diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 18/07/2012

All'indirizzo http://www.diritto.it/docs/33744-cloud-computing-the-official-opinion-of-the-eu-data-protection-authorities

Autore: Marcoccio Gloria

Cloud Computing: the official Opinion of the EU Data Protection Authorities

Cloud Computing: the official Opinion of the EU Data Protection Authorities

Gloria Marcoccio (gloria.marcoccio@glory.it)

June2012

On July 1st 2012 the WP 29, EU Data Protection Working Party, published an important Opinion on "Cloud Computing"[1].

Although the WP 29 Opinions are not regulations and consequently they do not entail new legal obligations to be observed, in any case they reflect the authoritative position of the European Data Protection Authorities (DPA in the following) and as such provide important guidance and clarifications in the matter dealt with. Furthermore, considering that, typically, the WP 29 Opinions on important issues (such as in the past: CCTV, systems allowing real time geo-location of individuals, ...) sooner or later give rise to corresponding national decisions by the DPAs concerned, and these latter ones are regulations to be fulfilled, as a consequence the "Opinion on Cloud Computing" assumes, even in perspective, a particular informative value.

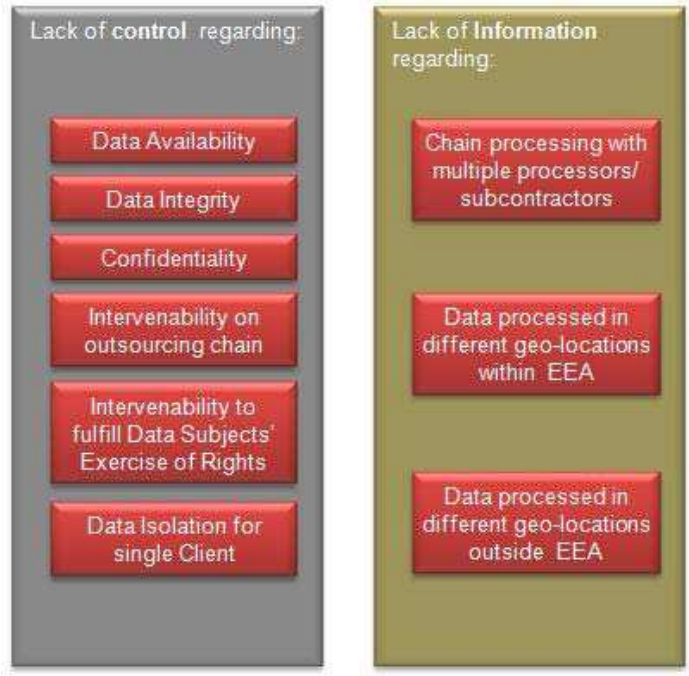
No doubt that Cloud Computing is a very popular topic and widely discussed for its many benefits and costs reductions brought but at the same time some concerns arise especially regarding aspects of security and data controllability, contractual issues, compliance with applicable laws.

It is a complex subject, full of facets certainly not yet entirely known, under spotlight in many contexts, international, EU and national[2]. Moreover, as regards the aspects of personal data protection and privacy, they play a fundamental role since data and related processing are the preeminent subjects of the services operated in Cloud Computing environment, which already cover, now and even more in the future, the majority of working environments in the private sector, public administration and networked society.

The recent Opinion provides an overview of main privacy issues of Cloud Computing as well as concrete guide for a systematic approach in addressing the risks associated, with indication of security measures and precautions and safeguards both at technical /organizational and contractual level, always with a view to provide guidance to operate in a manner consistent with European privacy laws, essentially the directives 95/46/EC and 2002/58/EC.

In particular the Opinion deals with the case, certainly of common interest, in which the Client of the Cloud Computing Service is data Controller and the Service Provider is data Processor (for Italy see as reference articles 4, 28 and 29 of Legislative Decree 196/03). The Data Subjects are those whose data are processed by the Controller (eg employees in relation to internal employer administration services, clients / subscribers of the services offered by the company, citizens in relation to services provided by the public administration, ...).

The main sources of risks reported in the WP 29 Opinion can be represented in terms of:



The Opinion provides a reference framework for systematic description of requirements under the European privacy regulations and presents a categorization of the necessary countermeasures.

However this framework needs to be contextualized in the specific system of law applicable to the Client: in fact, the national transposition of European directives may lead to specific requirements (eg for privacy: preliminary checks, authorizations, notifications to the national DPA, ...) , different from country to country: their respect is binding for the Client (as data Controller).

For example in Italy it is necessary to fulfill the measures and arrangements identified by the DPA with its Decisions already applicable to services based on Cloud Computing (for example: the Decision on the role of the system administrator, the Decision concerning security measures for traffic data in scope of electronic communication services publicly accessible, ...).

Next figure summarizes the main aspects of the regulatory framework and measures identified by the WP 29.

[1] Opinion 05/2012 on Cloud Computing –

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[2] in this regard to be mentioned the recent guide line issued by the Italian DPA: "CLOUD COMPUTING - PROTECT YOUR DATA WITHOUT FALLING FROM A CLOUD"- http://www.garanteprivacy.it/garante/doc.jsp?ID=1894503

WP 29 Opinion 5/12: summary of main aspects of the regulatory framework and identified measures

EU legislative framework for data protection:	
95/46/EC	2002/58/EC

Applicable Law:

The law of the country(ies) where the Client/Controller is established

Relationships Client -Provider -Subcontractors

Essential clarifications:

- responsibility allocation for law compliance purpose
- how to operatively allow the exercise of data subjects

Fundamental principles

Transparency	Purpose specification and limitation	Data retention/Data erasure
•Between Client and Data Subjects •Between Client and Provider Clear and complete contract	Risks from the presence of many Providers/ Subcontractors Tech. / Organiz. measures and contractual obligations	Necessary reliability in these operations Tech. / Organiz. measures and contractual obligations

Contractual safeguards, data transfers outside EEA

- Contract is necessary between Client and Provider
- Data transfer outside EEA:
  - In general the 95/46/EC exemption's cases are not applicable
  - Safe Harbour for U.S. Providers (however for cloud services a third party assessment should be performed)
  - in general, to be preferred the EU standard contractual clauses (eg. 2010/87/UE)

Technical-Organizational measures:	
Data Availability:	Data back-up and recovery procedures/ Data base redundancy Appropriate performance of Internet services
Data Integrity:	Intrusion Detection/prevention Systems, Cryptographic authentication mechanisms
Data Confidentiality:	Data encryption should be used both for data "in transit" on networks and data "at rest" in servers. Mechanisms of strong authentications of users (*)
Transparency:	Clear and complete contract
Processing limited to specified purposes	Governance when granting and controlling the access rights to personal data (*) and Related technical measures
Fulfilling the Data Subjects Exercise of Rights:	Contractual obligations for ensuring the Provider (and Subcontractors) support the Client
Data Portability (compatibility with other Providers-Systems)	Pre-contractual assessment and Contractual obligations for ensuring data portability at Contract termination (whatever is the reason)
Accountability: *In IT: ability to establish what an entity did at a certain point in time in the past and how* *In data protection field: the ability to demonstrate that appropriate measures have been taken for the purpose of law compliance*	Evidences of technical and organizational measures are required to demonstrate the existence of a privacy-security Policy and its effective implementation, including any certifications issued by third parties. Necessary appropriate contractual obligations Essential to allow the Client's answers to requests from competent authorities (DPA), as set forth by the law *(eg. "data breach" in the electronic communication services publicly accessible , introduced in Italy with the Legislative Decree 69/12)*

(*) at Provider, Subcontractors,...and Client side

The WP 29 in particular emphasizes the need to perform risk analysis by the Client, since in its role of Controller is directly liable in case of breach of regulatory requirements applicable to the service provided by its Provider. Are evident and reported by the WP 29 the (frequent) difficulties when Clients have less bargaining power than the Providers: objectively it does not appear really feasible for the them to allocate responsibilities and perform controls as required in their role of data Controllers, even taking into account, and this is true also for medium/large Clients, the costs necessary to make real and regular checks of technical, operational and governance nature. In this context the WP 29 points out, as viable, the implementation of programs for appropriate certifications / audits by third parties.

From the approach followed by the WP 29 with this Opinion and even with its recent working document[3] on Binding Corporate Rules applied to the case of data Processors , is becoming clear that the formation of the contractual relationship between Client and Provider of Cloud Computing service is the essential hub of consistent foundation, tuned on the actual needs of the Client and the obligations and liabilities required by law.

A possible successful path could be the proposal of Standard Contractual Clauses for contracts regarding Cloud Computing services. In fact, for such services some specific features seem to be consolidated, including:

- the variety of Providers/ Subcontractors involved and their dynamics during the term of contract with the Client
- the physical location, in principle anywhere in the world, of the servers used for data and applications and organizations (technicians,...), the relevant requirements of synchronization between the systems in view of availability and data integrity
- aspects of security and continuity of service, related both to the Cloud Computing Service Provider and the Internet Service Provider, chosen by the Client
- the relationship often imbalanced in favor of the Provider, which it makes difficult to put into practice the principles of transparency and, above all, the control by the Client in its role as data Controller….

In such a context, the Standard Contract Clauses for Cloud Computing could support in identifying those types of clauses and annexes that absolutely should not miss in a contract of Cloud Computing service. However, recognizing the need to establish predefined criteria of "tailoring" for the necessary adaptations to match the real nature and operational context of a specific service, such rules would provide a base from which to operate in accordance with the principle of transparency, overcoming the difficulties in the presence of unbalance of bargaining power between Client and Provider, providing a systematic and predefined approach for aspects of data transfers abroad (in this case using the appropriate EU decisions) and operating in liason with certification programs / audits in terms of privacy and security . In this regard it is certainly worth mentioning the study activities in place at Queen's University of London, which includes surveys and analysis of a number of actual Cloud Computing contracts, aimed to study their level of adequacy[4]. In Italy at the CSA Italy chapter, the Italian section of the Cloud Security Alliance organization, in the same track it has been activated a study[5] with the purpose to provide suggestions in defining standard rules to set up Cloud Computing contracts,

---

[3] Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules – http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

[4] QMUL Cloud Legal Project - http://www.cloudlegal.ccls.qmul.ac.uk/Research/researchpapers/37188.html

[5] Study coordinated by G.Marcoccio for CSA Italy Chapter - "Cloud Computing Standard Contractual Clauses" Contractual standards as enabling factors for cloud services - presented at the workshop ISACA 'Cloud Computing' in Rome, June 12, 2012