# Personal Data Protection in the era of cloud computing.

# New challenges for european regulators.

Panagiotis Kitsos, Paraskevi Pappa [1]

## Abstract

It is widely aknowledged that we are entering in an era of revolutionary changes in the field of Information and Communication Technologies .

The spread of broadband internet connections has led internet to function not only as a communications network but also as a platform for new computing applications .

The most recent application is the so called "cloud computing", which permits the running of software applications or the storage of data to be performed at remote servers which are connected to our computers through the Internet. Examples of these applications are the web-based email services, online computer back up, data storage sites services, file transfer services e.t.c

These applications though, raise considerably strong concerns among privacy advocates , scholars and data protection agencies on a number of privacy and personal data issues in relation to their unique features that might easily put at risk privacy rights and undermine current personal data protection policies

Key words : Data Protection, privacy, Cloud Computing , Directive 95/46/EC

## 1 Introduction

It is said that we are entering in an era of a new technological revolution in the sector of information and communication technologies. The emergence of cloud computing services raises several concerns related to the protection of personal data and privacy. which might include sensitive information is transmitted, processed, and stored in remote places .

The responsibility to secure this information falls into the hands of the hosting company. It is very important to determine the role of controllers and processors, to examine how much control and involvement over their personal data individuals have , how does the host company secure this data from possible breaches and which law applies in the clouds.

[1] Panagiotis Kitsos is a Lawyer and PhD candidate in the University of Macedonia, Paraskevi Pappa is a Lawyer, lecturer at Technological Institute of Epirus .

Our goal is to address these important data protection and privacy concerns within the relevant current European union legal framework and determine whether it can be the adequate response to these concerns.

## 2 What is cloud computing

The term "cloud computing"[2] is a term that has long been debated and described by IT specialists and fallen into hype. Phrases like *"the Cloud is the Computer*." [3] have made their way through numerous discussions on the exact definition of the term.

It has been characterized as a result of the ubiquitous broadband access which *is " becoming a platform for computing –vast, interconnected virtual supercomputer"*.[4]

The National Institute of Standards and Technology, Information Technology Laboratory NIST has defined "cloud computing" as *"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*" .

Further more both in National Institute's of Standards and Technology, definition of "cloud computing" [5] and the European Network and Information Security Agency's (ENISA) [6] report on "Cloud Computing"[7] three main categories of cloud computing are defined:

---

[2] The term "cloud" is used as a metaphor for the Internet, based on a cloud drawing used in the past to represent the telephone networks

[3] McFedries P. "The cloud is the computer", IEEE Spectrum, Online, August 2008. Electronic Magazine, available at http://www.spectrum.ieee.org/aug08/6490. We should be carefull though when defining the "cloud as the computer" since it is possible to underestimate the inherent security and privacy risks that cloud technologies entail. See also Fingar, P. (2009). in "Cloud computing set to unleash a perfect storm in business"., states :"In short, the cloud is the Real Internet, or what the Internet was really meant to be in the first place: an endless computer made up of networks of networks of computers. Even shorter: the Cloud is the Computer." http://www.cordys.com/ufc/file2/cordyscms_sites/download/6f5f4d1cfe8be9d78d972fa808d8702c/pu/cordial_fingar.pdf ]

[4] Cavoukian A. « Privacy in the clouds » White Paper on *Privacy* and digital identity: implications for the internet, *www.ipc.on.ca/images/Resources/privacyintheclouds.pdf*

[5] Mell, P , Grace T. "The NIST Definition of Cloud Computing" http:// *csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc*

[6] European Network and Information Security Agency, is as a **body of expertise**, set up by the EU to carry out very specific technical, scientific tasks in the field of Information Security. http://www.enisa.europa.eu/about-enisa

[7]Catteddu D. and.Hogben G. "*Cloud Computing: benefits, risks and recommendations for information security"* http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

1. Software as a service (SaaS): which is software offered by a third party provider, available on demand, usually via the Internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM (Customer relationship management)[8] services and web content delivery services (Salesforce CRM, Google Docs, etc). So anyone of us with a simple and even cheap computer with limited storage capacity or with a smartphone connected to the Internet or a company network, is able download or upload data from the cloud.

2. Platform as a service (PaaS): allows customers to develop new applications using APIs (Application Programming Interface)[9]. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine, Youtube.

3. Infrastructure as service (IaaS): provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud. [10]

Clouds may also be divided into:

(a) public: available publicly where any organisation may subscribe

(b) private: services built according to cloud computing principles, accessible only within a private network

Simply put, in the field in the cloud any computer connected to the Internet is connected to the same pool of computing power, applications, and files[11]. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites, photography websites, social networking sites, and many more.[12]

So users can store and access personal files such as music, pictures, videos, and bookmarks or play games or do word processing on a remote server rather than physically carrying around a storage medium such as a DVD or thumb drive. Those

---

[8] The management of a company's interactions with customers, clients and sales prospects

[9] It serves as an interface between different software programs and facilitates their interaction, similar to the way the user interface facilitates interaction between humans and computers. http://en.wikipedia.org/wiki/Api

[10] Infrastructure as a Service (IaaS) provides data center, infrastructure hardware and software resourcesover the Internet, such as server, operatingsystem, disk storage, database, and/or messaging resources.

[11] http://en.wikipedia.org/wiki/Cloud_computing

[12]Robert Gellman, " Privacy in the Clouds:Risks to Privacy and Confidentiality from Cloud Computing". study prepared for the World Privacy Forum February 23, 2009 http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

of us use web-based email such as Gmail, Hotmail, Yahoo, are making use of cloud email servers as well.

Cloud Computing Service Providers insist that cloud computing is the future in computing applications.

The advantages for users of cloud computing applications are many since any information stored locally on a computer could be stored in the cloud e.g a. the ability to store more data than a personal computer can available at very low -- or zero -- cost[13] b. freedom from having to deal with upgrades and security issues, c. It allows users to connect from a rmote place even without their computer, d. users do not have to purchase or maintain specific hardware and software applications since they simply rent these services . You pay for what you use and the amount of time you use it. e. The users do not have to afraid of possible loss of data due to a stolen or lost computer, cd or flash drive.[14]

The economic-benefits for both cloud computing users and national economies can be significant

According to a report, written by the Centre for Economics and Business a widespread adoption of cloud computing in Europe's five largest economies (France, Germany, Italy, Spain and the UK) has the potential to generate over €763 billion of cumulative economic benefits over the period 2010 to 2015.[15]

## 3 Privacy and Data Protection Concerns

Cloud computing though raises strong concerns among privacy advocates. It is pointed out that users, by uploading and storing their data with programs hosted on someone else's hardware, lose a degree of control over their personal information. The responsibility for protecting that information from hackers and data breaches then falls into the hands of the hosting company rather than the individual user.[16] That triggers a series of legal problems on user's privacy and confidentiality risks such as the sharing of information collected without consent and weaker privacy protection laws in the country where data centers are.

---

[13] Leslie Harris,Perils in the Privacy Cloud (2009) ABC News, 15 Sep 2009<http://abcnews.go.com/Technology/AheadoftheCurve/privacy-evaporates-computingcloud/Story?id=8573715&page=1>.

[14] See for the benefits of Cloud computing "Above the Clouds: A Berkeley View of Cloud Computing" by Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Technical Report EECS-2009-28, EECS Department, University of California, Berkeley.

[15] Centre for Economics and Business Research, "THE CLOUD DIVIDEND: Part One -The economic benefits of cloud computing to business and the wider EMEA economy France, Germany, Italy, Spain and UK" http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf

[16] http://www.privacyrights.org/ar/cloud-computing.htm

In a letter to the Federal Communications Commission (FCC) , David Vladeck, director of the Federal Trade Commission (FTC) Bureau of Consumer Protection, notes that "the ability of cloud computing services to collect and centrally store increasing amounts of consumer data, combined with the ease with which such centrally stored data may be shared with others, create a risk that larger amounts of data may be used by entities in ways not originally intended or understood by consumers." [17]

He added that the FTC is "considering cloud computing and identity management as part of a broader initiative to re-examine various models to promote consumer privacy." [18]

Robert Gellman a Privacy and Information Policy consultant has produced an influential report for World Privacy Forum on the implications for the privacy of personal information as well as for the confidentiality of business and governmental information.

In his document identifies the multiple and complex privacy and confidentiality issues that may arise by cloud computing services.

In particular he describes a number of data privacy concerns in Cloud environments such as

a. the user's privacy and confidentiality risks derived from the terms of service and privacy policy established by the cloud provider since many users are not aware of the details set out in these terms or of the consequences of sharing information with a cloud provider, b. the privacy and confidentiality rights, obligations, and status that may change when a user discloses information to a cloud provider, c.the consequences that could, disclosure and remote storage, have for the legal status of or protections for personal or business information, d. the effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information, since any information stored in the cloud eventually ends up on a physical machine owned by a particular company or a person located in a specific country, may be subject to the laws of the country where the physical machine is located, e. the user's information that moves from jurisdiction to jurisdiction, from provider to provider, or from machine to machine, f. the disclosure of users records to govenverment agents, g. whether t electronic communications laws apply to cloud computing communications or they may apply differently to different aspects of cloud computing.

These are only some of the concerns raised in relation to cloud computing services and cloud computing is nowadays one the top issues for privacy advocates.

---

[17] FTC to examine cloud computing privacy concerns http://homelandsecuritynewswire.com/ftc-examine-cloud-computing-privacy-concerns

[18] ibid

## 4 Regulatory challenges

A number of concerns need to be addressed within the framework of European Law for Data Protection.

Peter Hustinx The European Data Protection Supervisor in a speech given in 2010 in the Third European Cyber Security Awareness Day, has defined a number of challenges for European regulators such as the determination of responsibilities, the determination of the applicable law, the problems arising from international data transfers, the need of a more effective personal data protection laws in the new technologically advanced environment and the issue of protection to users of cloud computing services , who use them for purely personal purposes. [19]

### 4.1 Determination of responsibilities

The determination of responsibilities in the cloud computing environment can examined under the light of Directive 95/46/EC which provides obligations on the entities that process data as data controllers. Fewer obligations are imposed on data processors, entities that are 'entrusted' by controllers to process data.

In Hustinx's opinion , even when cloud providers play a mere "processing" role, they will have to engage in a very close cooperation with their clients to ensure that controllers are in a position to fulfil their data protection obligations.

The role of Data Controller and Data Processor is particularly important in the determination of the liability of the parties involved in the process of personal data . The determination of the responsible for compliance with data protection provisions is directly related to which national laws apply and which data protection authorities can effectively supervise data processing operations. [20]

In Article 29 Data Protection Working Party's , Opinion 1/2010 on the concepts of "controller" and "processor" it is stated that the 'processor' "plays an important role in the context of confidentiality and security of processing as it serves to identify the responsibilities of those who are more closely involved in the processing of personal data, either under direct authority of the controller or elsewhere on his behalf".

It is very important to distinguish between 'controller' and 'processor' in order to distinguish between those who is/are responsible as controller(s) and those that are only acting on their behalf. .

According to Directive 95/46/EC the 'controller' is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations,

---

[19] Hustinx Peter "Data Protection and Cloud Computing under EU law", speech delivered by Peter Hustinx at the Third European Cyber Security Awareness Day, Brussels April the 13th 2010. http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/SA2010 See also the analysis of Balboni, Paolo, "Data Protection and Data Security Issues Related to Cloud Computing in the EU" (August 18, 2010). ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference 2010; Tilburg Law School Research Paper No. 022/2010. Available at SSRN:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661437

[20] Article 29 Data Protection Working Party , Opinion 1/2010 on the concepts of "controller" and "processor" available http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

the controller or the specific criteria for his nomination may be designated by national or Community law";

The 'processor' "shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller";

The application of these definitions though to the cloud-computing environment is a rather difficult task .

On December 2010, the EU Article 29 Data Protection Working Party adopted Opinion 8/2010 on the territorial application of EU Data Protection Directive 95/46/EC and the national data protection laws transposing the Directive.[21]

The Opinion emphasises the complexity of the issue in the cloud computing environment stating that even if the exact place where data is located is not always known and it can change in time, this is not decisive to identify the law applicable.

According to Opinion "it is sufficient that the controller carries out processing in the context of an establishment within the EU, or that relevant means is located on EU territory to trigger the application of EU law…"

As it is stated in the Opinion the specification of the applicable rules is related to the identification of the controller and to the activities that take place at A certain level.

When the user of the cloud service is a data controller for example when a company uses an agenda service on-line to organize meetings with clients in the context of the activities of its establishment in the EU, EU law will be applicable on the basis of Article 4(1)a. [22]

In some circumstances the data controller can also be the cloud service provider when for example it provides for an agenda on-line where private parties can upload all their personal appointments and it offers added value services such as synchronization of appointments and contacts. If the cloud service provider uses means[23] in the EU, it will be subject to EU data protection law on the basis of Article 4(1) c.

### 4.2 Which law applies?

The determination of the applicable law is a key issue since in the Cloud computing environment, personal data are processed and stored on servers in several places

[21] Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, 16 December 2010, WP179, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

[22] The company should make sure that the service provides for adequate data protection safeguards, notably with regard to the security of personal data stored on the cloud. It will also have to inform its clients of the purpose and conditions of use of their data.

[23] It could include more specific equipment e.g. if the service uses calculating facilities, runs java scripts or installs cookies with the purpose of storing and retrieving personal data of users. The cloud service provider will then have to provide users with information on the way data are being processed, stored, possibly accessed by third parties

around the world[24], so the application of the provisions of the Directive 95/46/EC is becoming a complex issue.

Regarding the territorial application of Directive 95/46/EC article 4 of the Directive 95/46/EC requires that each Member State should apply the national provisions to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.

Article 29 WP in its Opinion 1/2008 on data protection issues related to search engines[25] has explained the concept of the "establishment" stating that "an establishment" implies the effective and real exercise of activity through stable arrangements, adding that the legal form of the establishment – a local office, a subsidiary with legal personality or a third party agency – is not decisive. Also on the requirement that the processing operation should carried out "in the context of the activities" of the establishment, that means that the establishment should also play a relevant role in the particular processing operation.[26]

When the same controller is established on the territory of several Member States, then he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable. This actually means that the establishment of the controller is determinative for the applicable national law and "possibly for a number of different applicable national laws and the way in which they relate to each other".[27]

Furthermore the same provisions apply both when the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law and where the controller is not established on Community territory but for purposes of processing personal data makes use of automated equipment (e.g., datacenters, servers, etc.) situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."[28]

---

[24] As Viviane Reing wrote in WSJ "a UK resident who creates an online personal agenda could use software hosted in Germany that is then processed in India, stored in Poland and accessed in Spain". See Viviane Reding "The Digital Forecast Is Cloudy European consumers need protection against misuse of their information in the online"cloud." http://online.wsj.com/article/SB10001424052748703555804576101591825228076.html and http://ec.europa.eu/commission_2010-2014/reding/pdf/news/cloud_en.pdf

[25] See Article 29 Data Protection Working Party's opinion 1/2008 on data protection issues related to search engines; available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm.

[26] Ibid

[27] Article 29 Data Protection Working Party , Opinion 1/2010 on the concepts of "controller" and "processor" available:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[28] Article 4 par. 1 (c) of the Directive 95/46/EC see also WP 29 Opinion 1/2008 on data protection issues related to search engines; available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm. wich states that "Search engines that use equipment on the territory of a Member State (EEA) for the processing of personal data also fall under the scope of that Member State's data protection law. A Member State's data protection law still applies where the controller[…] for purposes of processing personal data makes use of equipment, automated orotherwise, situated on the territory of the said

European Data Protection Supervisor, Peter Hustinx, in his abovementioned speech on "Data Protection and Cloud Computing under EU Law", also stated that: "(a)A cloud provider established in the EU – or acting as processor for a controller established in the EU – will in principle be 'caught' by the EU law. (b)A cloud provider which uses equipment (such as servers) in an EU Member State – or acting as a processor for a controller using such equipment – will also be caught. ( c) A cloud provider in other cases – even if it mainly and mostly targets European citizens – would not be caught by EU law".

Nevertheless as a last comment he added that, given that the Directive is in the process of being reviewed the amendments directed to ensure that Cloud Service Providers that target EU citizens "do not escape the application of EU law" may be considered.[29]

### 4.3 International data transfers

Closely related to the issue of the applicability of law is the problem of international data transfers.

According to Directive 95/46/EC , transfers of personal data to third countries without an adequate level of protection are prohibited.[30] By way of derogation from Article 25 Member States shall provide that a transfer of personal data to a third country which does not ensure an adequate level of protection may take place on condition that the data subject has given his consent or the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party, or the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims or the transfer is necessary in order to protect the vital interests of the data subject, and so on.[31]

Moreover Directive 95/46/EC allows a Member State to authorize a transfer or set of transfers to a 'non-adequate' third country 'where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. The provision specifies that 'such safeguards may in particular result from contractual clauses'.[32] Article 26(4) also gives a power to the Commission, acting in accordance with the procedure laid down in Article 31, to decide that certain standard contractual clauses offer the sufficient guarantees envisaged in Article 26(2). Also an exception

---

Member State, unless such equipment isused only for purposes of transit through the territory of the Community".

[29] Viviane Reding Vice-President of the European Commission, EU Justice Commissioner in her speech "The reform of the EU Data Protection Directive: the impact on businesses European Business Summit Brussels, 18 May 2011 has noted that this proposal would be one of her priorities in reforming the current data protection framework.

[30] Article 25 par. 1 Directive 95/46/EC

[31] Article 26 par. 1 Directive 95/46/EC

[32] Article 26 par. 1 Directive 95/46/EC

applies if the data controller provides adequate safeguards for the protection of personal data: for example, enter into a contract with the recipient of the data ensuring that the data will remain adequately protected. [33]

According to Hustinx the problem is that these rules rely on a definition of data transfer from 'point to point'. They require having a contract, a Model Contract for the transfer of personal data to third countries and sometimes a notification to the authority for each transfer to a country where the legal framework is not adequate.

In practice this is very difficult to implement, particularly in cloud computing which is characterized by a continuous transfer of personal data.

Other solutions such as Safe Harbor principles are no better in the cloud computing environment as the personal data moves to different countries and between several companies.

The solution according to Hustinx could also be found in the context of the review of the Directive with the introduction of an extended responsibility for controllers with respect to data transfers. Also the adoption of Binding Corporate Rules[34] by multinational companies to ensure an adequate level of protection for the intra-group transfers of personal data from a country in the EU or the European Economic Area (EEA) to a third country, seems to be an effective solution as well in the cloud computing environment.

### 4.4 Efficiency of EU regulatory framework

The overall goal to ensuring effective personal data protection in cloud computing environment is very important.

Article 29 WP has published a paper in 2010 called "The Future of Privacy"[35] in which proposes the introduction of "Accountability" principle and "Privacy by Design" principle.

The "Accountability Principle" is a provision included in the new legislative framework pursuant to which data controllers Data controllers should have in place the necessary internal mechanisms to demonstrate compliance to external stakeholders, including national data protection authorities and would also remain accountable and responsible for the protection of personal data for which they are

---

[33] Working Party article 29 Working Document "Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive" http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

[34] See the toolkit on Binding Corporate Rules (BCRs), issued the Article 29 Working Party on 2008 aimed at promoting them as a mechanism for transferring data to countries without an adequate level of data protection. The toolkit includes: (1) a table highlighting the elements and principles to be found in BCRs http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf; (2) a document setting up a framework for the structure of BCRs, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf; and (3) a revised version of the FAQs on BCRs, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf

[35] Article 29 Working Party "The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data"http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

controllers, even in the case the data have been transferred to other controllers outside the EU

The “Privacy by Design” principle obliges technology designers and producers as well as data controllers to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirement.

The introduction of “Privacy by Design” will also emphasize the need to implement privacy enhancing technologies (PETs), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data (e.g., access controls, encryption)in products and services provided to third parties and individual customers (e.g. WiFi-Routers, social networks and search engines).

As Hustinx points out “In the context of cloud computing services, this means that controllers and processors would have to demonstrate that they have taken all the necessary measures to ensure that data protection rules and principles are complied with. This approach would also be very interesting where personal data are entrusted to providers in third countries”.

4.5 Protection of household activities.

The protection of household activities in the cloud under EU law is also a matter that remains to be answered.

The transfer of personal data, such as the storage of pictures and calendars (which usually are stored on local desktops), to data centers that are considered as located in the cloud raises the question whether the cloud provider is covered by the EU data protection law.

Article 3 of Directive 95/46/EC excludes from the scope of application of the Directive data processing carried out "by natural persons in the course of a purely personal or household activity" .

If the information uploaded to the cloud is not covered by the Directive because it is information of a personal nature, then the processing activities that are carried out on behalf of the individuals involved might not be covered either.

This gap in the protection of end-users is definitely an obstacle to the objectives of European Union to protect the fundamental right to privacy and data protection .

So the cloud computing service providers when offering services to a private individual should be required to provide certain safeguards regarding the security, and the confidentiality of the information uploaded by users, regardless of whether their client is a data controller or an end user.

## Conclusions

The current European data protection regulatory framework seems rather week to adequately address privacy concerns related to cloud computing .

Issues such as the applicable law , the international data transfers, the definition of the responsibilities of data controllers and data processors might have to be readdressed in the context of cloud computing services.

The expected revision of Directive 95/46/EC should take into account all the developments in the Information and Communication Sector and provide a solid legal framework for the protection of personal which is an absolute precondition for cloud computing services to develop and boost the economy across Europe.

Not only consumers but small and medium enterprises are the ones to benefit most from an adequate legal framework for Cloud computing services since they usually lack the necessary funds to support advanced and updated data storage and security services.

Neelie Kroes, vice-president of the European Commission responsible for the Digital Agenda, has said "I want to make Europe not just cloud-friendly, but cloud-active. We can deliver cloud computing by using research and innovation to bring about better clouds. Along the way we can modernise our computing infrastructure and give our SMEs a new platform for innovation".[36]

We should bear in mind that balancing citizen's rights and Small and Medium enterprises interests is the way to ensure the economic and social progress and that the fundamental rights of individuals are safeguarded.

[36] Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50 , Towards a European Cloud Computing Strategy World Economic Forum Davos, 27 January 2011