply a transborder data flow the controller of whose is not necessarily easy to determine. From another

point of view, in a lot of cases, the cloud computing service provider might take advantage of storage or processing capacities offered by third parties, who could be considered as data processors of data processors.

If we introduce the distinction between data controller and data processor in the context of a C. of E. regulatory text it would be absolutely needed to specify the "legal" regime of this new actor and the specific duties, firstly, of the data controller who has recourse to a data processor (obligation to have a written contract specifying the tasks given to the data processor, requirement as regards the quality of the data processor, etc) and, secondly, of the data processor (prohibition of personal use of the data processed in the context of the tasks operated on behalf of the data controller, etc).

4 Legal issues dealing with domestic use / non domestic use

14. The cloud computing is currently serving the domestic and personal framework (social networking sites, webmail, online diaries, etc) as well as professional environments (legal bodies decentralizing their IT network to reduce costs, etc).

Knowing that European Union has, voluntarily, limited the scope of Directive 95/46 to the non domestic processing of personal data, is this limitation relevant in the context of cloud computing? This exception is particularly relevant in the context of some Cloud computing services (social networking sites, etc). But a practical interpretation thereof have to be found which would not deprive data subjects of their rights enshrined in data protection legislations, and would not suffocate other individuals by heavy rules. As the case may be and depending on the Cloud computing service at stake, it is necessary to think about the opportunity of establishing a softer – or not - data protection regime in spite of a wide application of an exemption to the scope of the legislation.

This distinction might have harmful consequences for individuals as far as transborder data flows are concerned. Indeed and in some national laws, the rules dealing with such situations are applicable only to the non domestic use. This means that the data subject concerned by a non domestic process enjoys more protection than the others who could lack some protection in the context of cloud computing services. How does it to be taken into account? In brief, is this distinction desirable in a cloud computing environment?

5 Legal issues dealing with the protection of legal persons

15. Another issue rose by the cloud computing relates to the concept of personal data. Do we have to confine this concept to the definition given by the ETS 108 which says that personal data *"means any information relating to an identified or identifiable individual ("data subject")"?*[5]

In the context of, if need be, a specific regulation targeting cloud computing, wouldn't it be relevant to extend the concept of personal data to any information relating to an identified or identifiable legal person? In the surroundings of cloud computing, does the concept of personal data have to be extended – and how – to information such as industrial secrets, know-how, etc (see above)?

Most countries do not extend data protection scope to legal persons. The cloud computing system may change this conception because it will be used by the legal persons as a way to reduce their IT costs. And, depending on the relevant market, they could be deprived of any bargaining power (e.g. SMEs and non-profit organizations). This would compel them to contract under unfavorable conditions to stay competitive, having thereof less regards for data protection and privacy.

For the record, the Strasbourg Court has always asserted that article 8 ECHR protects not only the individuals but also legal persons notably their industrial secrets, know-how, etc. Obviously, they want to keep them safe from any disclosure to third party without any prior authorization. The concern is to determine to what extent a protection should be provided for by the law to legal persons since the use of cloud computing by companies or other legal persons create such a technical and economic dependence for these companies in regard to the Cloud computing service. The imbalance of information powers between individuals and companies or administrations created by ICT use has been at the basis of data protection legislations. Perhaps it might be meaningful to extend data protection principles to the protection of legal persons when it is clear that the same imbalance exists, and, improving in so doing the protection of the individual concerned by legal person's files or databases. Furthermore it should be noticed that certain countries, members of the Council of Europe, have already extended their data protection legislations to legal persons (see notably partly Italy, Luxemburg, Norway).

Therefore, such consideration coming from companies who may be a major user of the cloud computing system, mainly on a B to B basis, has to be taken into account.

Using such system, companies will stock confidential information (as the know-how, industrial secrets, etc) on apart servers or they will use cloud computing for internal communication (email, VOIP, etc). Therefore, they expect a reasonable protection of such information. In case of lack of protection, they could be reluctant to use cloud computing systems.

16. A better protection of the data related to legal persons may be necessary due the concept itself of the cloud computing. Indeed, meta-processing are possible with such system because the cloud computing provider may access to information of various legal persons. With such crossed data, he may offer service of added value as risk analysis on companies, etc to third parties. Such attitude may constitute a major risk of disclosure of confidential information to third parties.

[5] Article 2a.

17. Taking these concerns into account, we need to determine if the concepts of personal data and data subject have to be extended to legal persons as regards cloud computing. Arguments might be drawn down from previous extension to legal persons as it has been the case under the EU e-Privacy Directive and under certain legislations of member states of the Council of Europe (Italy, Norway, Luxemburg, etc).

6 Legal issues dealing with the actors within any cloud computing system and their functions

18. Primary issues relate to the concepts of data controller and data processor. As has been seen before, the cloud computing system will involve both of them.

The main question is to define who is who and who does what.

For the record, the data controller is the natural or legal person who decides the purpose and the means of the processing. It is the cornerstone of the data processing. It has the responsibility of the main duties (information, security, etc). The determination of the data controller will have a huge impact on the legal structure of the cloud computing system.

In the determination of such data controller, we have to take into account the extraterritorial characteristic of actors and its consequences.

Indeed, main of the cloud computing actors are set up out of the territory covered by Council of Europe's competence. Consequently, the control of their use and policy can be difficult for both the authorities and the subscribers as well as for the data subjects.

So, it should be easier for the authorities to control the respect of the duties and to punish the possible lack of respect of them if the actor is set up on the European territory.

We may view the Cloud computing service provider as a data processor instead of a data controller. It should act on behalf of the user (or subscriber) who processes personal data. But sometimes, the Cloud computing service provider pursues its own purposes for the processing of personal data. And as far as these processing operations are concerned, it is a data controller. Two issues result from this assessment. First, when a Cloud computing service provider is data controller and data processor as regards a same user (or subscriber) could it be deemed appropriate and/or necessary to extend its quality of data controller for the whole processing operations? Secondly, if it is only a data processor, is it appropriate and/or necessary to establish, as the case may be, some specific duties (security, information, etc) and/or a specific rule of responsibility (e.g. as what exists as regards the responsibility of the intermediaries at the sense of the e-commerce Directive of June 8 2000) falling to the data processor?

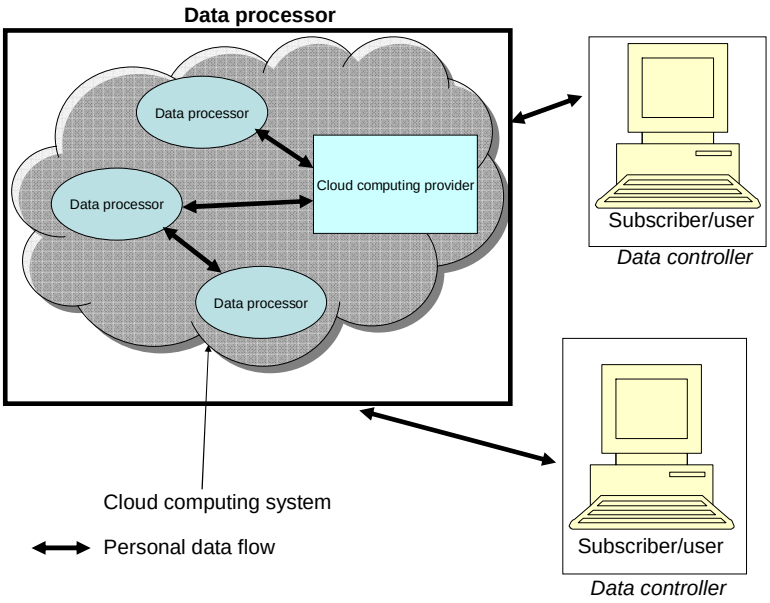
19. Therefore, it appears preferable that data controllers be under Council of Europe member states' jurisdiction. The question is also related to the right of protection of the users and data subjects. If the main actor is outside the scope of European's competence, how can the data subject or the subscriber or even the authorities control and sue him in case of lack of respect of its duties?

Consequently, from the data protection point of view:

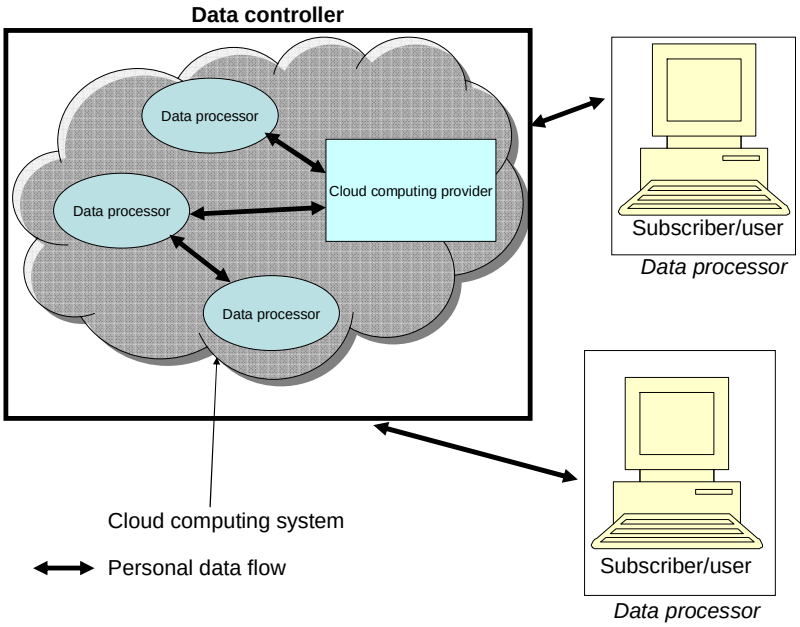
- Is the cloud computing provider data processor acting on behalf of the subscriber (data controller)?

-
- Is the subscriber a data processor towards the data controller (mainly outside Europe)?

We draw the system as follows:



or



Is that possible for subscribers to require by contract with the cloud computing service that the data generated or operated by the cloud computing services will be located in the territories of the Member states and to forbid any onward transfers…? What about the possibility for users to take benefit of this provision? A third party beneficiary provision ought to be included in cloud computing standard contract.

It has to be pointed out that in practice, both models could, in some extent and in a same relationship between the cloud computing service provider and its subscriber, overlap. Depending on the processing at stake, the provider could be data controller

and data processor at once with regard to the *same data* or to the *same data subjects*. In this respect, it has to be determined if the subscriber – following a basic view, that is to say the data controller – could be a *co-controller* as regards these processing the controller of which is the provider – following the same basic view, that is to say the data processor. To this end, raises the following fundamental question: what is the definition of the concept of "co-controllers" and does it have to be adapted in the context of the cloud computing? This is of course crucial due to the aforementioned scattered location of the actors of the cloud.

The following simple examples can illustrate the pertinence of the purpose. An employer decides to have recourse to encoding software offered by the cloud (SaaS) and designed to encode invoices from employees who seek refund for fees supported by them. The SaaS provider could offer its subscriber (employer) an additional – of course not free – service to monitor the expenses realized by his employees. The service could consist of the sending of monthly reports detailing in descending order the total amounts of expenses per employee. In such a case, could – and should – the purpose of the processing – monitoring of employees in a specific field –, being a complementary service, be deemed to be defined by the subscriber *and* the provider at once? Another example comes from the social networking sites context. The provider of such a network could offer a personalized advertisement service consisting of a SaaS enabling a company to choose a specific audience to deliver advertisements, without such company processing any personal data, the provider of the SaaS holding alone this task. Could – and should – the company ordering the advertising campaign be deemed to be a co-controller of the processing at stake? In both cases, the providers of SaaS define means for the processing of personal data and suggest to subscribers a purpose they assigned to the means they created, purpose the subscriber chooses to appropriate, bearing processing of personal data. Is it opportune to define – or redefine – a "co-responsibility" of the actors in such cases, and how could and should it be done?

7 Legal issues dealing with the duties of the actors

20. **Transparency** towards the users and data subjects should be a fundamental objective of any cloud computing system. This objective involves the obligations of information definitively with regards to the users but also perhaps with regards more generally all the data subjects.

Subscribers resorting to a cloud computing services should be under strict obligations of information to final users, when users are different from the subscriber (for instance in case of the relationships between an employer and an employee). It is not obvious that the consent of the users has to be obtained by the subscriber but definitively it seems that they have to be informed. When a person is giving his or her data to a data controller using cloud computing services as data processor, is the information about the recourse to this data processor needed, considering the specific risks linked with the activities of this data processor? I do not want necessarily to send my data or information on me to a third party which is not the direct contractor, especially if I have no certainty about the final place of the processing.

21. This **obligation of information** is directly linked to the article 5a which sets that the *"personal data undergoing automatic processing shall be obtained and processed fairly and lawfully"*. The term "fairly" involves this concept of information. As the cloud computing involves necessarily data processors, the several users or subcontractors should be informed about this situation. Otherwise, the processing will be unfair because of the lack of information towards people using the system.

22. Therefore, should article 5a terms be reviewed in order to fit the specific transparency issues raised in any cloud computing system? But, how far the data subject has to be informed of the particular technology at stake and its technical implications, such as the relocation of the storage of information in another State, the chain of sub-processors, and, as the case may be, its legal implications such as the occurring of processing operations in a non Contracting States where even adequate – but different – data protection rules merits mention?

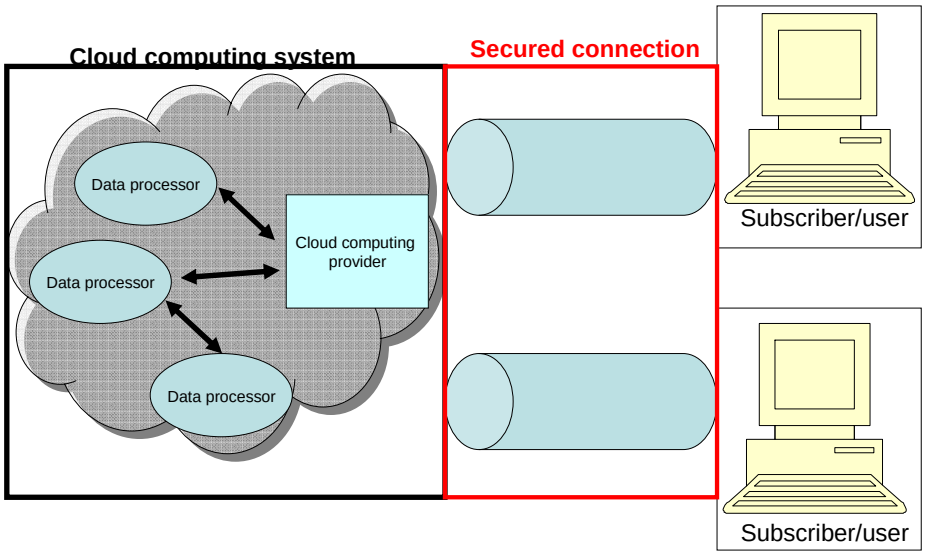
Who has this duty? Cloud computing provider or subscriber? The determination of the function of each actor will be decisive.

8 Legal issues dealing with security

8.1 Introduction

23. First of all, we have to make a distinction between two levels of security. The first one will deal with the connection between the user and the cloud computing provider and the second one will be the cloud computing system itself.

It can be drawn as this:



By making this distinction, we consider the data computing system as a kind of safety deposit box which can be accessible only by authorized person. On the other side, the access to this safety deposit box must be secured to avoid any access to the transferred data by unauthorized persons.

But, there is a damper to this. Indeed, we have to take into account that too much security kills performance. That means that we'll have to do the balance between absolute security and performance of the system.

24. The article 7 imposes "**appropriate security measures**". It does not define who has to support this that obligation. It might be the data controller, the data processor or even the sub processor (provided that these two last actors are not defined by the ETS 108). The concept of 'security' is quite broad, even if not defined precisely

by the article 7 of the Convention 108. It means under article 17(1) of the Data Protection Directive protection 'against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing'. So, for example, the risk of wiretapping by unauthorized third parties during the use of the services requires appropriate safeguards like the use of cryptography or secured lines (e.g. in case of electronic transmission of the credit card number). The possibility of intrusion within the provider's information system in order to collect all its customers' addresses or to manipulate certain data imposes the necessity to install firewalls and other security measures. The sending of worms through the information systems of a communications service provider or the creation of a mirror site in order to lead astray certain communication are other specific risks linked with the use of communications services. The obligation is not limited to technical measures but encompasses also organizational measures which might be the nomination of a data security manager competent to ensure the compliance of the functioning of the service with all Data protection requirements.

25. Security is essential in case of cloud computing services since it is quite clear that by trusting a cloud computing service, the subscriber aims at being protected against all risks linked not only with confidentiality (disclosure or intrusion) but also with integrity and availability of the data stored somewhere in the cloud. In other words, since the cloud computing service provider is offering services founded on the security in the broadest sense, it seems meaningful to impose them additional obligations as regards this obligation to security and more particularly in case of what is called: "security breach".

8.2 Specific obligations of security.

26. Regarding security and integrity of cloud computing services, according to the peculiar risks raised by such services due to the concentration of applications and or data used by different users and subscribers and the huge possibility for unauthorized people of aggregating all these data, it might be wise to impose new obligations to their providers. Amongst these appropriate security measures, three ones could be taken into consideration: The first one addresses the problem of unauthorized access by the provider's employees: providers of cloud computing services could be subject to an obligation to develop measures like systems of identity management in order to fix and control effectively the respective privilege afforded to each member of personnel regarding the access to personal data conveyed, stored or operated by the communications services. The second one would target the needed protection of these data against any loss, destruction or illegal access or storage. It refers to various technological security measures so the encryption of transmitted data, the adoption of automated control systems about the quality and integrity of stored or transmitted data, the setting up of log-in and log-out registries, etc. The last security measures would concern the adoption by the provider to express in clear language his security policy. This obligation participates to an increasing accountability of the data controllers by compelling them to envisage the risks associated with the services they provide, to define exactly how they manage these risks and by making them responsible in case of non respect of their commitments. Furthermore it might be envisaged that the cloud computing services' provider would be required to cooperate with the competent data protection authority(ies) in case they would like to audit the security measures promised or implemented by the providers. In the same line, the possibility for these authorities or standardization authorities to issue recommendations on best security practices ought to be assessed.

27. Some other organizational measures may be adopted in the context of the cloud computing matter as:

- Obligation to audit the system to put the risks and the lack of securities or confidentiality in an obvious place;

- Obligation to segregate the data stored by each subscriber in order to avoid any accidental or unlawful access to these data by another subscriber;

- Obligation to have a person responsible for the security who will be in charge to warrant the security of the cloud computing system for the provider;

- Standardization/normalization of the sector to give to the user/subscriber a kind of security in its choice. This standardization/normalization goes hand in hand with the delivery of quality-labels available for cloud computing providers who insure the respect of several conditions/obligations of quality.

28. The **bankruptcy or transfer of the cloud computing activities** might cause certain problems. The cloud provider's bankruptcy might lead to the sale of the cloud computing services to a company exercising competing activities with the subscriber's ones or having another privacy policy. The bankruptcy might in other cases lead to the termination of the activities. Anyway, the subscriber must be aware of the consequences of the disappearance or transfer of the cloud computing services on the data which are stored or put into circulation by it. So different questions would have to be analyzed. Do we have to provide the continuity of the contract with its confidentiality or security guarantees, etc? Is that possible for the subscriber to unilaterally terminate the agreement for privacy or competition reasons and, if it is the case, to be sure to get back his or her data?

Cloud computing business model and architecture calls for a deeper examination of the relevance of non regulatory instruments. Indeed, cloud computing companies are mostly international and implemented in a great number of countries. Advantages and disadvantages of self-regulatory instruments, such as the European Union model of Binding Corporate Rules, whether as an alternative or complement to the existing legal framework, need to be assessed. Due to the globalized nature of cloud computing companies, we strongly believe that European Union's experience with BCR could provide an interesting framework and point of departure for future debates.

8.3 Obligations in case of "security breach"

29. The **concept of security breach** is unknown by the C. of E. regulatory text but has been introduced recently in European Union by the Amending Directive on e-privacy. This Directive defines "personal data breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community. The main idea is to put on the shoulders of certain communication services providers' new obligations provided that specific risks are linked with the nature of their services.

As regards, European Union Directive, the targeted services are limited to publicly available electronic communication services even if it has been recognized that in the future the concept must be extended to other services due to the risks existing in other services like banking on line services or electronic healthcare online services. Clearly the

debate around the revision has asserted the need to re-open the debate about this limited scope and to follow the US example (see at the Federal level, the "Data Accountability and Trust Act", by extending certain obligations to any person engaged in interstate trade and who own or possesses electronic personal data shall notify a breach to individuals, if the breach leads to an unauthorized third person acquiring the data, and also to the Federal Trade Commission. So the first question is: "To what extent the specific nature of the risks linked with cloud computing services might justify the extension to these services?". Perhaps the U.S. extension or the extension to all Cloud computing services is too broad since they will conduct to minimize the obligations to impose but considering the nature of the risks offered by cloud computing services acting or not as data controller and offering not a specific services like a service assisting people in order to fix meetings (like Doodle) but services including more sensitive processing, what remains to be defined. The main criterion must be the importance of risks incurred by the subscriber of the service but more generally by the concerned people.

30. The second question, having solved positively the first one, envisages the different obligations linked with the "Security Breach" regime. It consists of two kinds of additional obligations:

- First all the legislation imposes a duty to inform through appropriate means the data subject, what might in case of cloud computing services go far beyond both the subscriber or the users and implies in cases of cloud computing offering purely technical or software facilities without having an access to the data themselves a partition of the tasks between the service provider and the subscriber and that in order to afford them an opportunity to take the needed measures to avoiding or reducing the risk. As regards the list of the beneficiaries of this obligation, can we consider, on the basis of the previous remarks, that in certain cases this obligation to notify must be extended at the benefit not only of individuals but also of legal persons?

- Second point, do we impose an obligation to alert at the same time the data protection authority? But in case of positive answer: which one (due to the global character of the provider)? Which information must be given? and through which channel?

- Finally we pinpoint the idea for standardization authorities of establishing in close connection with these independent agencies technical and security means.

9 Legal issues dealing with liability

31. As we deal with several actors working together, we necessarily have to raise the issue related to the liability of each one.

It goes hand to hand with the function of each of them in the system. If the ETS 108 gives duties to the data controller (controller of the file), there is nothing concerning the data processor for the simple reason that it is not considered by the Convention[6]. As has been seen before, the data processor is one of the main actors in a cloud computing system and it might be useful – and this has to be assessed – to impose on such data processors – or, as the case may be, on *some* data processors – specific duties by "law" instead of contract. Such specific duties could consist of security obligations, information obligations, a specific liability (e.g. as what exists as regards the responsibility of the intermediaries at the sense of the e-commerce Directive 200/31/EC). As stated above, a particular liability could be established as regards co-controllers. But it also have to be further assessed. Each time it is considered opportune to create new duties, the question of liability has of course to be studied.

32. The liability will be at several levels. The cloud computing provider (as data controller) will have to ensure a total security of its infrastructure and of the transmission of data from the users to its service. This duty of security should *also* be in charge of its own data processor(s) (subcontractor(s)). In this last case too, the duty can be enforced by law or by contract. The advantage of the law is to be compulsory and to give no autonomy to the parties and, therefore, to protect more efficiently the users. Indeed, it avoids the possible lack of balance of power between the parties (see above) to the detriment of the users.

10 Legal issues dealing with transborder data flows

33. Due to its highly virtualized architecture, cloud computing services involve great amount of data transfers, among which personal data as defined in the ETS 108, and by thus raise the issue of the applicability of the transborder data flows regime defined in the Additional Protocol 181. First, these transfers may occur between several actors: personal data may be transferred within the cloud provider's proprietary cloud, which can cover several countries; transfers may occur between cloud providers; transfers also occur between the cloud subscriber and his cloud provider, when he benefits from the cloud computing services wherever his location, such as when accessing, consulting or downloading personal data. Second, these transfers between actors may pursue different purposes: some transfers might be justified for purposes of transit or technical maintenance, while others are directly justified by the necessity to provide the cloud computing services requested by the user.

All these transfers may involve transborder data flows, since the cloud providers may resort to processing materials located in several countries to offer its services to subscribers/users soliciting cloud services from anyplace. Circulation of information, and as far as we are concerned, of personal data within and outside the cloud may occur in non State Parties to the ETS 108, among which most do not provide adequate level of protection. This state of fact raises the following issue.

[6] However, we can take the concept of data processor out of the article 7.

10.1 Applicability of the existing legal framework of additional protocol 181

34. The applicability of the existing legal framework to cloud computing technology requires deeper attention and assessment. Article 2 of additional protocol 181 basically prohibits international transfers of personal data toward states not party to the ETS 108 that would not ensure **adequate level of protection**. Any actor involved in cloud computing services, whether user, subscriber or cloud provider, should be fully aware of this prohibition and the legal risks associated with international transfers that would not satisfy to the TBDF regime.

35. Derogations to this general prohibition as provided in additional protocol 181 need further examination. As provided in article 2 a), national laws may allow transfers of personal data toward non-adequate destinations in case of "*specific interests of the data subject*" or when legitimate interests, especially important public interests prevail. Rightly applied, these exemptions could constitute a basis for several international transfers in the cloud computing context. As a first instance, the data subject's consent to the transfers at stake could be solicited. As a second instance, international transfers could be justified by the necessity of the performance of the contract concluded in the interest of the data subject between the cloud provider and the cloud subscriber/controller. Public authorities resorting to cloud computing services in the framework of their tasks could justify international transfers in the name of legitimate important interests.

As far as the second set of exemptions is concerned, article 2, b) offers possibilities of international transfers "if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law." Appropriate contractual clauses might constitute a relevant framework to ensure the legality of international transfers. However, such framework needs further assessment about its relevance in the cloud computing context, due to the necessity to take fully into account that the flows generated by the Cloud computing services often are concerning a lot of countries and a lot of companies as previously asserted. Perhaps the use of '**Binding Corporate rules**' adopted by large multinational companies offering cloud computing services can be at least a partial solution.

36. In general, the applicability of these two sets of derogations to the cloud computing context needs further assessment from the point of view of the level of data protection aimed at by the Council of Europe. In the context of unbalanced relationship between a cloud provider and its subscribers that could either be individuals or legal persons of little/medium influence, raising the data subject's consent or the necessity to perform a contract concluded between the cloud provider and the customer as primaries legitimate legal basis for international transfers could reveal wholly unsatisfactory.

10.2 International transfers of personal data/storage of personal data and law enforcement objectives

37. One of the most obvious and serious risks for data protection raised in the context of cloud computing architecture is a massive access by law enforcement authorities to the personal data and information stored in datacenters. Indeed, these datacenters can be established in countries that provide little or no protection of personal data in the framework of law enforcement activities. The development of datacenters might provide great opportunities to public authorities to access to great

amount of information pertaining to its citizens or to foreign citizens[7]. Even considering democratic countries, the United States of America constitute a problematic example due to the very controversy third party data issue in the limited scope of the Fourth Amendment protection.

10.3 Limitations to transborder flows and Applicable law

38. As stated above, cloud computing technologies involve countless transborder data flows implicating Parties to the ETS 108 and its additional protocol, as much as foreign States. A first set of rules is provided for in article 12 of the ETS 108 in consideration of transborder data flows between Parties to this Convention – only indirectly taking into account transborder data flows intended for non contracting States (article 12.3, b)) –, and a second one, provided for in article 2 of the additional protocol, directly addresses the issue of transborder data flows intended towards non contracting States.

39. The aforementioned sets of rules are targeted to the specific aim of reconciling guarantying effective data protection and fundamental rights and liberties – even outside national borders – on the one hand, and on the other hand, ensuring the free international circulation of information between people, as the case may be, avoiding forms of protectionism. In this respect, transborder data flows between Contracting States should not be subject to any *special controls;* the sole purpose of the protection of privacy cannot justify the *prohibition* or the submission to a *special authorization* of these flows of personal data. Therefore, the ETS 108 prohibits what we would call an "administrative control" on data flows. However, under article 12.3, a), a Party can disregard this rule if it has a specific legislation for certain categories of personal data or of *automated personal data files*, because of the nature of those data or those files, except where the legislation of the other Party provide an equivalent protection. So, as the case may be, a first question arises: could – and should be, for instance due to the characteristics of the service at stake – cloud computing technologies be deemed to constitute such a category of « automated personal *data file* » (e.g. health care online services) ? In other words, in the context of cloud computing services, the maneuver let by the ETS 108 to the contracting States to adopt a particular regulation as regards specific cloud computing services (e.g. concerning sensitive data) has to be assessed. As stated above, cloud computing recovers various realities and it could require specific rules and particular treatment in some cases and not in others (e.g. depending of the public nature of the cloud computing service, etc).

40. As far as the additional protocol and the transborder data flows implying non contracting States are concerned, and except the exceptions provided for in article 2.2 of the additional protocol, article 2.1 of the latter compels contracting States to forbid these flows if the concerned non contracting State (or organization) does not ensure an *adequate* level of protection for the intended data transfers. In this respect, the assessment of adequacy could be realized on a case by case basis. And again due to the diversity of cloud computing services, some distinctions could be drawn by the contracting States, and the protection offered by a non contracting State could be

[7] Except in cases where onion routing is used by cloud computing service. Onion routing is a technique allowing anonymous transactions within a computer network. The messages are encrypted repeatedly and sent through multiple networks nodes called onion routers. Each node decrypts the message in order to get the routing instruction and so encrypts and sends the message to the next onion router till the final destination. Intermediary nodes do not know the origin and the final destination of the message. In that case the national law enforcement agencies are unable to get access to the information if it is transmitted through onion router to a destination outside the national borders. On onion router example, *see* EFF'sTor: http://www.torproject.org ,

adequate in one case and not in another; which distinctions can and should/have to be drawn?

Two principal remarks can be made. Firstly, the aforementioned rule should be without prejudice to an analogical – and *a fortiori* – interpretation of article 12.3, a) of the ETS 108 in the present context of data flows targeted to non contracting States. That is to say that the Convention should be interpreted in such a way that a contracting State *can* prohibit – or subject to authorization – a transborder flow related to a specific "automated personal data files" aforementioned if, for instance, the foreign State concerned does not offer an equivalent protection, *even though* it ensures an adequate level of protection.

Secondly and more generally, the additional protocol doesn't compel the contracting States to do anything else if the targeted foreign State offers an adequate level of protection; it only forbids to allow transborder data flows targeted to non contracting States. In this respect, despite the fact that the protocol also pursues the free flow of information, it does not explicitly forbid contracting State to forbid personal data flows targeted to a non contracting State offering an adequate protection. So, the question in the context of cloud computing is the following: could a contracting State deem that a particular processing involved in a cloud computing service require an equivalent protection from the non contracting State, *even if* this particular processing is not deemed to constitute a particular "automated personal data files" under article 12.3, b) of the ETS 108, or to involve particular data? In other words, contracting States seems here to recover a larger margin of maneuver than it was the case under the ETS 108. But, on the one hand, how wide could be this maneuver if there is one? And, on the other hand, which cloud computing services could and should/has to be specially treated through this potential margin?

41. Beyond what we called an "administrative control", the ETS 108 and its additional protocol, although they try to solve – in a certain manner – the issue of transborder data flows, don't provide for any rule related to *conflicts of law*. And this is also true as regards personal data flows between contracting States. As far as these latter are concerned, the explanatory report recognizes that "it may not always be easy to determine which […] national law applies", and it underlines that "the "common core" will result in a harmonization of the laws of the Contracting States and hence decrease the possibility of conflicts of law or jurisdiction ". However, neither the Convention, nor the additional Protocol addresses this issue. Moreover, the Explanatory Report also specifies that the principle of freedom of flow of personal data provided for in article 12.2 "does not mean that a Contracting State may not take certain measures to keep itself informed of data traffic between its territory and that of another Contracting State, for example by means of declarations to be submitted by controllers of data files". In the context of cloud computing, the scattered worldwide locations of the actors involved (i.e. cloud computing service providers, subscribers, users and data subjects, controllers or processors) exacerbate conflict of laws concerns – that already existed – and *have to* be faced by national legislations; but how can they regulate and which constraints limit their margin?

42. The already quoted directive 95/46/EC addresses, in some extent, the question of the applicable law, by compelling the Member States to apply their national laws in the cases defined in article 4 of this directive. This article marks the spatial boundaries of European data protection law. It seems that this rule needs to be implemented as an "unilateral conflict of law rule" defining the applicability of the national law at stake following the defined criterions. However, despite the fact that the directive also provides rules as regards transborder data flows targeted to a non Member State, it

does not provide for a general "bilateral conflict of laws rule" the Member States could be deemed free to adopt.

Contracting States (here, the legislator or the jurisdictions) have to define which law apply to which particular processing of personal data. And they have different ways to determine the applicable law. They can adopt a bilateral conflict of laws rule determining the applicable law in all instance, they can define the criterions of applicability of their law (for instance, taking into account the place of establishment of the data controller and/or the location of the equipments it uses for the purposes of a particular processing, *see* art. 4 of the directive 95/46/EC) with an unilateral rule, or they can also define a particular "public order exception clause". However that may be, cloud computing technologies require a reflection on part of contracting States to the Convention on which criteria are the best to cause the applicability of their national data protection laws and to fit into the particular issues arising from the above mentioned technologies. In this respect, for example, only some rules of data protection could receive a particular territorial scope as regards cloud computing services in general or even some cloud computing services in particular. For instance, a particular specific duty of information and right of access could have a more extended territorial scope if some data protection rules are extended to the processors, imposing them specific duties or responsibilities – if deemed necessary –, the applicability of these rules could depend on specific criteria differing from those applicable to the data controller according to already established general data protection rules. Needless to say that such a conflict of laws rule would gain in quality – from a practical point of view – if it would be discussed at an international level – for instance, under the auspices of the C. of E. for instance. It should also be noted that directive 95/46/EC is in process of modification. A discussion relating to conflicts of law seems to be of high interest and pressing to guarantee the practical enforcement of data subjects' protection, and to bring legal certainty to the emergent and promising market of cloud computing.

43. A final point can be underlined as regards conflict of laws: which – if it can – influence would have article 8 ECHR on data protection conflict of laws rules? Article 1 ECHR reads as follows: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention". In this respect, the jurisdictions of these contracting Parties, applying the law of a non-contracting State of the ECHR, could have to ignore this foreign law if, in the particular case, it rises to a conflicting situation with the fundamental rights provided for by the ECHR. The European Court of Human Rights has already approached this concern as regards article 6 ECHR. Four questions need to be addressed. Firstly, which "rights" recognized under article 8 ECHR could influence the application, in a particular case, of conflict of laws rules? Secondly, which data protection rules fall within the scope of article 8 ECHR and these rights? For instance, which rules of the "common core" of the [ETS] 108"? And finally, which "connections" an international case involving cloud computing technologies need to have with the Council of Europe's members States' territories to require the applicability of these identified rights? It has to be recalled that this would happen under the final control of the European Court of Human Rights.

44. To sum up, closely regarding the specificities of cloud computing technologies, contracting States to the ETS 108 have to determine which applicability of which national data protection rule to international cases is desirable and permitted and/or required.

11 Data retention and restriction for some matters

45. At this point of the discussion, we also have to pay attention to the question of the extension of certain legal obligations for certain communications services' providers to retain data about the uses of their services or to cooperate with law enforcement authorities at their request or even at their own initiative[8]. That obligation would be more or less similar to the obligation imposed by the EU Directive to the IAPs and publicly available e-communication services' operators.

For instance, should Facebook have an obligation to retain some data and to cooperate with law enforcement authorities?

12 Conclusions

46. The first question raised by the consideration and questions set above is to know if a specific regulation on cloud computing is needed.

At this very provisional stage, following considerations can be addressed. It is not obvious that, from a Privacy legal point of view, it will be possible to envisage on equal footing, even if they have common characteristics, all the cloud computing services. To be short: Facebook does not raise the same problems than Azure of Microsoft.

Anyway, as showed previously, new definitions and concepts like data processor, subscriber, ought to be introduced if we want to approach correctly the problems.

According to the specificities of each cloud computing services, different contractual models ought to be proposed between subscribers and cloud computing services with provisions about responsibilities, law applicable and competent jurisdiction, right to the data subjects to take benefit of the contract, etc.

Additionally, it might be interesting to see to what extent certain new obligations might be the object of a Council of Europe Recommendation. This Recommendation would target both subscribers/user and cloud computing services' providers. It might concern notably the obligation to inform the users and the data subjects about the main characteristics of the service and their qualification as data controller or data processor, about data breaches, additional obligation to security, etc.

As regards security questions, perhaps provisions about the role of standardization authorities and labeling systems would be appropriate;

The idea to have specific Corporate Binding Rules in cases of multinational cloud computing services' providers has to be assessed.

47. At this stage, we isolated questions as regards the Council of Europe Convention 108 amongst which we have:

- Do we have to specify new actors in the context of cloud computing?

- What is the lot of the data circulating/stored when the user, data subject or subscriber dies? What happens with the data put into the cloud if the cloud service is transferred to a new operator (fusion, etc)?

[8] *See* the Council of Europe Cybercrime Convention, article 17.

- Is the differentiation between domestic use/non domestic use pertinent?

- Do we need to extend the protection to the legal person and to change the concept of personal data?

- Is it useful to add some definitions which do not exist yet in the ETS 108 and to modify some others?

- On the security field, do we need to make special provisions for the cloud computing? What's about the role of standardization bodies? Do we need to envisage security breach provisions in that context?

- Do we have to ban or restrict the use of cloud computing services as regards sensitive matters, professions or activities (public or not)?

- How to manage the transborder data flow questions and the applicable law issue?

48. To distil the substance of the present report, it has first and foremost to be underlined that cloud computing is a very wide – and not precisely defined – concept consisting of lots of different realities. On the one hand, the offered *services* have various natures – e.g. IaaS, PaaS or SaaS, private or public clouds, etc, – and various purposes – domestic, professional, public, etc. And on the other hand, the involved *actors* are also very different – individuals who are consumers or professionals, SMEs, NPOs, administrations, worldwide corporations, etc, and numerous imbalances could exist between them. Therefore, the questions identified above could receive varying *answers* according to the many facets of cloud computing technologies that will most probably continually evolve. In fact, these facets not necessarily raise the same concerns as regards data protection. Moreover, in the same sense, these *questions* could also vary according to the particular services and actors at stake, and they could not always have the same pertinence.

So there is a preliminary recurrent question: **which particular cloud computing service is at stake and who is involved?** Keeping the *specific and multifaceted* context of cloud computing in mind, the questions we identified – and we do not aspire to be exhaustive – can be summarized as follows:

1) Who are the actors of cloud computing? Do they need to be legally defined if it is not already the case? If they are already legally defined, do the definitions at stake need to be modified? We identified five, sometimes overlapping, categories of actors: subscribers, users, data subjects, controllers (co-controllers) and data processors. Two principal questions to raise:

- Does the concept of data processor need to be defined under ETS 108?
- Do legal persons need to be protected under the data protection rules of the ETS 108, with regard to which data (extension of the definition of the personal data and, therefore, of the data subject)?

2) Which existing duties under ETS 108 need to be adapted? Which non-existing duties under ETS 108 need to be created? As the case may be, which actor has to bear these modifications or these creations? More precisely:

- Should data processors have to support specific duties provided for by the law, and which duties (e.g. in general as regards transparence and liability)?

- Should co-controllers to be targeted by specific liability rules and a particular allocation of duties under ETS 108?
- Should a specific duty as regards security breaches be established? Who would have to support this new duty (provider and/or subscriber), towards which actor (subscriber and/or data subjects) and in which cases?
- How to treat the distinction between non-domestic and domestic processing activities? When is it still relevant and how to improve the protection of data subjects when a domestic use exception could apply (total exclusion of data protection law or establishment of a softer legal regime)?
- Should data retention obligations have to be imposed on cloud computing services providers, when and how?
- Due to the possible imbalance between the actors of the cloud, is consent always an adequate basis of the legitimacy of the processing at stake or should data controllers – and if so when – have a duty to base the legitimacy of their processing on an additional basis?

3) How could what call the "data protection continuity" be maintained? This question can be subdivided into the following concerns:

- When the cloud computing service provider or its user (data subject) terminates the contractual relationship at stake, how can it be guaranteed that the data subject (user) will recover the total "ownership" (control) of data relating to him?
- In cases of bankruptcies, mergers of corporations or sales of corporations, etc, how can it be guaranteed that the level of protection originally ensured to the data subject will remain at least equivalent?

4) How to face the numerous concerns arising out of the international character inherent in cloud computing? This broad question also needs to be sliced into parts:

- Do some specific cloud computing services (e.g. involving sensitive data) need to be forbidden when they imply transborder data flows between contracting States and, a fortiori, non-contracting States ensuring an adequate level of protection?
- Which concerns can be solved by binding corporate rules?
- How to assess the adequacy of non-contracting States to ETS 108 as regards the processing of personal data for law enforcement purposes?
- How far could consent and contract authorize transborder data flows outside the territories of contracting States, towards non-contracting States not ensuring an adequate level of protection?
- How to resolve conflict of laws when actors involved in the cloud are located anywhere in the world and rules on conflict resolution do not yet exist? In other words, we should work out rules to solve conflicts of law at least in the context of Cloud computing.
- Does the "territoriality" of data protection rules have to be differently defined depending on the duties (e.g. security or transparence) and the actors (data controller or data processor) at stake, and if so, how?

_____