THE RIGHTS AND OBLIGATIONS OF THE MAIN STAKEHOLDERS IN CLOUD COMPUTING SERVICES

PhD. student **Marioara MAXIM**[1]

Abstract

The current technological progress triggers a new approach in the way the personal data are collected, processed or stored, by a multitude of data controllers or processors involved in the chain of trophic relations in the delivering of cloud computing services. In this circumstances, it is our objective to examine the rights and obligations of the contractual parties involved in the cloud computing agreements according to the European Union law and national legislation, and their legal consequences for the data subjects.

Keywords: *cloud computing, data privacy, contract, data protection*

JEL Classification: K12, K23, K30

1. Introduction

In the context of current technological progress which generates new business models rather on short and medium term, and in the view of transition from the digital era of megabyte (1 000 000 000 Bytes) to Exabyte (1 000 000 000 000 000 000 Bytes), the phenomenon of data processing entered into a different dimension, even though the main European Union Directive 95/46/EC remained unchanged from 1995[2]. The most significant risks identified in case of cloud computing, as stated in Opinion no. 05/2012 of Article 29 Data Protection Working Party[3] on Cloud Computing[4] are the lack of control on the data and on the means of processing, but also lack of transparency considering that not only the data subjects, but also the controllers "might not be aware of potential threats and risks and thus cannot take measures they deem appropriate". Despite the fact that there are several opinions issued by the Article 29 Data Protection Working Party (Article 29 Working Party or Working Party), there are still several aspects to be clarified in terms of data subjects' rights or the delimitation of the controller and processor/s obligations, especially in Romania, where the complexity of cloud computing adds to the lack of awareness of the data subjects on the content of data protection regulations.

Taking into account the applicable legislation, the multiple jurisdictions implied by the practical aspects raised by cloud computing services, such as the transfer of data to other UE/EEA countries or even to third countries, different security requirements or different level of data protection in some third countries where the labor cost is lower than in UE/EEA countries, and therefore there is an appetite to outsource services to these countries, our analysis will include into the meaning of the main roll-out models of cloud computing, the rights of the data subjects, rights and obligations of the controller/s (cloud client) and processor/s (cloud service provider), underlining the differences identified in the Romanian legislation that transposes the Directive 95/46/CE.

The main research method is interpretation of the European Union legislation, and the Article 29 Working Party opinions, the national legislation, and the jurisprudence of the European Court of Justice.

---

[1] Marioara Maxim - Law Faculty, Bucharest University, av.maria_maxim@yahoo.com .

[2] Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281/31, 23/11/1995.

[3] The Article 29 Data Privacy Working Party was set up according to Article 29 and 30 of the Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf, last time consulted on 7th of November 2015.

The article does not have the purpose to analyze the aspects related to civil or criminal liabilities, or to go underground of the identified potential conflict in laws, but we will refer to them only in the context of the contractual clauses included in the service contracts or in the commissioning data processing agreements.

Based on the research, we came to the conclusion that specific regulation for protection of individuals with regard to the processing of personal data in cloud computing services would be useful for all stakeholders in terms of ensuring more clarity on the content of their legal relationship, respectively on the contractual frame, grounded on detailed requirements for the contractual clauses, which might be included in a standalone commissioning data processing contract, or in an annex to the cloud computing services contract. The obligations of the cloud service provider shall contain in our opinion an expressly regulated obligation to notify his sub-processors to the competent supervisory authority, irrespective of the fact that it becomes or not a co-controller during the delivery of the cloud computing services. Specific provisions in case of international transfer of data to UE/EEA countries, and third countries will give the opportunity to the national supervisory authority to address the differences in the national legislation identified in our analysis with potential implications in case of international transfer, such as the notification provided by article 29, paragraph 3) of Law no. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data[5].

2. Definition and models of cloud computing

Cloud computing is defined as a "model for enabling ubiquitous, 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. This Cloud model is composed of five essential characteristics, three service models, and four deployment models."[6]

The same definition of cloud computing was considered by Article 29 Working Party in Opinion no. 05/2012 on cloud computing (annex), where the roll-out models of cloud computing include: (i) public cloud, which usually is an infrastructure, hardware and software, owned by a cloud service provider or/and by its sub-contractors, opened to the general public or to a large group of legal entities and individuals, (ii) private cloud, consisting of an infrastructure that is used by a single cloud client, (iii) community cloud, which is a typology of private cloud, but shared with clear partitions by several cloud clients, such as subsidiaries of a multinational company, or even a group of legal entities in the same sector (e.g. public authorities), and (iv) hybrid cloud, that can be a combination of the public cloud with private cloud or a community cloud, ensuring specific firewall between the partitions.

The highest security and data protection risks are presented by the public clouds, as in this case the infrastructure is commonly used by several groups of individuals or legal entities, with direct access from the Internet, and the isolation between the cloud computing solution (e.g. software hosted on the public infrastructure, the applications) containing personal databases, might elude the security barriers causing accidental destruction, or even worse, loss of personal data, unauthorized disclosure to third parties, combined with the impossibility to fully recover the data from the Internet.

In terms of service cloud computing models, NIST and Article 29 Working Party classified them in three groups, as follows:

a) IaaS (Infrastructure as a Service), when a cloud service provider leases its infrastructure to a cloud client in order for the latter to use it from the distance (e.g. virtual remote servers), and deploy platforms, software, operating systems, and applications on it. Typically, the infrastructure providers have huge capabilities of storage and hostage of servers in their data centers. The cloud client does

[5] Published in the Official Romanian Journal Part I., no.790 of December 12th, 2001.

[6] National Institute of Standard and Technology (NIST), Special publication 800-145, 2002, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, last time consulted on 5th of November 2015.

not have the control over the infrastructure, but has it over his own hardware or software connected or downloaded on the leased infrastructure. The infrastructure provider can be also a provider of a publicly available electronic communications service. In such a case the cloud provider has to fulfill also the specific obligations provided by the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[7], and the national legislation[8].

b) PaaS (Platform as a Service), when the cloud service provider leases the hardware capacities (e.g. servers, network, operating systems) to the cloud client in order for the latter to deploy on it his own software and applications, and to be able to access the cloud provider capacities of data storage. In this situation, the cloud client does not have control to the leased platform, but keeps control to the downloaded applications. In this specific service model, the cloud service provider can sub-contract the infrastructure capacities to an infrastructure provider. Even if the platform as such might be a private cloud (a server used by a single legal entity), the infrastructure where is connected is usually a public cloud infrastructure, with isolated partitions for each end-user.

c) SaaS (Software as a Service), when the cloud service provider offers its applications to the cloud client, without being necessary required to download them on their hardware. The applications are hosted on the cloud service provider hardware and can be accessed by the cloud client through its connection to the Internet. The cloud client has no control over the infrastructure (hardware and software) or over the application, except the possibility to customize it according to its needs (configuration settings). The cloud service provider might use sub-contractors for the required hardware and software capabilities, which can be provided under the private, public or a hybrid deployment model.

The five essential characteristics provided by NIST[9] refer to benefits of cloud computing in terms of ensuring (i) *on-demand self-service*, (ii) *broad network access* from the cloud client several platforms, (iii) *resource pooling*, (iv) *rapid elasticity*, and (v) *measured services*, as the cloud client can use the capabilities depending on its needs, and mostly adapt them remotely without being necessary to allocate on site any human or additional resources.

All these characteristics, mainly because of the flexibility offered in terms of distance, capabilities, but also because of the cost efficiency analysis, make the cloud computing services attractive for the companies, but also for the public authorities when it comes to consider the IT needs and resources.

Nevertheless, when the cloud computing services are used for processing personal data, or when the developed cloud computing solutions include personal data, the data protection requirements have to be considered, and the balance between the economic interests of the cloud clients and the cloud service providers on one hand and the protection of fundamental rights of the data subjects on the other hand has to be ensured and continuously fine-tuned.

In the following sections, we will examine the legal frame which has to be considered by the controllers, in their capacity of cloud clients and by their processors, even from the design phase of such cloud computing solutions.

3. General legal framework applicable in Romania

As the cloud computing solutions include personal data, either by collecting, accessing or storing them, the legislation in the matter of data privacy and data protection is applicable in terms of security requirements and data protection principles.

---

[7] Published in the Official Journal of the European Union L 201/37, of July 31st, 2002.

[8] Law no.506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, published in the Official Journal of Romania, Part I, no. 1101 of November 25th, 2004.

[9] NIST, Special publication 800-145, 2002, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, p. 2, and last time consulted on 5th of November 2015.

Consequently, whenever the client cloud decides to acquire or outsource IT resources, which process personal data, he has to consider as well the following European Unions and national legislation:

i) Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46), transposed by Romanian Law no. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data;

ii) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive 2002/58), transposed by Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as amended[10];

iii) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation no. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws[11].

iv) Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council[12];

v) Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, Set II, under Directive 95/46/EC[13];

vi) Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC[14]

vii) Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries[15];

viii) The secondary legislation issued by the Romanian national supervisory authority, respectively *Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP)[16], such as Decision no 95/2008 regarding the notification template as provided by the Law 677/2001;

ix) Ombudsman Order no. 52/2002 regarding the minimum security requirements applicable for the personal data processing[17].

In its capacity of ensuring harmonization in the implementation of the Directive 95/46 at the level of the European Union by its member states, the Article 29 Working Party issued several opinions and recommendation for the interpretation of the relevant notions for cloud computing, such as "personal data"[18], Opinion 1/2010 on the concepts of "controller" and "processor"[19] "processing

---

[10] Law no. 235/2015 for the amendment of Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, Published in the Official Journal of Romania, Part I, no. 767 of October, 14th, 2015

[11] Published in the Official Journal of the European Union, L 337/11 of December 18th, 2009.

[12] [12] Published in the Official Journal of the European Union no. L 181/19, of February 2nd, 2010.

[13] Published in Published in the Official Journal of the European Union no. L 173/2, of July, 7th, 2001.

[14] Published in Official Journal of the European Union no. L 6/52, of January 10th, 2002.

[15] Published in Official Journal of the European Union no. L 385/74, of December 29, 2004.

[16] The ANSPDCP's decisions are posted on the authority's site, at http://www.dataprotection.ro, last time consulted on 9th of November, 2015.

[17] http://www.dataprotection.ro/servlet/ViewDocument?id=8, last time consulted on 5th of November, 2015.

[18] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, last time consulted on 9th of November, 2015.

[19] Article 29 Data Protection Working Party 29, Opinion 1/2010 on the concepts of controller and processor, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, last time consulted on 9th of November, 2015.

of location data for value added services"[20], "legitimate interest of the data controller"[21], "online behavioral advertising"[22], "applicable law"[23], "consent"[24], etc. Besides these opinions that are of relevance in any category of personal data processing, as above-mentioned, the Working Party issued two opinions of specific applicability for the cloud computing services: Opinion no. 5/2012 on cloud computing and Opinion 2/2015 on C-SIG Code of Conduct on Cloud Computing[25], the latter being significant in underlining the fact that the previous Working Party's recommendations remained valid.

It is to be mentioned that the legislation on data protection or cloud computing cannot be applied in an isolated manner and has to be corroborated with the general legal provisions in areas such as civil law, administrative law, criminal law, international public law. For instance, when the consent of the data subject is required, in order to be able to examine its validity, the interpreter needs to check the legal conditions provided by the national law. In case of Romania, for instance, the consent of the data subject will have to fulfill the requirements provided by article 1204-1224 from the Romanian Civil Code. The same rules applies in case of termination of the contract, depending on the national law applicable to the personal data commissioning agreement signed between the cloud service provider and cloud client.

Nonetheless, if there is a conflict between the Romanian Civil Code and the European Union law, the priority is given to the provisions of the latter, irrespective of the capacity or the statute of the parties involved in the judicial relationship[26]. This means, that if there is any conflict between the national legislation and the European Union law in the field of data protection, we need to apply in principle the European Union law. The restrictions and the derogations from the Directive 95/46 have to be examined in the context and the permission expressly provided by the Directive 95/46, as for instance in case of cross-border transfer of data to third parties (article 26).

4. Data subject's rights

We can refer to the data subject's rights in the meaning of the data protection legislation whenever the cloud computing services include processing of personal data. According to the Article 2, letter a) of Directive 95/46, "personal data" is represented by "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". The same definition, without any difference is provided by the Law no. 677/2001, in article 3).

The definition is very large, and includes thus not only the information that directly can identify a person, but also the information that, along with other pieces of information, can make the connection to an individual. In this context, in terms of cloud computing, we shall include in the meaning of personal data for instance: the name and the address of the person, the work place, the number of his/her employment number, the IP (Internet Protocol address), irrespective of its fix or

---

[20] Article 29 Data Protection Working Party 29, Opinion on the use of location data with a view to providing value added services, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf, last time consulted on 9th of November, 2015.

[21] Article 29 Working Party 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, last time consulted on 9th of November, 2015.

[22] Article 29 Working Party, Opinion 2/2010 on online behavioral advertising, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf, last time consulted on 9th of November, 2015

[23] Article 29 Working Party, Opinion 8/2010 on applicable law, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf, last time consulted on 9th of November, 2015.

[24] Article 29 Working Party 29, Opinion 15/2011 on the definition of consent, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, last time consulted on 9th of November, 2015.

[25] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf, last time consulted on 9th of November, 2015.

[26] Article 5, Law no. 287/2009 regarding the Civil Code, republished in Official Journal of Romania, Part I, no. 505, 15th of July, 2011.

mobile characteristics, the identity number of hand sets, the geo-location information, the serial number of his/her identity card, his preferences (in case of profiling), etc.

According to article 5 of the Law no. 677/2001 the processing of personal data is allowed if the data subject gives his/her consent in an "express and unequivocal" manner. This means that the Romanian legislator adopted undoubtedly an opt-in solution, respectively the data subject has to agree expressly to the processing of his/her data before any stage of the processing takes place. An opt-out solution is not possible in this context, including in the cloud computing services, exceptions being strictly provided by the law. Still, as we will observe at a systematic examination, the text used by the Romanian law is not so clear and leaves room of interpretation which is not always predictable for the cloud service providers (processors) or for the cloud clients (controllers), and neither for the data subjects.

Thus, the Directive 95/46 sets for in article 7, letter a) that "Member States shall provide that personal data may be processed only if: a) the data subject has *unambiguously* given his consent; or b)…" The same terminology is used in article 26 of the Directive 95/46, which sets forth the exceptions from the principle applied for the transfer of personal data to third countries, stating that the data subject has to give his/her consent unambiguously to the proposed transfer. The difference comes in article 8 of the Directive 95/46 regarding the processing of special personal data, when the processing of the data is legitimate if the data subject has given his *explicit consent* to the processing of those data.

By comparison, in the Law 677/2001, the law maker provided a different concept on consent, as the article 5 sets forth that the processing of personal data "may be carried out only if the data subject has given his/her *express and unequivocal consent* for that processing".

In article 7 and 8) of the Law 677/2001 regulating the processing of special categories of data and the personal identification number (e.g. CNP), is stated as an exception from the general rule above-mentioned that the processing of such data is possible "when the data subject has *expressly given his/her consent* for such data processing". Finally the Law no. 677/2001, in article 30 transposed the article 26, letter a) of the Directive 95/46 with some distinctions, providing that the transfer of the personal data in third countries is possible if the data subject gives *explicitly his/her consent*. Moreover, in the second sentence of the same letter, it is provided that in case of processing of personal data set forth in article 7) and 8) before mentioned, the consent has to be given by the data subject in *written*.

Interpreting this text in the light of the general rules provided by the Romanian Civil Code in article 1204, in the sense that the consent has to be expressed freely, genuinely and knowledgeable, we can conclude that the data subject can give his/her consent in writing, by electronical means (e.g. accepting the terms and conditions provided by various applications) or even verbally, providing that the consent was expressed freely, unequivocally and knowledgeable. The only exception provided by the Romanian legislation might be in case of transfer of personal data of special categories (article 7) and personal identification number (article 8), or even the judicial records (article 10), when the consent has to be given in writing. Theoretically, the consent can be given in an electronic format, but then the evidence has to be undoubtedly provided (e.g. electronical signature), which in the end could represent an additional effort, or an impossible mission, for the controller/cloud client and the cloud service providers. Nonetheless, considering the technological progress and the development of the digital solutions, including the cloud computing services, the approach, at least in the Romanian text has to be reviewed and up-dated to the European Union law, or to the new European Union General Data Protection Regulation (GDPR) currently under discussions, which expressly provides in Recital 25, the possibility of the data subject to express his/her consent by "ticking a box when visiting an Internet website[27]". It is to be mentioned, that the principle of opt-in is maintained by the new GDPR, as the same recitals establishes that the passive attitude of the data subject or the mere use of the services do not represent a consent in the meaning of the regulation.

[27]http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-20140212+0+DOC+XML+V0//EN, last consulted on 8th of November, 2015

In order for the consent to be valid, it has to be free of any error (article 1206 of the Romanian Civil Code), and moreover has to be given in a knowledgeable manner. This is in line with Section IV of Directive 95/46 transposed as such by article 12 of Law no. 677/2001, as the data subject has the right to be informed mainly about the following aspects:

i) the identity of the data controller and its representative (e.g. in cases when the data controller does not have an establishment in the member state);
ii) the purpose of the processing of personal data, which has to be presented explicit. The purpose has to be legitimate, and not forbidden by the law (e.g. criminal offences databases by controllers that do not have such competences by the law);
iii) the personal data to be processed, including the special categories, as the case may be;
iv) the identification of the recipients[28], or the categories of recipients of the data;
v) the data subjects specific right towards the processing: the right to access his/her personal data, to have them corrected or erased or the right to object.

The obligation to inform the data subject has to be fulfilled by the controller, meaning the cloud client, even if the data are not directly obtained from the data subject, and it has to be observed before the first disclosure to a third party takes place, at latest. The exception must be applicable only in cases where the disclosure is required by a law enforcement authority and only if such disclosure to the data subject is prohibited expressly by the law.

The data subject whose data are processed in a cloud computing services has preserved the rights provided by Directive 95/46, as follows:

i) the right to access the data at a reasonable period (1 year, according to paragraph 1, article 13 of Law 677/2001), without any expense, and without any delay (the cloud client has to reply to the data subject's request in maximum 15 days, according to paragraph 3 of the same article);
ii) the right to intervene on the data by asking, without any cost for the data subject, the rectification, amendment, erasure, or blocking the data or their anonymization, as they are obsolete or are dated in the past, being not necessary for the purpose of their initial collection or publication, as established by the European Court of Justice (ECJ) in the case of Google Spain vs. Mario Costeja González[29];
iii) the right to object, at any time, on the grounds of legitimate reasons considering his/her particular situation. The controller has to consider the data subject request in maximum 15 days, as the data subject has the correlative right to receive an answer in the specified term. Nevertheless, it has to be mentioned that in case of special categories of data, and the personal numeric code, the data subject has no obligation to justify his/her own option to object to such processing. Consequently, the controller has to comply to the data subject's request;
iv) the right not to be subject to a decision grounded on a solely automated processing, if such decision produces legal effects, except in the case when it is in relation with a conclusion of a contract, and the contract materialized, or in case the data subject has the right to express his/her opinion, and consequently the decision is revised.
v) the right to appeal to a court, when the data subject considers that his/her rights have not been properly observed by the controller (cloud client), or by the processor (cloud service provider), having thus the possibility to address his complaint to both parties, remaining in the capacity of the controller to prove that it did not breach the law.

For the exercise of his/her rights, the data subject may address directly to the cloud client/controller, who needs the full cooperation of the cloud service provider/processor, and its sub-contractors to fulfill its obligations in due time.

---

[28] Article 3, letter h) of Law 677/2001, defines the "recipient" as "any natural or legal person, of private or public law, including public authorities, institutions and their local bodies, to whom the data are disclosed, regardless of the fact that it is a third party or not; the public authorities which receive data in accordance with a special type of inquiry competence will not be considered consignees".

[29] European Court of Justice, Case C-131/12, Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos and Mario Costeja González, judgment of the court (Grand Chamber) of May 13th, 2014, http://curia.europa.eu/juris/document/ document_print.jsf?doclang=EN&docid=152065, last consulted on 5th of November, 2015.

5. Rights and obligations of the cloud client/controller and cloud service provider/processor/ sub-processors

As in the cloud computing, the chain of data processing involves multiple cloud services providers, in their capacity of processors and sub-processors, it is crucial for the controller/cloud client to conclude very clear and comprehensive contracts – service agreement, service level agreement, and commissioning data processing agreement with its cloud service provider, where the rights and obligations of each party are being of significant importance for the delimitation of the parties responsibilities and liability, but also for reaching an efficient level of data protection.

5.1. Cloud Client/Controller's rights and obligations.

The cloud client has all the obligations provided by the Directive 96/54 and the Law no. 677/2001 for the controller. As said, the cloud client is the controller, and has to ensure that all the data subjects' right are fully observed.

Thus, the cloud client, in his capacity of controller has first the obligation to perform, in-house or by an external expert, a comprehensive risk assessment of the cloud computing solutions when he decides to outsource the IT services to a cloud service provider. The matrix of risks has to cover the data protection requirements and the security requirements as they are established through by the Directive 95/46, Romanian Law 677/2001, and the Ombudsman Order no. 52/2002 regarding the minimum security requirements applicable for the personal data processing.

From this perspective, the first obligation of the cloud client/data controller is to ensure that the cloud service provider implements the appropriate technical and organizational measures to guarantee a level of protection of personal data in line with the legal requirements.

The controller has the right to run an audit on the sites of the processor or its sub-processor/s, including all the locations where the servers are hosted, or the personal data are processed. The obligation is maintained on the entire contractual period. In case of irregularities identified either by the controller or by the national supervisory authority, the cloud service provider has the obligation to fix them, which brings to our attention the importance of establishing in the contract the obligation of the processor to solve and implement the required security measures on its own cost.

The controller has the right to be informed by the processor and the right to approve or decline the employment of sub-processors. Nevertheless, the cloud client can approve the possibility of sub-contracting, and even the sub-processors from the beginning, through the contract signed with the processor, or later on by signing an addendum to the contract, or by signing a tripartite contract.

Considering that the controller has the correlative obligations to ensure the data processing fulfills the criteria of a legitimate data processing, as for instance the data subjects consented to the processing of their personal data, in full acknowledgment of the conditions in which their data are processed, and for a specific purpose, as presented to them, the controller has the right to instruct the cloud service provider on the way the personal data are accessed, used or stored. Irrespective of the applicable exceptions from the rule of consent, provided by the articles 5, 7, 8, 9 and 10 of the Law no. 677/2001 that are to be considered, on a case by case analysis, the processor has the obligation to act only based on the controller instructions. It is to be mentioned that in case the processor exceeds the specific purpose of processing, for instance by using the personal data for direct or indirect marketing, profiling, big data projects, etc, the processor becomes for that specific processing a controller with all the legal consequences provided by the data protection legislation.

According to the article 17, paragraph 3) of Directive 95/46, the controller has the obligation to conclude a contract or a legal act binding the processor to safeguard at least the obligation of the cloud service provider/processor to roll-out the technical and organizational measures to guarantee the security of the data, and the obligation for the processor to process the data only based on the instructions received from the controller. As mentioned by the Article 29 Working Party, the

controller and the processor, part of the same group of companies, can apply between themselves binding corporate rules. Nevertheless, by comparison with article 17, paragraph 3 of the Directive 95/46, the Romanian Law no. 677/2001 stipulates in article 20, paragraph 5, that the parties have to conclude a written contract for safeguarding the security measures and the right of the controller to give mandatory instructions to the cloud service providers in terms of data processing, eliminating thus the option referred to *any other legal binding act* for the processor toward the controller. Still, it has to be mentioned that the Romanian supervisory authority accepts the concept of the binding corporate rules between the companies of the same group, as a base for intra-group commissioning data processing. Regarding the practice of the big cloud service providers to impose over the cloud client their own pre-drafted contracts without a real possibility of the cloud client to amend them, especially in case of small and medium enterprises with low power of negotiation, we consider that in the field of data protection the adhesion contracts, as regulated by article 1175 of Romanian Civil Code[30] should not be in principle appropriate, and seems to be in conflict with the scope of the legal obligations assigned by the law to the cloud client, as it has the role of the controller.

The controller has also the obligation to notify the data processing to the Romanian supervisory authority, by filling in the on-line notification with the required information, as the category of personal data, purpose of the processing, the means, the security and organizational measures, the methods of obtaining the data subject's consent, the information of the data subject, the location of the data processing, etc. It is our opinion that in case of cloud computing services, the controller by the way of describing the processing of data might refer to the cloud computing even if the notification template does not provide a special requirement for such information. According to the article 29, paragraph 3) of Law 677/2001, all the data processing performed internationally have to be notified to ANSPDCP. Therefore, even if one specific data processing would be exempted from the notification (e.g. the processing of employees' personal data done for the fulfilment of the employer obligations provided by the labor law), in case the data processing is done outside Romanian borders, the controller has the obligation to notify the data processing, including the transfer to EU/EEA. The notification has to be afterwards submitted also in a hard copy to the ANSPDCP. The notification has to be always submitted before the processing takes place.

When it comes to third countries, whose level of data protection has not been considered adequate either by ANSPDCP or by the Commission, the controller has the obligation to apply for the authorization. In such a case, the controller has to provide appropriate security measures, and sufficient guaranties on data protection, governed by a written contract concluded between the parties with the observation of the standard contractual clauses adopted by the Commission.

5.2. Cloud Service Provider/Processor's rights and obligations

According to the Directive 95/46, article 2, the concept of *processor* includes "any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". Likewise, the *processing of personal* data includes "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage , adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". By the interpretation of these two definitions, it naturally results that whenever the cloud computing solution includes one of the operations listed in the concept of processing of personal data, done by the cloud service provider on behalf of the controller, the cloud service provider becomes also a data processor, with all the legal effects related to such capacity.

Hence, the cloud service provider will have the obligation to conclude a written contract with the controller, as said before, to safeguard the security and organizational measures that the processor has to implement and to guarantee that the measures will be implemented as such, and even up-dated

[30] "The adhesion contract is defined as a contract whose essential clauses are either imposed or drafted by one of the parties, for itself or based on its own instructions, the other party could not have other option than to accept them, as such.

to the new digital environment, to the foreseen threats, so that to be able to prevent any data loss, or unauthorized disclosure.

The security procedures includes those technical and organizational measures provided by Ombudsmen Order no. 52/2002, but also the specific requests to the cloud service provider underlined by the Working Party in its opinions on cloud computing, as follows:

i) *Availability to the processed data* must be guaranteed at any time, based on the controller instructions. This means that the cloud provider shall ensure the access of the controller to the infrastructure, and the fact that the potential accidental disconnections are prevented by appropriate means. Also, the cloud service provider shall put in place back-up solutions in order to diminish as much as possible the potential damage of the controller or data subjects from a potential disconnection or accidental loss of data. The controller shall not give up entirely to the access to its databases, or to the server administration settings, if possible. In this respect, the contract shall provide exactly the responsibility of the cloud service provider to allow the controller access to the databases, and the related conditions.

ii) *Integrity of the data*. It has to be maintained by proper security measures suitable for preventing any alteration of the data during their collection, organization, transmission, or storage, or any other operation that falls under the definition of data processing. The Working Party recommends the usage of cryptographic authentication methods, such as the electronic signature of the authorized users.

iii) *Confidentiality of the data and isolation of the data*. These are general obligations that have to be fulfilled in principle when processing personal data, not only by the means of a cloud computing service, but in all the cases when the controller uses centralized filing systems. Nevertheless, the cloud service provider has the obligation to set up its cloud infrastructure on a basis of encryption mechanisms of the personal data, and establish clear partitions to avoid unauthorized dissemination of the data to third parties, or to the other cloud clients that leased the infrastructure of the same cloud service provider. The confidentiality of data shall be ensured with encryption solutions before the data are sent to cloud, or even during the performance of the contract if the data processing does not require personal data to be accessed in its original format (e.g. profiling). In case the cloud service provider is also a provider for the public electronical communication services, as for instance the telecommunication providers (mobile, fix, internet, included value added services), the obligations provided by article 4 of the Romanian Law no.506/2004, that transposes article 5 of the Directive 2002/58, have to be also fulfilled by the cloud service provider (e.g. prevention of the unlawful interception), while the controller has to ensure the fulfillment of the specific conditions provided for the data processing (e.g. to obtain the express and prior consent of the data subject in case of value added services).

iv) *Portability of the data*. It is the controller right to migrate to a different cloud computing solution, respectively to change the cloud service provider with another provider, or even to insource the IT resources, if the case may be. Consequently, the cloud service provider has to guarantee that the personal data can be migrated to another infrastructure, or platform, based on controller instructions. The cloud client has to check from the beginning the possibility of the cloud computing solution to provide portability and migration of the personal data, without any alteration of the data.

v) *Accountability* refers to the obligation of the cloud service provider to ensure, by implementing specific technical and organizational measures, that the controller and the data subjects can have access to the history of the processing of personal data, so that to be able to check if there have been any abusive or unauthorized access to the data, and in such a case to see exactly when did it happen, by whom the data have been altered, etc, and in general all the operations done on the infrastructure leased by the cloud client.

vi) *Intervenability* on the data, based on the controller request, grounded by the data subjects' right to have their personal data rectified, erased or blocked. Accordingly, the cloud service

provider has the obligation to inform immediately the cloud client in case the data subject requests to have his/her data erased, blocked or rectified, being the responsibility of the cloud client to analyze such a request, and the obligation of the processor / cloud service provider to act only based on the controller instructions. Nevertheless, the cloud service provider has to cooperate with the cloud client from the design phase in certain conditions, and during the performance of the contract to ensure the implementation of the technical measures capable to comply with the instructions of the controller in case the data have to be blocked, erased or altered. Following the same principle, the same technical possibility has to be implemented towards the back-up solutions, as the data subject has the right to have his/her data erased or altered from all the related filling systems.

The cloud service provider has the obligation to inform the cloud client about all the sub-processors involved in the processing chain and give the possibility to the cloud client to approve the involvement of any sub-contractor that might have access to the personal databases. If the cloud client denies the involvement of a specific sub-contractor, the cloud service provider has the obligation to refrain from employing it. However, the service contract, or the commissioning data processing agreement have to establish the consequences of such denial.

The cloud service provider has to notify, on behalf of the controller, to the competent national supervisory authority the sub-processors, the circumstances of the data processing and the location of the processing (e.g. data centers, servers, or any other infrastructure).

The processor has the obligation to give access to the controller to review and perform audits on site, to all locations, including those owned by its sub-contractors.

The cloud service provider has the obligation to inform immediately the cloud client in case of a breach of data protection, as the controller has the obligation to report it the national supervisory authority in certain cases[31].

All the obligations provided by the law to the processor has to be mirrored within the contract signed between the processor and its sub-contractors/sub-processors, as the processor is liable towards the controller for any loss caused by sub-processors.

In case of supervisory authority investigations, the processor and its sub-processors have the obligation to cooperate and convey the information required by the authority, and implement them technical and organizational measures to solve the potential irregularities.

Finally, following the termination of the service contract, the cloud service provider has the obligation to hand over to the cloud client all the personal data bases, or destroy / anonymize them, as instructed by the latter.

6. International transfer of personal data

6.1. Notification and authorization procedure.

As the cloud computing services involve most of the time infrastructure located in a different country, in EU/EEA or in third countries, the cross-border transfer of data has to comply with the requirements provided by article 29 of the Romanian Law no. 677/2001, in terms of authorization or notification[32].

Henceforth, according with paragraph 3) of article 29, the international transfer of data has to be notified to the Romanian supervisory authority in all the cases, including when the transfer is done within UE/EEA.

---

[31] Commission Regulation no. 611/2013 of 24th June, 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications, published in the Official Journal of the European Union L 173/2, of June 26th, 2013.

[32] The content of the notification is provided by article 22 of Law no 677/2001, and the Notification Guidance posted in the ANSPDCP site: http://www.dataprotection.ro/?page=ghid_notificare, last time consulted on 5th of November, 2015;

Actually the Chapter VII of the Romanian Law 677/2001 does not keep the distinction mentioned in the Chapter IV of the Directive, namely the transfer of personal data to third countries, referring thus to all cross-border transfers of personal data.

Nonetheless, when it comes to the transfer of the data to third countries, the Romanian Law 677/2001 maintains the same principles and conditions provided by the Directive 95/46, being mandatory for a controller to apply for an authorization, unless the particular third country has already been exempted by the ANSPDCP or by the Commission on the grounds of having proved an adequate level of data protection. In these latter cases, international transfer has to be only notified.

In case of the authorization process, the controller or the processor on behalf of the controller has to submit to the supervisory authority the concluded contract in a written format, which has to include the standard contractual clauses regulated by the Commission, in the decisions mentioned in Section II of the study. The additional clauses meant to strengthen the goals of data protection or security are allowed, providing that they are not conflicting the standard contractual clauses.

It has to be mentioned that the international transfers to US cloud service providers, currently requires authorization of ANSPDCP before the data processing takes place, following the European Court of Justice judgement in the case of Maximillian Schrems vs. Data Protection Commissioner[33] which decides that Decision no. 2000/520[34], on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, is invalid.

All the same, the cloud controller has to consider that the supervisory authority has the right to run a preliminary control following the notification of a data processing, including in case of international transfer of data. Henceforth, article 23, paragraph 3) of the Romanian Law no. 677/2001, sets forth that the processing of data can begin, if the supervisory authority did not inform the controller in 5 days from the date of submission that the supervisory authority will perform a preliminary control. In this respect, on a logical interpretation, we might be tempted to consider that the notification could be done in advance with minimum 5 days, but such interpretation would contravene the reality, as the authority has also the right to ask the controller to review the notification following specific recommendations.

In case of authorization, the regulation does not provide any deadline, just the principle to have it before the data processing takes place. The same diligent assessment has to be applied. Even if we shall consider the general term of replying in case of Romanian authorities (30 days from the date of application), the preliminary review might take more time, as the ANSPDCP has the right to ask for additional information and clarifications.

6.2. Applicable law in case of cross-border transfer.

Considering that in case of cloud computing, there are multiple controller/s and processors/sub-processors, it is of significant importance for the parties to establish within the concluded contract the applicable law for the data processing. As a principle, the national data protection law may be applied outside the national jurisdiction of the supervisory authority or internal courts.

According to the Opinion 8/2010 of Article 29 Working Party, Section II.2.b), "the main criteria in determining the applicable law are the location of the establishment of the controller and the location of the means or equipment being used when the controller is established outside the EEA", the latter criterion ensuring that no illegitimate or abusive data processing takes place in UE/EEA. In the same section, the Working Party conclude upon the fact that "the nationality or place

[33] European Court of Justice, Case – 362/14, Maximillian Schrems vs. data Protection Commissioner, judgement of the Grand Chamber of October 6th, 2015, http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd94c86bb9731647b3af97f379845710ee.e34KaxiLc3qMb40Rch0SaxuRc3n0?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=70911, last time consulted on 9th of November, 2015

[34] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML, last time consulted on 9th of November, 2015.

of habitual residence of data subjects" and "the physical location of the personal data" are not decisive for the purpose of establishing which national law in applicable.

Thus, according to article 4 of the Directive 95/46[35], the principles to establish the applicable law in case of cloud computing data processing, are the following:

The applicable law is firstly the national law of the member state where the controller has an establishment, "and the processing takes place in the context of the activities of the said establishment or another establishment in the same member state". Same principle is provided by article 2, paragraph 2) of Romanian Law no.677/2001. This means that if the controller has an establishment in Romania and the data processing is done in Romania in the context of the activities performed by the controller's establishment/s in Romania, the applicable law for the data processing is the Romanian law.

If we are not in the situation provided at the above paragraph, article 4, letter b) of the Directive 95/46 sets forth that if the data processing takes place in the context of the activities run by an establishment on the territory of other member state, the applicable law will be the national law of the other member state, and not of the state where the processing takes place. This means that if a Romanian company has an establishment in Germany (e.g. subsidiary), the data processing being performed in Romania, but in the context of the activities performed by the German establishment, the applicable law is the German data protection law, and not the Romanian Law no. 677/2001. Contrary to the article 4, letter b) of Directive 95/46, the Romanian Law no. 677/2001 sets in article 2, letter c) that the Romanian law is applicable also to "personal data processing, carried out within the activities of data controllers not established in Romania, by using any means on Romanian territory, unless these means are only used for transiting the processed personal data through Romanian territory". Practically, the Romanian legislator transposed the letter c) of the article 4 of the Directive 95/46 in a restrictive perspective, referring to the controller outside Romania, and not outside EU. This means in theory that in the example above-mentioned, the applicable law would be Romanian Law no. 677/2001, even if according to Directive 95/46, the applicable law should be the German law.

This inconsistency between the two provisions has to be addressed by the Romanian legislator, as the Romanian text of article 2, letter c) contravenes to the EU data protection goals, as stated in Recital 1) of the Directive 95/46.

Nonetheless, in case of a litigation between the parties, if the parties did not mention the applicable law in the contract, any of them, either the controller or the processor or the data subject can claim the applicability of a foreign law, if the data are processed by a controller whose establishment is in another member state than Romania, and the processing is done in that member state for the activities carried on in the geographical territory of that member state, or even for the situation when the data are processed in Romania, but for the benefit or in the context of the activity performed by the establishments on the other member state (article 5 of the Romanian Civil Code). In addition, according to the Romanian Civil Procedural Code (article 22), the courts can apply and bring into the parties debate the applicability of the foreign law.

7. Conclusion

As a conclusion, the cloud computing services, as they are currently defined, and as their characteristics revealed us, comprise most of the time personal data processing. The chain of

[35] Article 4, paragraph 1) "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) 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; (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, 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."

processing is complex and involves several operations that fall under the concepts of "personal data" and "data processing" as they are regulated by the Directive 95/46 and the Romanian Law no. 677/2001. Therefore, the cloud client, respectively the controller has to fulfill its obligations towards the data subjects, and ensure transparency, security measures, and a genuine possibility for data subjects to exercise their rights, especially the right of access to the personal data, to be fully informed, to have the data corrected, erased or blocked, and not be subject of an abuse and excessive data processing. In fulfilling its obligations, the controller is fully dependent on the processor/s, and multiple sub-processors. In this respects, it is of a high importance to safeguard the rights of the data subjects and the obligations of the controllers and the processors through real technical and organizational measures, and clear contractual clauses. The standard contractual clauses, or ad-hoc contracts may serve the purpose, as based on the Romanian Law, the main instrument resides in a written contract, without an express permission for other binding acts towards processors.

It is our opinion that besides the revision of the Romanian Law no.677/2001, the Ombudsman Order 52/2002 on the minimum security requirements applicable for the personal data processing, needs to be aligned with the Directive 95/46, and with the specific requirements of data processing in the current technological environment.

Considering that currently the proposal of the new EU General Data Protection Regulation is planned to be adopted by 2016, with direct effects to the member states after two years of transition, we believe that a national guidance on cloud computing services might serve as well the purpose of clarification of the data processing by electronical means, and can pass the balancing test between the economic legitimate interests of the cloud clients/controllers on one hand, and the protection of personal data of the individuals on the other hand.

Bibliography

1. Directive no. 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data Official Journal L 281/31, 23.11.1995.
2. National Institute of Standard and Technology (NIST) Special Publication 800-145, 2002 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf consulted last time on November 5 2015.
3. Law 506/2004 concerning the processing of personal data and privacy in the electronic communications sector, published in the Official Gazette of Romania, Part I, no. 1101 of November 25, 2004.
4. NIST Special Publication 800-145, 2002 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, p. 2, last consulted on November 5, 2015.
5. Law 235/2015 amending and supplementing Law no. 506/2004 concerning the processing of personal data and privacy in the electronic communications sector, published in the Official Gazette of Romania, Part I, no. 767 of 14 October 2015.
6. Law no. 287/2009, the Civil Code, republished in the Official Gazette of Romania, Part I, no. 505 15 July 2011.
7. Regulation (EC) no. 611/2013 of 24 June 2013 on measures applicable breach notification of personal data under Directive 2002/58 / EC of the European Parliament and of the Council on privacy and electronic communications, published in the Official Journal of the European Union no. L 173/2 of 26 July 2013.