Certain Data Privacy Issues in the Cloud Computing Environment from a Macedonian Perspective – A Comparative Analysis of the Legislation

Ana Pepeljugoska*

Table of Contents

A. Introduction 109
B. The Notion of Cloud Data Base 111
C. Data Privacy Issues and Problems 113
I. The European Union Regulatory Framework 114
1. Development of the Data Privacy Law 114
2. The Reform of the Data Privacy Law 119
3. Future Challenges 122
II. The Regulatory Framework of the Republic of Macedonia 124
1. Overview of the Data Privacy Legislation 124
2. Significant Provisions of the Data Privacy Act for Cloud Computing 125
D. Conclusion 130

A. Introduction

The internet, social media and digital technologies are transforming our life. The latest big innovation in the IT industry is the cloud computing, which intends to maximize the use of the internet. Cloud computing represents a huge paradigm shift in the way that computing power is provided to organizations and to end users. Rather than procuring their own hardware and software licenses, organizations now can choose which parts or layers of the computing architecture to own, and which to rent, and on what terms and conditions. In this way the computing power may be offered more economically and with higher flexibility through a level playing field of providers offering computing services out of their "cloud" infrastructures, typically through Internet connectivity.

The potential benefits of cloud computing are enormous. They include greater efficiencies for organizations to customize and rapidly scale their systems for particular needs, expanded access to computational capabilities, better collaboration through

* Ana Pepeljugoska LL.M., Ph.D. Candidate University Ss. Cyril and Methodius Faculty of Law Justinianus Primus Skopje, Attorney at law.

"anywhere, anytime" access to IT for users located around the world, and new opportunities for innovation as developers' flock to this latest computing paradigm.

Unfortunately, despite the fact that we accepted the advantages in our world of communications, we must not forget the potential dangerousness which are coming together with the development of new technologies. The usage of cloud computing will most likely involve certain data privacy concerns. The main reason for this is the fact that the basic principles of cloud computing enable storage of all kinds of data which may cause certain problems in the data protection context. The fact that more data is constantly linking to individual persons, triggers the debate concerning the data protection requirements in the cloud transactions.[1] It also emphasizes the need to finally define the status of the anonymized, pseudo anonymized and encrypted data in the "personal data" concept.

Following the destiny of the other technological innovation before, it has not been easy to determine and bring the cloud uses within the existing legal framework. The European Union, at least, has attempted to ensure harmonization of the data privacy framework of its member states, however does it really address the cloud computing problem? European data protection law is location focused, assuming physical movement of data which makes it difficult to reconcile some of its provisions with the notion of cloud computing. Having recognized this, the data protection reform and the new rules will address the lack of certain cloud specific issues. It is expected to finally define the broad concept of "personal data" and thus to strengthen citizen's rights such as the right to be forgotten, the right to data portability and the right to be informed of personal data breaches. On the other hand, the data protection law of the Republic of Macedonia is also location focused and it is treating the movement of data from one physical place to another. This basically means that it also does not cover the location-agnostic concept of the cloud. It also makes no reference or precise interpretation of the term "personal data" and what falls out of this scope. However, there is no upcoming reform, nor any proposal as to amend the existing rules.

Taking into consideration the above mentioned, the aim of this paper is to identify the crucial data privacy concepts (anonymized, pseudo anonymized and encrypted data) that may raise certain issues in the cloud computing environment. Furthermore, this paper will make brief analysis of the existing legal regulations in the European Union and in the Republic of Macedonia and it will present an overview of the forthcoming EU reform. It is hoped that this reform will properly address all issues concerning the status of the anonymized, pseudo anonymized and encrypted data, the possibility of their collection, processing and transfer in the "clouds". Additionally, this paper will show that this or a similar reform should also affect the legislation of the Republic Macedonia so as to fill in some of the missing links.

1 *Yoran*, Cloud Computing and Data Residency Laws, Sys-con Media, www.sys-con.com/node/2660874 (25/1/2016).

B. The Notion of Cloud Data Base

The US National Institute of Science and Technology's definition of cloud computing declares that cloud computing is a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort" of the cloud service provider.[2] It has four essential characteristics:

- On-demand self-service: a client administrator can provision computing capabilities automatically, without requiring human interaction with the service provider; Broad network access: variety of client platforms (PCs, tablets, smartphones) may access the computing capabilities over the network;
- Resource pooling: the cloud service provider's resources are pooled to serve multiple consumers using a multi-tenant model, when different physical and virtual resources are dynamically assigned according to consumer demand;
- Rapid elasticity: capabilities can scale rapidly up and down so they appear to be unlimited to the consumer, and to be available at any time;
- Measured service: resource usage has metering capability while providing transparency for both the provider and consumer of the utilized service.[3]

In light of the proposed characteristics the cloud bases can be classified in several deployment categories. The first deployment category of the cloud base is the private cloud. It is defined as for exclusive use by a single organization or enterprise comprising multiple user groups (e.g. business units). It may be owned, managed, and operated by the organization or by a third party. The second deployment category is the public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Resources are externally hosted and are dynamically provisioned and typically billed according to a structured price list. And finally the third deployment category is the hybrid cloud. The cloud infrastructure is a composition of private and public clouds that are usually provided through separate arrangements, but are bound together for data and application portability (examples of this are: public cloud providing offloading capability for specific workloads).[4]

Depending on user requirements, there are several cloud computing solutions available on the market; they can be grouped into three main categories or "service models":

- Infrastructure as a Service (IaaS):[5] a cloud provider leases virtual remote servers that end users can rely on in accordance with provisioning mechanisms and contractual arrangements. This model is comparable to a situation when users install both the operating system and the applications on new hardware themselves, and they are responsible for keeping the whole software stack up to date and manageable. The

2 The NIST Definition of Cloud Computing, Sept. 2011 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (25/1/2016).

3 *Suchankova*, Cloud Computing in the Czech Republic – Regulatory Framework, 2014, p. 8.

4 See http://marketrealist.com/2014/07/must-know-cloud-computing-services-and-models/ (25/1/2016).

5 Examples: Amazon Web Services EC2, MicrosoftOneDrive, GoogleDrive, Dropbox.

real difference is that in the case of cloud IaaS this "new hardware" is not physically available locally, but it is available somewhere in the cloud in the form of a "virtual computer" or "virtual machine" through internet connectivity. Users usually install so-called "images" of the complete software stack into such a remote virtual server environment. The terms and conditions usually include the metered-by-use cost model and allow the end user to expand their use of the infrastructure as needed, usually via self-service portals.

- Platform as a Service (PaaS):[6] a cloud provider offers solutions for hosting of applications. As a simplified description, the user gets a virtual computer (or "virtual machine") in the cloud running a particular type and version of the operating system, together with needed middleware and libraries that support installation of compatible applications. The cloud provider is responsible for keeping the operating system up to date, and for managing all the underlying hardware and networking. PaaS is widely used for testing and deployment of new applications without having to provision local virtual machines together with instances of the operating system.
- Software as a Service (SaaS)[7] is a model where an application is delivered over the Internet and users pay on a per-use basis. In SaaS, the user is only focused on the finished application, without having to manage the application or the underlying operating system and infrastructure.[8]

According to IDC research from December 2013,[9] the fastest growing segment of cloud services globally will be SaaS – it is predicted to grow nearly five times faster than the software market as a whole. By 2016, about 25 % of all new business software purchases will be of service enabled software, and SaaS delivery will constitute about 16.4 % of worldwide software spending across all primary markets and 18.8 % of applications spending.[10]

The main reason for this evolution is found in the cloud opportunities perceived by business management such as (i) IT efficiency – deliver IT resources quickly and at an acceptable price point, (ii) IT agility – services that are easily consumable, consistent, and paid-per-use, and (iii) Business innovation – cloud helps address user opportunities faster, enable and optimize business performance.[11]

It is significant to note that the cloud users see these services as integrated services and do not bother with the underlying components.[12] Regrettably this has the tendency of mistreating certain categories of data and shifting the control of the collected data, affairs which are yet to be addressed in the analysis.

6 Examples: Google App Engine, Windows Azure.
7 Examples: Microsoft Office 365, Google Maps, Google Apps for Business, iCloud.
8 *Sosinsky*, Cloud Computing Bible, 2011, p. 30.
9 IDC Market Analysis Perspective, Worldwide SaaS and Cloud Software, 2013 (IDC #245047), www.idc.com/getdoc.jsp?containerId=245047 (25/1/2016).
10 Ibid.
11 *Suchankova*, (fn. 3), p. 13.
12 See www.katescomment.com/iaas-paas-saas-definition/ (25/1/2016).

C. Data Privacy Issues and Problems

It is now generally accepted that cloud computing services, whether provided as a SaaS, PaaS or IaaS service model, will involve some kind of processing of personal data. Therefore, the cloud computing scenarios involve different players with different roles and usually the cloud providers will be considered as "data processors" while cloud users who determine the ultimate purpose of the processing and decide on the outsourcing and the delegation of all or part of the processing activities to an external organization will in most cases be deemed "data controllers".

In cloud computing, the "personal data" definitional issue and its interpretation is most relevant in several specific contexts: anonymized and pseudo anonymized data, encrypted data – whether encrypted in transmission (i.e. data in motion or data in transit) or in storage (data at rest). In each case, the question is, should such data be treated as "personal data" and thus fall under the data protection rules?[13]

Anonymized or pseudo anonymized data are made by deliberately concealing or hiding the data subjects' identities. In the digital environment it is considered that the anonymity and pseudonymity protects a person and enables it to speak freely, to enforce its legal rights without the fear of sanctions.[14] Respectively the person is willing to share as little as possible. In cloud computing, a cloud user may perform an anonymization or pseudo anonymization procedure on a data set before processing the resulting data in the cloud in the sense that it takes the most identifying field within a database and replaces them with artificial identifiers. Many anonymization and pseudo anonymization techniques involve amendments to part only of a data set.[15] The revealing of the identity of this kind of data is strictly forbidden by data protection laws. This is due to the fact that the user is relying on the fact that these data will remain secret and thus the user could not be identified.[16]

Encrypted data normally involve encrypting the entire data set for security purposes. The security of encrypted data depends on several factors, notably the strength of the encryption method used (i.e. the cryptographic strength of the algorithm) and the length of the encryption key, with longer keys generally providing better security against attacks, another important factor being the management of the decryption key – how securely the key is stored, how many people have access to it etc. The data transmission may itself be encrypted or unencrypted, usually depending on how the cloud provider has set up its systems, for example to use encrypted connections.[17]

In considering the free processing of personal data in the cloud, the scope of "personal data" is critical. The information which is not, or which ceases to be, "personal

13 *Suchankova*, (fn. 3), p. 9.
14 *Härting*, Internetrecht, 5th ed. 2014, p. 632.
15 See www.pseudonymised.com (25/1/2016).
16 *Härting*, (fn. 14), p. 644.
17 *Hon/Millard/Walden*, The Problem of "Personal Data" in Cloud Computing – What Information is Regulated?, The Cloud of Unknowing, Part 1, Queen Mary School of Law Legal Studies Research Paper No. 75/2011, p. 8.

data", may be processed and transferred, in the cloud or otherwise, free of data protection law requirements.[18]

As one of the important elements of adequacy in the cloud is the effectiveness of the implementation of the data protection. At present, the US did not have a data privacy regime that would meet the requirements of the EU for transfer of data to non-EU countries. This was and still is especially challenging taking into consideration the fact the cloud providers are basically all incorporated and operating under the laws of the US.

Therefore, in order to overcome the created situation, the US Department of Commerce was involved in the creation of a "safe harbor" for US companies. These principles, generally know as the Safe Harbor Privacy Principles were elaborated between the EU and the US for US's business companies. The concept behind these principles is that a company entitled to the safe harbor status would automatically be granted a presumption of adequate compliance with the Data Protection Directive and thus data transfers from the European Union to it would be allowed for the data considered to be "personal data". The principles also provide for a certain amount of state supervision and only those companies can join the safe harbor, which are subject to the supervision of the US Federal Trade Commission.[19] The aim of these principles is to provide an adequate privacy protection for European citizens but which would also reflect the interest requirements and provide for a predictable and cost effective framework for the private sector. The goal of these principles is to maintain the established standards as a role model for transfer of data to other non-EU member states. As may be gathered from the foregoing analysis, this is not an easy task especially for countries with relatively new data privacy legislation and especially with regard to the questions that are not explicitly referred even in the current EU legislation.

I. The European Union Regulatory Framework

1. Development of the Data Privacy Law

When the European Convention on Human Rights came into force on 3 September 1953 the Convention already stipulated a right to "represent private and family life" (Article 8(1) ECHR). However, this was not considered as a fundamental right to data protection yet, as it is known today in the context of the European Union law.[20] The inception of the modern data privacy regulation started in the 1980s with the OECD

18 Ibid., p. 10.

19 *McCarty-Snead/Hilby*, Research Guide to European Data Protection Law, Berkley Law Scholarship Repository, Legal Research Series 11-2013, p. 265.

20 See *von dem Bussche/Stamm*, Data Protection Germany, 2013, p. 1.

Data Protection Principles in 1980[21] and the Council of Europe's Convention on the Automated Processing of Personal Data of 1981 (Convention 108).[22] The basic aims of the Convention 108 were to protect the privacy rights of individuals in circumstances where information about them was to be processed automatically; and facilitate a common international standard of protection for individuals, with the aim that the free flow of information across international boundaries could proceed without disruption.[23]

However, the nature and scope of the member states' data privacy laws were extremely varied.[24] Therefore, by the early 1990s, this lack of consistency was beginning to be viewed by the EU Commission as potentially serious impediment to the attain-

21 The OECD's eight data protection principles, as outlined in Part II of the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, are as follows: "1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject; 2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date; 3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose; 4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a. with the consent of the data subject or b. by the authority of law; 5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data; 6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller; 7. Individual Participation Principle: An individual should have the right: to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating to him i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to him; to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended; 8. Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles states above." See www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2 (25/1/2016).

22 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, Council of Europe, Strasbourg 1981.

23 *Charlesworth*, Clash of the Data Titans?, US and EU Data Privacy Regulation, European Public Law 6 (2000), p. 256.

24 Germany was a forerunner: On 30/9/1970, the German federal state of Hessen enacted the world's first data protection act, and the first data protection act in Germany at federal level came into force on 1/1/1978, see *von dem Bussche/Stamm*, (fn. 20), p. 1. An article in the French Napoleonic Code dated back to the 19th century even guaranteed the right to private life. The French Parliament in 1978 decreed that any person, company or government agency receiving or processing personal information without authorization could be punished by up to six months in prison and a maximum fine of 20.000 francs (3.000 Euro), www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711 (25/1/2016).

ment of the single market. This resulted in the rather pragmatic proposal for legislative measures by the European Commission in 1992.[25] The main purpose of the forthcoming directive was thus to harmonize the existing laws (ranging from indifference to its elevation as a quasi-human right). Its adoption was widely discussed, between the business organization, associations, public authorities, law enforcement stakeholders, a number of studies and comprehensive opinions were also launched and public consultations through EU citizens' surveys were enforced, all welcoming the new milestone in the history of data protection.

The centerpiece of existing EU legislation on personal data protection, Directive 95/46/EC,[26] was adopted in 1995 with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between member states. The Data Protection Directive is designed to give substance to the principles of the right to privacy already contained in the Convention 108 and to expand them. The Data Protection Directive, however, draws on the possibility provided for in the Article 11 of the Convention 108 of adding on instruments of protection (such as the instrument for improving compliance with data protection rules). As the Data Protection Directive could address only EU member states, an additional legal instrument was needed in order to establish data protection for the processing of personal data by institutions and bodies of the EU. The Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data (EU Institutions Data Protection Regulation) fulfils this task.[27] Additionally, even in areas covered by the Data Protection Directive, more detailed data protection provisions are often needed in order to achieve the necessary clarity in balancing other legitimate interests. Two examples are the Directive 2002/58/EC[28] on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public com-

25 *Hetmank*, Internetrecht, Grundlagen – Streitfragen – Aktuelle Entwicklungen, 2016, pp. 147-172.

26 Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23/11/1995, p. 31.

27 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18/12/2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ L 8 of 12/1/2001, p. 1.

28 Directive 2002/58/EC of the European Parliament and of the Council of 12/7/2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 of 31/7/2002, p. 37.

munications networks and amending Directive 2002/58/EC (Data Retention Directive, invalidated on 8 April 2014).[29]

Thus, the data protection liberties have a long standing tradition in the EU member states[30] and as some discussions back than pointed out "perhaps it's more of a sensitivity or sensibility issue, why people are worried about the protection of their private life and their independence".[31]

The right to data protection in the EU developed out of the right to respect for private life, one of the fundamental rights under the European Convention on Human Rights. The concept of private life relates to human beings. Under EU law, the natural persons (living beings) are, therefore, the primary beneficiaries of data protection. In this context their personal data are defined as "any information relating to an identified or identifiable natural person (data subject)".[32]

It is considered that under EU law, the information contains data about a person if: an individual is identified in this information, or if an individual can be identified by conducting further research. Both types of information are protected under the European data protection law. The legal definitions of personal data do not further clarify when a person is considered to be identified. Evidently, identification requires elements which describe a person in such a way that he or she is distinguishable from all other persons and recognizable as an individual.[33] A person's name is a prime example of such elements of description. In exceptional cases, other identifiers can have a similar effect to a name (example: date and place of birth, personalize numbers etc.).[34] For the applicability of European data protection law, however, there is no need for high-quality identification of the data subject; it is sufficient that the person concerned may be identifiable. A person is considered identifiable if a piece of information contains elements of identification through which the person can be identified, directly or indirectly.[35]

29 Directive 2006/24/EC of the European Parliament and of the Council of 15/3/2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), OJ L 105 of 13/4/2006, p. 54, invalidated on 8/4/2014.

30 Such as France and Germany.

31 See www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711 (25/1/2016).

32 Article 2(a) Data Protection Directive 95/46/EC; Article 2(a) Convention 108.

33 The CJEU stated in case C-275/06, *Promusicae*, EU:C:2008:54, para. 45 that "it is not disputed that the communication sought by Promusicae of the names and addresses of certain users of [a certain internet file-sharing platform] involves the making available of personal data, that is, information relating to identified or identifiable natural persons, in accordance with the definition in Article 2(a) of Directive 95/46 [...]. That communication of information which, as Promusicae submits and Telefónica does not contest, is stored by Telefónica constitutes the processing of personal data within the meaning of the first paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 2(b) of Directive 95/46".

34 European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, 2014, p. 39.

35 Article 2(a) Data Protection Directive 95/46/EC.

Taking into consideration the definition, any kind of information can be personal data providing that it relates to a person. The personal data covers information pertaining to the private life of a person as well as information about his or her professional or public life.[36] Respectively, data relate to persons also if the content of the information indirectly reveals data about a person.

The form in which the personal data is stored or used is not relevant to the applicability of data protection law. However, according to the principle of limited retention of data, contained in the Data Protection Directive, the data must be kept "in a form which permits identification of data subjects for no longer than it is necessary for the purpose for which the data were collected or for which they are further processed".[37] Consequently data would have to be anonymized if a controller wanted to store them after they were outdated and no longer served their initial purpose. It is considered that the data are anonymized if all identifying elements have been eliminated from a set of personal data. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned. Where data has been successfully anonymized, they are no longer personal data.[38]

Unlike the anonymized, the pseudo anonymized data are not explicitly mentioned in the legal definitions of the Data Protection Directive. However, the Explanatory Report to Convention 108 states in its Article 42 that

> "[t]he requirement [...] concerning the time-limits for the storage of data in their name-linked form does not mean that data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should not be possible to link readily the data and the identifiers".

This is an effect which can be achieved by pseudo anonymizing the data. For everyone who is not in possession of the decryption key, pseudo anonymized data can be identifiable with difficulty. The link to an identity still exists in form of the pseudonym plus the decryption key. For those who are entitled to use the decryption key, re-identification is easily possible. The use of encryption keys by unauthorized persons must be particularly guarded against. Personal data with encrypted identifiers are used in many contexts as a means to keep secret the identity of persons. This is particularly useful where data controllers need to ensure that they are dealing with the same data subjects but do not require, or ought not to have, the data subjects' real identities. Pseudo anonymization is therefore a strong link in the armory of privacy-enhancing technology. It can function as an important element when implementing privacy by

36 In joined cases C-92/09 and C-93/09, *Volker and Markus Schecke and Eifert*, EU:C:2010:662, para. 59 the CJEU stated that "it is of no relevance in this respect that the data published concerns activities of a professional nature [...]. The European Court of Human Rights has held on this point, with reference to the interpretation of Article 8 of the Convention, that the term "private life" must not be interpreted restrictively and that there is no reason of principle to justify excluding activities of a professional [...] nature from the notion of private life".

37 Article 6(1)(e) Data Protection Directive 95/46/EC.

38 European Union Agency for Fundamental Rights, (fn. 34), p. 44.

design. This means having data protection built into the fabric of advanced data-processing systems.[39]

There is currently no conclusive decision or guidance on the EU level on when encrypted data may be safely regarded as anonymized data and thus outside of the scope of personal data protection since the question of personal data is a question of fact varying from case to case. However, in praxis the widest interoperation of the definition in certain number of cases covers also these types of data.[40]

Some EU jurisdictions[41] provide a simpler view of this kind of data. Namely, when deleting the direct identifiers of the subject, the data are classified as indirectly personal data. In this way the controller, processor or recipient of the data cannot identify the individuals using legally permissible means. Indirectly personal data are, effectively, a kind of pseudonymous data, where identities can be retraced, but not via legal methods. Such information, presumably because risks to individuals are considered lower, is given less protection than fully-fledged "personal data". It can, for example, be transferred out of the EEA without regulatory approval.[42]

Therefore, it is useful to recall that the reasons for enacting the first data protection laws stemmed from the fact that new technology in the form of electronic data processing allows easier and more widespread access to personal data than the traditional forms of data handling. An undesirable result would be that of ending up applying data protection rules to situations which were not intended to be covered by those rules and for which they were not designed by the legislator. Another general limitation for the application of data protection under the Data Protection Directive would be processing of data under circumstances, where means for identifying the data subject are not "likely reasonably to be used".[43] National Data Protection Supervisory Authorities play an essential role in this respect in the framework of their missions of monitoring the application of data protection law, which involves providing interpretation of legal provisions and concrete guidance to controllers and data subjects. They should endorse a definition that is wide enough so that it can anticipate evolutions and catch all "shadow zones" within its scope, while making legitimate use of the flexibility contained in the Data Protection Directive.[44]

2. The Reform of the Data Privacy Law

Having in mind that in today's new, challenging digital environment, existing rules provide neither the degree of harmonisation required, nor the necessary efficiency to ensure the right to personal data protection, most of the European citizens were con-

39 Ibid., p. 46.
40 The Working Party Opinion no. 4/2007 adopted on 20/6/2007 referenced as WP 136 states that "the intention of the European Lawmaker was to treat the term personal data broadly, covering all information that may be linked to an individual".
41 Such as Austria.
42 *Sosinsky*, (fn. 8), p. 51.
43 Working Party Opinion no. 4/2007, (fn. 40), p. 5.
44 Ibid.

cerned about the collected data without their consent. This problem was especially highlighted in the field of mobile applications.[45] However the same and even bigger problem might arise from everyday increasing of usage of cloud computing. The rapid pace of technological change and globalisation have profoundly transformed the way in which an ever-increasing volume of personal data is collected, accessed, used and transferred. New ways of sharing information through cloud computing services and storing large amounts of data remotely have become part of life for many of Europe's 250 million internet users. At the same time, personal data has become an asset for many businesses.[46]

In this new digital environment, individuals have the right to enjoy effective control over their personal information. Data protection is considered to be a fundamental right in Europe, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, as well as in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), which needs to be protected accordingly.[47] These discussions made clear that both citizens and businesses wanted the European Commission to reform EU data protection rules in a comprehensive manner. Especially if we take into account the fact that the Data Protection Directive did not fulfill its primary task of providing full harmonization, therefore creating discrepancies in application between the member states.

After assessing the impacts of different policy options, the European Commission is now proposing a strong and consistent legislative framework across Union policies, enhancing individuals' rights, the single market dimension of data protection the so called "reform's data protection rules", were enacted by the Commission in 2012. The proposed rules came back to the European Parliament in March 2014. Due to the aforementioned, an important step is taken by EU officials in order for data protection rules to be finalized. The reform's package[48] of data protection rules consists of a regulation,[49] which sets out a general EU framework for data protection, i.e. to replace the 1995 Directive. A regulation has been chosen because, once adopted, this format

45 Nine out of ten Europeans (92 %) say they are concerned about mobile apps collecting their data without their consent. Seven Europeans out of ten are concerned about the potential use that companies may make of the information disclosed. See European Commission, Progress on EU data protection reform now irreversible following European Parliament vote, MEMO/14/186 of 12/3/2014.

46 European Commission, Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century, COM (2012) 9 final, p. 1.

47 Vice-President *Viviane Reding*, the EU's Justice Commissioner, www.dw.com/en/eu-wants-to-give-consumers-more-control-over-their-data/a-6191278 (25/1/2016).

48 MEMO/14/186, (fn. 45): "The message the European Parliament is sending is unequivocal: This reform is a necessity, and now it is irreversible. Europe's directly elected parliamentarians have listened to European citizens and European businesses and, with this vote, have made clear that we need a uniform and strong European data protection law, which will make life easier for business and strengthen the protection of our citizens" said Vice-President *Viviane Reding*, the EU's Justice Commissioner.

49 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final.

should be immediately applicable in all member states. Also, there is a Directive,[50] which specifically deals with protecting personal data processed in a law enforcement context.

The new rules will put citizens back in control of their data, notably through:

(1) A right to be forgotten:[51] When you no longer want your data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted;[52]

(2) Easier access to your own data: Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way;

(3) Right to data portability will make it easier for you to transfer your personal data between service providers;

(4) The right to know when your data has been hacked: Companies and organizations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours) so that users can take appropriate measures;

(5) Data protection first, not an afterthought: "Data protection by design" and "Data protection by default" will also become essential principles in EU data protection rules. Data protection safeguards should be built into products and services from the earliest stage of development.[53]

Strengthening Europe's high standards of data protection is a business opportunity. This data protection reform will help the digital single market realized, through the following:

(1) One continent, one law: The Regulation will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws;

50 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final.

51 See CJEU, case C-131/12, *Google v Costeja González*, EU:C:2014:317, para. 93: Individuals have the right – under certain conditions – to ask the search engines to remove links with personal information about them. This applies where the information is inaccurate, inadequate or excessive for the purpose of data processing. Para. 85: The court found that in this particular case the interference with a person's right to data protection could not be justified merely by the economic interest of the search engine. At the same time the court explicitly clarified that the right to be forgotten is not absolute but always need to be balanced against other fundamental rights, such as the freedom of expression and of the media. European Commission, Factsheet on the "Right to be Forgotten" ruling (C-131/12), 2014.

52 There also have been ongoing discussions about putting a deadline on photos and posts – the idea is that the user could then select when items should be automatically deleted. "But it's doubtable if that would be a feature social networks would actually welcome, what happens if you forget about the deadline you set and half of your page has been raided?" See *Hoeren*, in: *Steffen*, EU wants to give consumers more control over their data, www.dw.com/en/eu-wants-to-give-consumers-more-control-over-their-data/a-6191278 (25/1/2016).

53 European Commission, (fn. 46), p. 4.

(2) One-stop-shop: The Regulation will establish a "one-stop-shop" for businesses: companies will only have to deal with one single supervisory authority;

(3) The same rules for all companies – regardless of where they are established: Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business on the European single market. With the reform, the same rules will apply to companies based outside of Europe;

(4) European regulators will be equipped with strong enforcement powers: data protection authorities will be able to fine companies who do not comply with EU rules up to 2 % of their global annual turnover.[54]

As seen from the proposal, the draft regulation retains the core concepts and basic principles enshrined in the Data Protection Directive, such as technology neutrality, controller-processor dichotomy and legal bases for data transfer to third countries, among others. This means that there are no specific provisions for cloud computing per se, even though they are referred in the European Commission's Proposal, and the data controller remains responsible for data processed on its behalf, no matter the means.

3. Future Challenges

While the draft regulation and various amendments to it are being debated, it is important to point out some other issues that have not yet been addressed in the proposal, especially in relation to cloud computing. As it seems the regulation will not change drastically the conditions for the EU cloud users, under which the data is being processed.[55]

First, as pointed out earlier, cloud computing involves various layers and intermediaries of actors for which a strict application of data controller- processor dichotomy may be ambiguous and misleading. So far, the draft regulation has not taken proper cognizance of these sets of actors. The closest attempt at recognizing this gap is in a new provision in the LIBE Committee's report that introduced a new party defined as "producers". Though by a stretch of argument the definition of "data producer" may include some cloud intermediaries, this may be an ambiguous way of describing all of them, since some of the intermediaries do not have any infrastructure for producing or processing data but only provide monitoring services.[56] Of course, making every party in the chain of transaction joint controllers will not solve the problem as

54 MEMO/14/186, (fn. 45).

55 *Niemann/Paul*, Rechtsfragen des Cloud Computing: Herausforderungen für die unternehmerische Praxis, 2014, p. 101.

56 "Producer" means a natural or legal person, public authority, agency or any other body which creates automated data processing or ling systems designed for the processing of personal data by data controllers and data processors. See Article 4 (point 6a (new)) of the LIBE Report, www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN (25/1/2016).

purported in Article 24 of the draft regulation.[57] A number of opinions have called for a rethinking in the classification of actors in view of modern data processing possibilities, of which cloud computing is a ready example. The draft regulation, as well as the various parliamentary amendments, has not devoted significant attention to this issue of finding a solution for the mutual relationships, which can no longer be characterized as a simple "relationship of command" or "principal-delegate relationship".[58]

Regarding the anonymized data, the draft regulation in point 23 of the preamble provides that

> "the principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable".

Respectively, the draft regulation does not provide anything in regards to the pseudo anonymized or encrypted data. However, the pseudo anonymization of data is one of the most important means of achieving protection on a large scale, where it is not possible entirely to refrain from using personal data. Here, the issue of pseudo anonymization affects directly the effectiveness of the data protection. This is especially true if we take into consideration the fact that the information which is not "personal data" in the hands of one person (such as cloud user) may, depending on the circumstances, become "personal data" when obtained or processed by another (such as a cloud provider).[59] On the other hand, the lack of clear guidance regarding the nature of the anonymized and pseudo anonymized data can result in a general conclusion that the anonymized data are not to be considered as personal data (since they are explicitly excluded) and the pseudo anonymized are in fact personal data in the sense of the new draft regulation, since there is no reference at all and no possibility of developed court practice in the draft stage of the regulation. Regarding the encrypted data, it seems that they are not part of this framework at all, since none of the analyzed documents preceding the draft regulation does not mention them. In order for the reform to represent a step forward, however, it should also address these issues, because this gap may otherwise lead to unintended consequences.

57 *Hert/Papakonstantinou*, The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals, Computer Law & Security Review 28 (2012), pp. 130-142: "the distinction between data controllers and data processors, that was perhaps clear at the time the Directive was introduced, is increasingly disputed in the contemporary complex business environment. [...] The distinction between the two data processing actors is becoming increasingly blurred in an interconnected world of ubiquitous computing. In view of the above, perhaps the preferable way forward would be for the Commission to boldly abolish the notion of "data processors" from its Regulation altogether, and vest the data controller title, rights and obligations upon anyone processing personal information, regardless of its means, conditions or purposes".

58 *Nwankwo*, Missing Links in the Proposed EU Data Protection Regulation and Cloud Computing Scenarios: A Brief Overview, JIPITEC 5 (2014), p. 36.

59 *Hon/Millard/Walden*, (fn. 17), p. 13.

Also, some of the provisions of the draft regulation on the international data transfer raise interesting questions. According to the EU data protection law, as stated above, the transfer and processing of data to and in non-EU states is subject to strict regulations. It has to be ensured that the controller as a user of a cloud computing service always compiles with the requirements outlined in the legislation. This is a highly complicated task. For instance, the controller always has to ensure that the cloud provider observes adequate level of protection. Considering the big international operating service providers, the controller will often have no legal or practical opportunities to verify the level of data protection and security of the particular service provider.[60]

Additionally, in spite of the controversies surrounding the use of "onward transfer" in the EU-US safe harbor framework, it has been recognized in the regulation without any definition or mechanism for its application.[61] Article 40 derives a general principle, that the compliance with the obligations in that chapter is mandatory for any transfers of personal data to third countries or international organizations, including onward transfers. The concept entails that after EU personal data is transferred to a safe harbor-certified US entity, further transfers from the importer to a third party (onward transfers) are possible, subject to restrictions under the safe harbor.[62]

From my perspective it is not clear how this concept will apply to other entities that are not subject to the safe harbor framework, since the original concept has been limited to the US. On the other hand, the Article 42 of the draft regulation requires for transfers to third countries, where no adequate decision has been adopted by the Commission to adduce appropriate safeguards, in particular standard data protection clauses, binding corporate rules and contractual clauses. The possibility of making use of Commission standard data protection clauses is based on Article 26(4) of Directive 95/46/EC. As a new component, such standard data protection clauses may now also be adopted by a supervisory authority and be declared generally valid by the Commission. In light of the aforementioned, there is a need for more clarity in the application of the concept if it is intended to have a general application, so that it does not serve as a tool to circumvent data protection requirements.[63]

II. The Regulatory Framework of the Republic of Macedonia

1. Overview of the Data Privacy Legislation

The data privacy protection is considered to be a relatively new area in the legislative system of the Republic of Macedonia. Even though the protection of the personal data

60 See *von dem Bussche/Stamm*, (fn. 20), p. 67.
61 Article 40 of the General Data Protection Regulation, (fn. 49).
62 *Kuner*, Onward Transfer of Personal Data under the U.S. Safe Harbor Framework, Privacy and Security Law Report 2009, p. 1 et seq.; *Münyl/Pauly/Reti*, Cloud Computing als neue Herausforderung für Management und IT, 2015, p. 45.
63 *Nwankwo*, (fn. 58), p. 36.

is guaranteed in the Constitution of the Republic of Macedonia,[64] the specific legal framework is established in 2005 by passing of the Data Privacy Act.[65]

The necessity of providing adequate and effective legal protection of the right of data privacy protection is considered to be very important in the process of accession of the Republic of Macedonia towards the European Union. This is also pointed out in the Stabilization and Association Agreement (SAA)[66] with the European Union which the Republic of Macedonia signed in April 2001. Respectively, Article 68 of the SAA provided that

> "the Republic of Macedonia recognizes the importance of the approximation of the existing and future laws to those of the Community and shall endeavor to ensure that its laws will be gradually made compatible with those of the Community. This gradual approximation will take place in two stages, where as in the first stage starting on the signing date of the SAA the approximation of law shall extend to certain fundamental elements of the Internal Market along a programmed defined together with the Commission. Deadlines will be set for […] data protection law".

Even though the data privacy protection was not considered as a priority by the State bodies for a longer period of time, under the influence of the Data Protection Directive and the appropriate EU legislation, the Republic of Macedonia finally embraced the inevitability of passing appropriate legislation.

The Data Privacy Act contains basically the same structure as the Directive and it covers almost all aspects of data privacy protection which are subject matter of the Directive.[67] However, we must emphasize that the Data Privacy Act and the bylaws which are passed do not contain sufficient explanatory notes regarding the issues raised in this paper.

2. Significant Provisions of the Data Privacy Act for Cloud Computing

Firstly, the Data Privacy Act defines the "personal data" objectively in a sense as any information pertaining to an identified or identifiable natural person, the identifiable entity being an entity whose identity can be determined directly or indirectly, especially as according to the personal identification number of the citizen or on the basis of one or more characteristics, specific for his/her physical, mental, economic, cultural or social identity.[68]

64 Article 18 of the Macedonian Constitution: the citizens of the Republic of Macedonia are granted with 1. the safety and secrecy of the personal data; 2. The protection of breach of their personal integrity which derives out of the record and processing of their personal data.

65 The governing legal act in the Republic of Macedonia is the Law on protection of personal data – hereinafter referred to as the "Data Privacy Act", Official Gazette of RM no. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015.

66 OJ L 84 of 20/3/2004, p. 13.

67 Commission Staff Working Document, The Former Yugoslav Republic of Macedonia Report 2015, SWD (2015) 212 final, p. 57: "The Law on Personal Data Protection is largely aligned with the EU *acquis*."

68 Article 2(1)(1) of the Data Privacy Act.

The aim of the Data Privacy Act is not only the protection of the personal data, but protection of the person to which these data refer and thus it is right to maintain privacy over the shared information. Therefore, the Data Privacy Act does not cover the entire spectrum of data privacy rights, but only that part reflecting the information regarding the person. Consequently, the content of the data privacy protection encompasses the right to give consent for the processing of the data, the right of information about the processing, the right of insight, the right of making a copy and the right of an amendment.[69]

The most important pillar of the data processing in the cloud is a written agreement on the processing of personal data. A data processing agreement needs to be executed between the data controller and the data processor before any data processing operation in the cloud is carried out. The controller may transfer matters of his or her scope of work, related to the personal data processing, to the processor. The internal rights and obligations of the controller and processor have to be regulated by an agreement in written form, obligatory containing: the obligation of the processor to act solely in accordance with directions received from the controller, the obligation for the processor to undertake technical and organizational measures to provide secrecy and protection of the personal data processing and the mandatory provision for the manner of testing and inspecting of protection matters and controls of the processor for the processing of the personal data.[70] In principle, the Data Privacy Act also allows the use of sub-processors. The sub-processors are defined as "third party", which shall be any natural person or legal entity, a state administration body or other body, which is not a personal data subject, a controller, a personal data collection processor or any person who, under a direct authorization by the controller or by the personal data collection processor is authorized to process the data. The Data Privacy Act requires the consent of the data subject in order for the data to be disclosed to such third parties.[71]

In addition, within the framework of its indexing programs the cloud provider may also record and organize the data which are stored on its servers, whether these be classified as personal data or not. These operations are also not referred expressly and unconditionally in the Data Privacy Act; however, we believe that they have to be classified as processing regardless of the fact that the cloud provider carries them out without distinction in respect of other information. Under our observation of the situation, the activity of a cloud provider is similar to that of publishers of websites and is liable to affect significantly the fundamental rights to privacy and to the protection of personal data, the cloud provider must ensure, within the framework of its responsibilities, powers and capabilities, that its activity complies with the requirements of the Data Privacy Act.

If we analyze in detail the definition of "personal data" provided in the Data Privacy Act, it is obvious that it does not make any reference to the anonymous and pseudo

69 Article 10 of the Data Privacy Act.
70 Article 26 of the Data Privacy Act.
71 Article 2(1)(7) of the Data Privacy Act.

anonymous or encrypted data, respectively whether these types of data may or should be subject to the processing agreement. However, it reads that data is personal if it relates to an identified or at least identifiable person, the data subject. That is information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information, respectively conducting further research.[72] However, by definition the data are considered to be anonymized if they no longer contain any identifiers, or pseudo anonymized if the identifiers are encrypted. Therefore, the Data Privacy Act excludes implicitly, the anonymized, pseudo anonymized and encrypted data from its scope of application.

This simple analysis does not seem to have always a practical validation. The exact factual background from the praxis of the Directorate reveals a different situation.[73] Namely, the Act provides explicitly that prior to initiating any personal data processing, the controller shall be obliged to notify[74] the Directorate and this notification has predetermined content.[75] The controller may initiate the personal data processing being subject of the notification only after obtaining the confirmation letter for the performed notification referred before. Therefore, by default, this provision requires that the Directorate should be informed for every possible collection of data and the assessment criteria of the Directorate are based on the objective interpretation of the term "personal data". These objective identifiers also include the possibility of a person being directly or indirectly identified by a certain characteristic or combination of characteristic which make he or she distinguishable from all other persons and recognizable as an individual, by any available means for identification used by the controller or any other person that has access to the base.

72 ECtHR, no. 27798/95, *Amann v. Switzerland* [GC], para. 65.

73 The Directorate for Personal Data Protection continued to strengthen its capacity through ongoing training, employment of four new staff and a slight budget increase. It further increased its activities in 2014, carrying out 404 inspections in the public and private sectors (387 in 2013) and finding 300 violations in total. It received 371 complaints in 2014 (404 in 2013), mostly concerning abuse of personal data on social networks. The number of personal data controllers and processors trained increased to 66 in 2014 (54 in 2013) and active public awareness-raising measures continued. The Directorate was consulted on draft legislation, public policies and operations of data controllers more frequently than in previous years. Further efforts are needed to ensure full harmonisation of sectorial legislation with the Data Privacy Act. The Directorate, which is an independent regulatory body, has yet to take action following the recent disclosure of massive unlawful interception of individuals' electronic communications. This has raised questions about its ability to act with full independence, see European Commission, The Former Yugoslav Republic of Macedonia Progress Report, Enlargement, October 2014, p. 57.

74 Article 11 of the Data Privacy Act.

75 The notification must contain: the title of the personal data collection; title i.e. the personal name of the controller and his/her head office, i.e. address, as well as the name and the address of his/her representative, if any; purpose or purposes of the processing, legal basis for the establishment of a personal data collection; category or categories of the personal data subjects and personal data i.e categories of personal data referring to him/her or them; the users or the categories of users to whom the personal data may be given for use; time period for keeping the personal data; transfer of personal data to other states, and general description that shall enable primary assessment of the properness of the undertaken technical and organizational measures for personal data protection and their processing.

If the Directorate considers that a certain form of data collection should be subject to the Data Privacy Act and to stricter policies than the Directorate will make a reference in the confirmation letter even if the data in question are in fact anonymized, pseudo anonymized and encrypted data. In addition, all data processing activities are recorded in the Directorates' Central Register which represents a quasi case law base so if there is a prior similar case, the Directorate will most likely decide in the same manner. Also, if having any doubts regarding the type of data or the interpretation collected the Directorate will ask for assistance by the European Commission and/or the Member States' National Authorities.

In order to provide secrecy and protection of the processing of the subject's personal data, the controller and processor have to apply proper technical and organizational measures for protection of accidental or illegal damaging of the personal data, or their accidental loss, change, unauthorized disclosing or approach, especially when the processing includes transmission of data over a network and protection of any kind of illegal forms of processing.[76]

The personal data referred, may be transferred via electronic telecommunications network only if specially protected by proper methods, therefore not being readable in the transfer process. The personal data transfer to other countries may be carried out only if the other country provides an adequate degree of personal data protection which confirms the fact that the transfer and processing of data to and in non-EU states is subject to strict regulations. The personal data transfer in other countries, which fail to provide at least the same level of personal data protection as in the Republic of Macedonia, may be performed after prior approval from the Directorate, under the condition to have provided proper guarantees for protection of the personal data, rights and freedoms of the personal data subject.[77] Also in a case of hardware or software maintenance or other activities of the information system the transfer of personal data can be made to other countries only under the conditions determined in the Data Privacy Act.[78] The Data Privacy Act makes explicit reference to the decisions of the European Commission, respectively if the European Commission shall determine that the third country does not provide proper level of protection regarding the transfer or category of personal data transfer, the Directorate shall issue a determination for prohibition of personal data transfer.[79] If the Directorate shall assess that the determined third country fails to provide a proper level of protection regarding the personal data transfer, it shall immediately notify the European Commission and impose the controller to freeze the data transfer.[80]

On the other hand, the facilitation of data flows to the EU member states and the countries members to the European Economic Space is done without any obstacles

76 Article 5(1)(4) of the Data Privacy Act.
77 Article 33(3) of the Data Privacy Act.
78 Article 9a of the Rulebook for the technical and organizational measures for providing of secrecy and protection of the processing of personal data, Official Gazette of the Republic of Macedonia no. 38/2009 and 158/2010.
79 Article 31(4) of the Data Privacy Act.
80 Article 31(5) of the Data Privacy Act.

or additional requirements.[81] Furthermore, under the Data Privacy Act also the transfer to the US under the safe harbor principles is allowed due to the fact that the Data Privacy Act makes explicit reference to the decisions of the European Commission in this regard. Therefore, the Data Privacy Act also recognizes any such transfer without any definition or mechanism for its application.

It is evident that the objective of the Data Privacy Act is the protection of fundamental rights and freedoms when personal data are processed while removing obstacles to the free flow of such data. Very little is said however, for the cloud computing of anonymized and pseudo anonymized data, even though these services are also offered by the Macedonian cloud computing providers.[82] However, if we adopt the opinion that due to the lack of specific provisions in the Republic of Macedonia the data protection rules do not apply for these specific categories of data, still certain activities considering their collection, processing and transfer may constitute an interference with the some of the most important legal texts of all time such as the European Convention on Human Rights,[83] the Convention 108 as well as the Macedonian Constitution,[84] and the rules of the Data Privacy Act,[85] which all refer to the protection of the right to private and family life.

It is important, however, to point out that therefore other sets of rules exist in the Republic of Macedonia, such as tort law, criminal law[86] or antidiscrimination law under which a person claiming a privacy breach for data that do not clarify as "personal" (such as the anonymized, pseudo anonymized and encrypted data) may seek protection in a court procedure. The main reason for the existence of this possibility lies in the fact that the existing data privacy legislation does not provide extensive protection to individuals in those specific cases. However, the legislator recognizes that the cases involving abuse of anonymized, pseudo anonymized and encrypted data where various legitimate interests may be at stake and therefore they cannot fall out of the scope of the entire legal system.

81 Article 31(3) of the Data Privacy Act.

82 Example for this is the Macedonian cloud provider Unet, http://unetcloud.mk/6.UnetCloud.html (25/1/2016).

83 Article 8 ECHR: "Right to respect for private and family life 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

84 Article 25 of the Macedonian Constitution: each citizen is entitled to protection of the privacy its personal and family life and dignity.

85 The Article 5(3) of the Data Privacy Act: while keeping the personal data account should be taken for the protection of the personal and private life of the subject and all reasonable measures should be undertaken in order to anonymize the data.

86 Article 150 of the Criminal Code (Official Gazette of RM no. 37/1996, 80/1999, 48/2001, 4/2002, 16/2002, 43/2003, 19/2004, 40/2004, 81/2005, 50/2006, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015 and 226/2015) reads: There is no criminal act only if the secret has been revealed in general interest or in order to protect the the interest of a third person.

D. Conclusion

The cloud computing concept represents a novelty in today's internet relations. It is undisputed that this concept has numerous benefits for the individuals as well as for the businesses. However, these days there are many unclear issues connected with cloud computing and the protection of personal data. This especially if we take into consideration the fact that today one of the most important tasks of the cloud computing provider is to protect the stored data and not to allow circumvention of the data privacy rules.

In order not to be misunderstood, the starting point of this paper was that the protection of personal data is not hiding of certain data, but enabling the right of privacy which is granted by the ECHR, other conventions and most of the national constitutions and legal acts in the world. The starting premise reflects also to the contested issue whether the anonymized, pseudo anonymized and encrypted data are to be considered as "personal data" in light of the analyzed legislative framework.

In most clouds, data are significantly encrypted or even anonymized and as such it is questioned whether these data are even to be considered as "personal data", in particular on those who do not hold the encryption key. Some of the current European data protection regulators take the view they are and as such, in general, one recommends to treat encrypted data in practice as personal data, all the more since encrypted data must be decrypted for operations, with such operations constituting processing of "personal data".[87] This view may however be contested: it does not seem to be fair that a processor, who is holding encrypted data without holding the keys and as such is not aware of the contents and nature of these data, is required to comply with extensive data protection requirements. It is my position that whether encrypted data should be considered as personal data depends on the circumstances, particularly "the means likely reasonably to be used" (fair or foul) to re-identify individuals and the security of encrypted data against decryption.[88] The same goes for unencrypted or weakly encrypted data, for which two criteria can be considered: (1) the effectiveness of access control restrictions (i.e. the measures to prevent persons other than the user from accessing a user's data) and (2) any means for a provider to access personal data. The more secured the cryptography method, the less likely that information will be personal data. As such, one could argue that data processed by cloud providers may

87 Encrypted personal data remain personal data, and consequently, all data protection law requirements continue to apply to these data in anyone's hands, irrespective of key access or knowledge as to the data's nature; Article 29 Data Protection Working, Opinion 05/2012 on Cloud Computing, WP 196 (2012), as of 14/3/2014.

88 *Hon/Millard/Walden*, (fn. 17): What is Regulated as Personal Data in Clouds: Retraceable pseudo anonymized data, such as key-coded data, may remain personal data. Aggregating pseudo anonymized data, for examples through non-unique codes, may render data "anonymous" and enable cloud processing of anonymous data free of the Data Protection Directive. If pseudo anonymization indeed reduces risks for individuals, then data protection rules could be applied more flexibly and processing of these types of data may be subject to less strict conditions compared to processing of information regarding directly identifiable individuals.

be removed from the scope of data protection legislation on the condition that these data have been strongly encrypted by the controller before transmission and the provider cannot access the key and as such, individuals cannot be identified.[89]

The analyzed EU and Macedonian legal texts show that no precise interpretation of the notion of personal data is present. However, there is a consistency that the certain categories of data (such as the anonymized, pseudo anonymized and encrypted data) do not fall under the scope of the data privacy rules. Consequently, these data are not subject to the data privacy regime due to the fact that they are already protected per se by hiding/changing their identifying marks. In light of this it is important to point out that these types of data usually contain valuable information which resulted in the need of their anonymization in the first place. Therefore, account should be taken that in the hands of the right (or wrong) person, their availability and disclosure may lead to data privacy abuse. In order to avoid any such situation, it is extremely important for the National Data Privacy Authorities to assess every aspect of these data before classifying them as not being personal data and thus not subject to the stricter data privacy rules.

Considering this problematic issue and the undertaken steps on EU level, there is a tendency of moving forward with the proposal of the new regulation. It is encouraging that the draft regulation will bring a level of harmonization into the data protection regime within the EU.[90] However, the cloud realities show that much still needs to be done in order to reap the full potential of cloud computing in Europe.[91] First, there is a need for the legislators to understand the architecture and models of cloud computing. This inevitably affects the relationship between cloud providers and their users in light of their contractual relations. Therefore, it is not entirely true that the cloud contract terms are poor in regard to protection of certain categories of data, but data protection laws assume certain things which are not true in the cloud.[92] Reflecting privacy in a pragmatic way without disproportionately interfering with technological advancements is essential in this e-age.[93] On the other hand, reflecting all data privacy issues (including the interpretation of what is and what is not considered as personal data) appropriately will represent a step forward to regulating the collection and processing of data in the cloud. It is therefore our opinion that all of these missing links should be solved while the proposal of the regulation is still in debate.[94] Especially if we take into account the very own European Commission Action Plan, which underlines that

89 *Hellemans*, Legal Implications on Cloud Computing, Cloud for Europe Project Number FP7-610650, 2014, p. 17.
90 *Nwankwo*, (fn. 58), p. 34.
91 Ibid.
92 *Hon/Millard*, Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA?, The Cloud of Unknowing, Part 4, 2011.
93 *Pyykko*, Data Protection at the Cost of Economic Growth?" ECRI Commentary No. 11, November 2012, p. 2.
94 If, when and with which rules these legal framework will become reality is yet to be seen. However, in the following years 2017 and 2018 it is expected that the data privacy issues in the cloud computing will be strengthened. See *Niemann/Paul*, (fn. 55), p. 62.

> "in a global society characterized by rapid technological change where information exchange knows no borders, it is particularly important that privacy must be preserved. The Union must ensure that the fundamental right to data protection is consistently applied" (added remark: in its entirety).

On the other hand, it is considered that the on-going debate of data privacy is not of such intense interest in the Republic of Macedonia in general as well as in the expert public. The practical experience shows that the lack of interest and public discussions on this topic leaves certain questions unanswered. This analysis identified a few basic problems in the protection of data privacy in the Republic of Macedonia: the question of personal data is not being interpreted in light of the anonymized, pseudo anonymized and encrypted data, so conclusions can only be made by our free interpretation of the definition; the citizens are not familiar with their rights of data privacy; not every company has developed a data privacy corporate policy (the so called Binding Corporate Rules, which are also mandatory with the new regulation proposal), including but not limited to the companies with foreign capital operating in the territory of the Republic of Macedonia; the concept of data privacy issues on the Internet and specifically in the cloud environment is very vague etc.

Following the SAA and the adherence process towards the EU, the Republic of Macedonia will have to eventually implement these new rules in the Data Privacy Act and to broaden the level of data privacy protection. It is also important to primarily enforce the "soft measures" such as awareness raising campaign, campaigns for clarifying the data protection risks for individuals and businesses, joint activities of the Directorate with the Competition Authorities in regards to the drafting of the Binding Corporate Rules for international transfers, organizing public forums and discussions in order to establish the practical problems of the enforcement of the existing Data Protection Act, surveying the public opinion and similar activities which will ease the legislation making process and will bring it to the EU standards. However, in this entire process it will be very important to obtain the appropriate support from the competent EU authorities and legislation makers. Additionally, the Macedonian Directorate requires specific training for the complex data privacy issues (such as the anonymized, pseudo anonymized and encrypted data) and should also be able to gain access to the EU case law bases which will help their decision making process. The Macedonian Directorate should also work on strengthening its independence and powers, while requesting additional incentives for the offices that are currently not equipped with appropriate powers and adequate resources. Finally, the approximation of the laws should also extend to other elements of the *acquis*, especially over the e-transactions and the cloud environment which should be subject to in depth amendment either of the existing Data Privacy Act rules or it will require passing of new specific legislation.