ISSN 2029-7564 (online)
SOCIALINĖS TECHNOLOGIJOS
SOCIAL TECHNOLOGIES
2013, 3(2), p. 390–414.

EVALUATION OF LEGAL DATA PROTECTION REQUIREMENTS IN CLOUD SERVICES IN THE CONTEXT OF CONTRACTUAL RELATIONS WITH END-USERS

Darius Štitilis

Mykolas Romeris University, Lithuania, stitilis@mruni.eu

Inga Malinauskaitė

Mykolas Romeris University, Lithuania, inga.malinauskaite@mruni.eu

doi:10.13165/ST-13-3-2-11

Abstract

Purpose *– to analyse the compliance with basic principles of data protection in selected consumer oriented cloud services contracts, and also to highlight the adequate level of data protection in the mentioned contracts, evaluating existing data protection directive 95/46/EC, also proposed General data protection regulation.*

Design/methodology/approach – *various survey methods have been used in the work integrated. Documental analysis method has been used in analysis of scientific literature, legal acts and other documents, where aspects of legal data protection requirements have been included. Legal documents analysis method together with logical-analytic method has been used in analysing Directive 95/46/EU, Proposal for a regulation of the European Parliament and of the Council and jurisprudence of the European Court of Human Rights. Comparative method has been applied for revealing difference between particular cloud services contracts and also comparing the compliance of cloud services contracts to requirements of basic European data protection principles, established in the international documents.*

ISSN 2029-7564 (online)
https://www.mruni.eu/lt/mokslo_darbai/st/apie_leidini/
https://www.mruni.eu/en/mokslo_darbai/st/apie_leidini/index.php

Findings *– from the brief analysis of selected consumer oriented cloud service providers, it may be implied that more or less all the legal principles, established in the legal acts, are reflected in the privacy policies and/or service agreements. However, it shall be noted that there is a big difference in wording of the analysed documents. Regarding other principles, all examined cloud service providers do not have indemnification provisions regarding unlawful use of personal data.*

Research limitations/implications *– the concept of the contract was presented in a broad sense, including the privacy policies and/or terms and conditions of the service providers. In accordance with the content of the principles, the authors grouped data protection principles, applied in cloud services into fundamental and recommendatory.*

Practical implications *– the research results will be helpful for cloud service providers, dealing with personal data of data subjects (natural persons).*

Originality/value *– the mentioned research of cloud provider contracts examined 4 sets of standard terms and conditions of cloud service providers targeting individual consumers. The following personal data protection principles were evaluated: transparency, purpose specification and limitation, erasure of data, confidentiality, availability, integrity, indemnification.*

Keywords**:** *privacy and data protection, cloud services, compliance principles, legal regulation.*

Research type**:** *research paper, viewpoint, case study.*

1. Introduction

Cloud services have become one of the most popular topics of conversation among different communities. Quickly spreading global technological infrastructure raises variety of legal issues – applicable law, data portability, liability, copyright, etc. Some authors (Gervais, D. J. and Svantesson, D., 2012) indicate that one of the major challenges in cloud environment is the concern regarding data protection issues, which shall be explicitly analysed.

Based on the fundamental legal requirements, established in the European Union data protection directive 95/46/EU[1] (hereinafter – Directive 95/46/EU), the principles of data protection, applicable in the cloud environment, should be examined. However, Directive 95/46/EU was enacted at the times when cloud services did not exist. In addition, currently prepared Regulation of the European Parliament and the Council on the protection of individuals with the processing of personal data and on the free movement of persons[2] (hereinafter – general data protection regulation or regulation)

1 24 October 1995 Directive of the European Parliament and of the Council 95/46/EB on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [1995] O.L. L281/31.

2 European Commission. 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

should be examined, and with analysed data protection provisions contributed to the content of principles, applicable in the cloud services environment. Some aspects of application of legal principles in internet environment in the jurisprudence of European Court of Human Rights should be reviewed and presented, as well.

2. The concept and features of cloud services

Before presenting the major concern of data protection in cloud environment, the authors will briefly examine the definition of the phenomena, main features, advantages and disadvantages of cloud services. It is important to understand the theoretical concept of cloud services, to analyse the functional part of the technology in order to reveal the issue of privacy element in the context of contractual relations with end-users.

In general, it may be said that the definition of cloud services may be described in several ways. The majority of sources determine cloud services in a quit different manner, although the essence of the definition does not vary so much. In the opinion of European Commission, cloud computing is the storing, processing and use of data on remotely located computers accessed over the internet (European Commission Memo). The concept of cloud services is also established in Data protection review of the European Parliament. According to this document, cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Data Protection Review). In accordance to the opinion of some authors (Wittow, M.H. and Buller, D.J., 2010), cloud computing generally involves a subscription-based service that satisfies computing and storage needs from a virtually unlimited hardware and communication infrastructure, which is managed by a third party provider. In the opinion of the authors, cloud services may be defined as the complex structure, enabled by the internet, and by which services are provided for the end-user, also the end-user himself or herself is empowered to implement the majority of actions in quit simple and convenient environment of services management. The authors grounded their definition on further presented functional features of the phenomenon.

Using special software, the end-users connect their devices to a remote platform. In this platform, data processing is provided by huge data centres' with hundreds of servers and data storage systems, which are capable of interacting with any of the software, which is needed for the end-users. The European Commission Communication on Unleashing the Potential of Cloud Computing in Europe[3] (hereinafter – the Communication) establishes the following features in cloud services:

data. Brussels, 25 January 2012 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>.

3 European Commission. Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions. Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.9.2012 COM (2012) 529 final, p. 3-4 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf>.

- hardware (computers, storage devices);
- the use of hardware is dynamically optimised across a network of computers, so that the exact location of data or processes, as well as the information, which piece of hardware is actually serving a particular user at a given moment, does not in principle have to concern the user, even though it may have an important bearing on the applicable legal environment;
- cloud providers often move their end-users' workloads around (e.g., from one computer to another or from one data centre to another) to optimise the use of available hardware;
- remote hardware stores and processes data and makes it available, e.g., through applications;
- organisations and individuals can access their content and use their software when and where they need it, e.g., on desktop computers, laptops, tablets and smartphones;
- a cloud set-up consists of layers: hardware, middleware or platform, and application software;
- end-users normally pay by usage, avoiding the large upfront and fixed costs;
- at the same time, users can very easily modify the amount of hardware they use.

Based on the above listed features, the software functionality, enabled by cloud services, provides the services for the end-users, regardless of their location or the computer device they are using. In this way, users are becoming more and more independent from offices, homes and even from their existing computer equipment and the feature of extraterritoriality may be distinguished. Billhorn (2010) distinguished two separate methods of cloud services. The same methods were also mentioned in the Opinion on cloud computing of Article 29 data protection working party. First method is public cloud, available for public or big industries and which belongs to the company, delivering the services of cloud. Other method is personal (private) cloud services infrastructure, which belongs to one organisation, delivering cloud services, whereas the organisation itself or third party might be controlled any time and from any place. In this way, cloud services may be defined not only as technology, but also as products, an architecture and a business model. Cloud services mean an online environment (technology) of service creation and use which allows describing a complex structure.

Choo (2010) mentioned the lowest capital and running costs as the main advantages of cloud services. The end-user pays only for the actual used capacity on a "pay as you go" economic model. Therefore, the end-users avoid the expenses and time consuming tasks, such as buying software, maintaining hardware and taking care about storage of data. While talking about physical entities, the majority of cloud services' end-users refer to the simplicity and convenience as the principal features of usage of cloud services, also the availability to access the data from any computer device. The increasing popularity of Internet notebooks, or "netbooks", contributes to the end-users' choice to use the cloud. Netbooks are usually low-cost, lightweight laptop computers with reduced hardware capacity that are primarily designed to provide the user with access to the internet. The Communication of European Commission establishes the advantages of cloud services,

such as enhanced mobile working, productivity, standardisation, as well as new business opportunities[4].

Despite the cloud services benefits mentioned above, the end-users shall also take into account the technological, commercial and legal challenges, created by the new technology. First, the attention shall be taken to the fact that cloud services are the integral part of the internet and are directly dependant on the network. This means that if there are problems with internet connection, there will be delays or temporary terminations in delivering the cloud services. The end-users of cloud services are also dependant on traditional internet environment risks, such as technical mistakes, cybercrimes, etc.

Another big concern and also challenge in cloud services is closely related to the legal aspects of the phenomenon – data security[5] and confidentiality, and this is particularly important for the business companies, managing huge amount of confidential information. In cloud environment, end-users neither possess their data, nor control such data. Cloud users have no access to the physical hardware providing their storage and processor resources. The end-users trust that cloud services providers are taking risks of data loss and security seriously. Buller and Wittow (2010) stated that the users' expectations of security and reliability and the lack of direct control that the users have over the hardware providing the data and processing power present particularly challenging problems for the cloud services model. Data protection as the concern issue in cloud environment is also presented in the document of the European Commission, supplementing Communication on unleashing the potential of cloud computing in Europe.

As a result of the above presented challenges, ensuring the data protection issues in cloud environment is probably the most basic concern in the modern world. The authors further will discuss the legal data protection principals, which are applied (or should be applied) in the case of cloud services in the context of contractual relations with end-users. In addition, the authors will compare the compliance of the presented principles in chosen contracts and/or privacy policies with service providers regarding cloud services provision.

3. Legal principles and data protection in cloud services in the context of contractual relations with end-users

Deriving the privacy and data protection issues from the basic and fundamental human rights, the regulation of the mentioned concepts was always treated seriously by the legislators. The concept of protection of privacy and data protection dates back

4 European Commission. Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions. Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.9.2012 COM (2012) 529 final, p. 4 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf>.

5 Commission staff working document accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions.

to 1950, when the European Convention of Human Rights (ECHR)[6] was drafted. In this document, the protection of privacy and data protection was codified as one of the fundamental human rights. The expanded concept of privacy and data protection is established in the EU Charter of Fundamental Rights (EUCFR)[7], proclaimed in 2000. The EUCFR became binding with full legal effect in all countries of European Union since the Lisbon Treaty's entry into force in 2009. The comprehensive legal regulation of data protection and privacy is established in data protection Directive 95/46/EC and in future directly applicable General data protection regulation. The European Commission is to finalize and adopt the new framework in 2014. The historical development of legal instruments regulating privacy and data protection principles shows that these issues are treated with high respect and codified as imperative legal norms. The importance of protection of privacy is also largely stressed in the jurisprudence of the European Court of Human Rights. The Court stated in *S. and Marper v. The United Kingdom* (2008)[8] that the protection of personal data is of fundamental importance to a person's enjoyment of his right to respect for private and family life. From the evolution of the content in different legal instruments regulating data protection issues, it may be presumed that existing legal framework does not always adequately interact with new forms of technology deployment, e.g., cloud services. For this reason, the future oriented General protection regulation draws the new guidelines for data protection regulation, emphasizing the aspects of globalization and technology developments. The General data protection regulation provides stricter data protection legislation cloud customers and cloud providers could face. Considering new technologies issue, the European Court of Human Rights refers to the definition of informational privacy, which presumably would include the privacy of access to the Internet[9].

This article will further discuss data protection legislation and its consequences on cloud services, and therefore, for practical reasons, the authors will only focus on data protection legal requirements in the context of contractual relations with end-users.

Legal requirements may be defined as a set of rules, stated in the regulations, and in which are established the forms of possible activities and techniques. Legal requirements, related to the privacy and insurance of data protection in cloud environment in the context of contractual relations with end-users, are derived from data protection Directive 95/46/EC. Since in the Directive 95/46/EC there are no special rules regulating cloud services, in order to emphasize the specific legal requirements of the examined object, the principles, set in the Directive 95/46/EC, will be considered. In addition, since in the immediate term the Directive 95/46/EC is intended to be replaced by the

---

6 Council of Europe. European Convention on Human Rights. Rome, 4 November 1950 [interactive]. [accessed on 20-09-2013]. <http://www.echr.coe.int/Documents/Convention_ENG.pdf>.

7 The European Parliament. European Union Charter of Fundamental Rights. The Council and the Commission, 2000 [interactive]. [accessed on 20-09-2013]. <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

8 S.and Marper v. The United Kingdom [GC], Nos. 30562/04 and 30566/04, § 41, 4 December 2008. Council of Europe, 2011 [interactive].[accessed on 20-09-2013]. <http://echr.coe.int/Documents/Research_report_internet_ENG.pdf>.

9 Internet: Case-law of the European Court of Human Rights. Council of Europe, 2011 [interactive]. [accessed on 20-09-2013]. <http://echr.coe.int/Documents/Research_report_internet_ENG.pdf>.

currently prepared general data protection regulation, principles, set out in the proposal for regulation, will be presented in the article.

The word principle is derived from the Latin word principium and has the meaning of start, foundation. In the most common sense, principle is understood as guiding sense of requirements in the particular phenomenon underlying the content, specific manifestations of individual elements. In accordance to the dictionary, legal principles are the principles underlying the formulation of jurisprudence. According to the examination of different data protection principles, applied for cloud services and established in legal acts, it can be noticed that these principles should ensure the successful and effective background in cloud services. These principles are important for several reasons. First, they are the guidelines cloud services providers and end-users shall comply with. Second, the principles are more general, they do not necessary define each new situation. Third, the principles implement the function of filling the legal gaps, and fourth, the principles help to unify and improve cloud services strategies. Moreover, they should be taken into account when interpreting arisen practical situations.

Considering the fact that cloud services are usually provided by the companies and sometimes big enterprises, it is obvious that arising issues of privacy and personal data protection brings a lot of uncertainty and lack of confidence for the end-users, at the same time threatening the smooth development of information society. In the article, the European Union's data protection principles in the context of cloud services will be presented so far, as related to the contracts with end-users – transparency, purpose specification and limitation, erasure of data immediately after they are not needed. It should be noted that in the article, the contracts with the end-users are understood in a broad sense. The concept of the contracts also includes the privacy policies and/or terms and conditions of the service providers.

The following part will present particular data protection principles, applicable in a cloud services environment and the binding nature of them in the cloud services contracts. Taking into account the content of the principles, the authors grouped data protection principles, applicable in cloud services into fundamental and recommendatory.

3.1. Fundamental principles in cloud services contracts

Fundamental data protection principles establish the basic and most important provisions of personal data to ensure the appropriate and adequate level of data protection. The lawfulness of the processing of personal data in the cloud depends on the adherence to the basic principles of data protection law. In the opinion of the authors, these principles shall be imperatively included into each cloud services contract in order to ensure the essential data protection.

Transparency

Transparency is one of the main features in order to ensure fair and legitimate processing of personal data. Directive 95/46/EC obliges the cloud service provider to deliver a data subject from which data relating to him are collected with information on

his identity and the purpose of the processing[10]. The cloud service providers should also give any further information, such as on the recipients or categories of recipients of the data, which can also include processors and sub-processors in so far as such information is necessary to guarantee fair processing in respect of the data subject. As it is stated in the Opinion on cloud computing of the Article 29 data protection working party, transparency in the cloud means it is necessary for the cloud service provider to be made aware of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centres personal data may be processed at. [11]

On the other hand, Article 12 of Directive 95/46/EC describes the conditions, under which a cloud services end-user has the right to obtain information, including, but not limited to, approval, whether the data, related to the end-user of services is being processed and information at least as related to the purposes of the processing, the categories of end-users to whom the data is disclosed, or categories; notice in an understandable form about the processed data and about any available information, related to the data resources.

In the case the end-user is properly informed in accordance to the provisions of Directive 95/46/EC, the end-user may become an active in evaluation of the transparency in cloud environment. Contrary, if the end-user is not informed or is informed insufficiently due to the conditions of Directive 95/46/EC, there is a breach in rights of the end-user and it increases the situation of legal uncertainty and confidence. In addition, as it is referred in the Opinion on cloud computing of Article 29 data protection working party, if, for instance, the provision of the service requires the installation of software on the end-user's systems, the cloud service provider should as a matter of good practice inform the client about this circumstance and in particular about its implications from a data protection and data security point of view. Vice versa, the end-user should raise this matter ex ante if it is not addressed sufficiently by the cloud service provider[12].

General data protection regulation also establishes the principle of transparency. In Article 11 of the regulation, it is stated that the controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of end-users rights. The controller also shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the end-user. Where personal data relating to the end-user is collected, Article 14 of the regulation establishes

---

10 24 October 1995 Directive of the Parliament and of the Council 95/46/EB on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [1995] O.L. L281/31.

11 European Commission. European Union Data Protection Directive 95/46/EC Article 29 data protection working party opinion 05/2012 on cloud computing. Brussels, 1 July 2012, p. 11 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>.

12 European Commission. European Union Data Protection Directive 95/46/EC Article 29 data protection working party opinion 05/2012 on cloud computing. Brussels, 1 July 2012, p. 11 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>.

the imperatively provided information amount, which should be submitted to the end-user by the data controller. Such defined information amount consists of information, including, but not limited, to the purposes of the processing, for which the personal data are intended, including the contract terms and general conditions, where the processing is based; the period for which the personal data will be stored; the recipients or categories of recipients of the personal data. On the other hand, based on Article 15, the end-user shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. In addition, regulation establishes the imperatively provided information by data controller. Such information includes the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom the personal data are to be or have been disclosed; the period for which the personal data will be stored and other data.

Transparency is closely linked to the principle of democracy, which is established in Article 6 of the Treaty of the European Union as one of the fundamental principles of EC Law. The relevant jurisprudence of the Court of the European Union and of the General Court (hereinafter – the Courts) regarding the application of transparency principle in cloud environment is rare; however, transparency as a general principle of European Union law is significantly interpreted. In this context, the Courts ruled that the relevant exceptions of the transparency principle are to be interpreted and applied as restrictively as possible[13]. In the European Union law context, transparency principle is also related to the principle of legal certainty, which is recognized as a general principle of Community.

According to the above mentioned specific content and the wording in legal acts of the European Union of transparency principle, it should be concluded that the transparency principle should be established in a cloud services contract as one of the binding contractual obligations from the service provider side. Such establishment of transparency principle would increase the end-users' legal certainty and confidence in the whole environment of cloud services provision.

Purpose specification and limitation

The principle of purpose specification and limitation requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Article 6(b) of Directive 95/46/EC)[14]. The same principle is also established in the General data protection regulation (Article 5(b)).

Cloud service provider must define the purpose of data collection before starting to collect data from the end-user and to inform the end-user about these circumstances. The service provider shall not transfer data for other purposes than those obviously defined and

13 European Court of Justice C-353/99, Case Council/ Hautala, 2001, I-9565, para. 25; European Court of Justice, Joined Cases C-174/98 και C-189/98 (Netherlands and van der Val/Commission), 2000, I-1, para. 27; European Court of Justice C-64/05, Case Sweden/Commission (IWAF-1), 2007, I-11389, para. 66.

14 24 October 1995 Directive of the Parliament and of the Council 95/46/EB on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [1995] O.L. L281/31.

identified. In addition, data shall be adequate, relevant and not excessive in relation to the purposes, for which they are collected and/or further processed (Article 6(c) of Directive 95/46/EC). The authors presume that the purpose specification and limitation principle shall be one of mandatory conditions in cloud services agreements. The end-user shall be ensured that personal data would not be unlawfully processed for other purposes than those defined in the provisions of cloud services providers and subcontractors. As usual, cloud environment model may easily involve a large number of subcontractors and the risk of processing of personal data for further, incompatible purposes must, therefore, be assessed as being quite high. According to the opinion on cloud computing of Article 29 data protection working party, in order to minimise the risk, the contract between cloud provider and end-user should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of cloud provider or subcontractors. The Opinion also states about the imposition of penalties in the contract against the provider or subcontractor if data protection legislation is breached.

Erasure of data

In accordance to the Article 6(e) of Directive 95/46/EC, personal data shall be kept in a form, which permits identification of data subjects for no longer than it is necessary for the purposes for which the data were collected or for which they are further processed[15]. Personal data that are not necessary any more shall be erased or truly anonymised. If this data cannot be erased due to legal retention rules, access to this personal data should be blocked. It shall be noted that erasure of data is important for both cases – during the cloud services contract period and after its termination. The principle of erasure of data principle is also important in case of change of subcontractor. The principle of erasure of data applies to personal data regardless of the location and manner of storage of data, e.g., if personal data is kept redundantly on different servers locations, it must be ensured that each instance of them is erased irretrievably. Temporary files and even fragments are to be deleted, as well.

The end-users shall be aware of the fact that log data, modifications or erasure of data also qualify as personal data relating to the person who initiated the respective processing operation.

Article 17 of the general data protection regulation establishes the right of end-users to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data, which are made available by the end-users while he or she was a child. The general data protection regulation states the grounds, according to which the end-user is able to request the erasure of his or her personal data. These grounds include the circumstances, whereas the data are no longer necessary in relation to the purposes, for which they

15 24 October 1995 Directive of the Parliament and of the Council 95/46/EB on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [1995] O.L. L281/31.

were collected or otherwise processed; the data subject withdraws consent, on which the processing is based; the data subject objects to the processing of personal data; the processing of the data does not comply with this General data protection regulation for other reasons.

Following the established provisions of legal acts, it may be concluded that cloud services providers shall ensure secure erasure in the above-mentioned sense and cloud services contract contains clear and binding provision for the erasure of personal data. The same shall be applied for the contracts between cloud providers and subcontractors.

3.2. Recommended principles in cloud services contracts

A further part of this article will present data protection principles, which are relevant in the cloud environment. The authors believe that the following legal principles as of their content and features should be treated as recommended conditions for cloud services contracts.

Confidentiality

In cloud environment, most of the data by the end-user is being transferred for the service provider. In doing so, the end-users want to be assured that the service provider is using the data only for service use and/or will not disclose them without the end-user's consent. The assurance of service provider that the data will be transferred and stored complying with the requirements of privacy and confidentiality should be clearly set out in the terms of cloud services contracts. Such obligation is established in Article 16 of the Directive 95/46/EC, stating that any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process them, except on instructions from the controller, unless he is required to do so by law. Some researchers (Rong, Z.; Minqi, Z.; Aoying, Z.; Weining, Q.; Wei, X., 2010) distinguished two basic approaches of confidentiality in cloud services – physical isolation and cryptography.

The working group of Article 29 of Directive 95/46/EC emphasizes the importance of encryption of personal data in cloud environment[16]. However, encryption may contribute to the confidentiality of personal data protection, if used in a correct way, not rendering personal data irreversibly anonymous[17]. Also, personal data encryption could be used for data transit and transfer of data, e.g., transfer of medical records into cloud in the context of Article 8 Directive 95/46/EC (the processing of special categories of data), having in mind the particular question of professional secrecy.

---

16 European Commission. European Union Data Protection Directive 95/46/EC Article 29 data protection working party opinion 05/2012 on cloud computing. Brussels, 1 July 2012, p. 1 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>.

17 According to the Directive 95/46/EC preamble clause 26, whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

In some cases (e.g., IaaS storage service), cloud end-user cannot rely on cryptography service, offered by service provider; however, in this case, the end-user may encrypt the data himself or herself before sending it to the service provider.

Other technical measures, established in the Opinion on cloud computing of 29 Article data protection working party in order to protect confidentiality, include authorization mechanisms and strong authentification. Keeping in mind the above mentioned circumstances, it may be concluded that assurance of personal data confidentiality in cloud services contracts with end-users, which is an important and one of the recommended conditions. Service provider wants to be sure that the data will be transferred and stored in accordance with the privacy and confidentiality requirements and, in the authors' opinion, such contractual clause would be advisable to include into each cloud services contract.

The principle of confidentiality is also established in the jurisprudence of the European Court of Human Rights. In the *K.U. v. Finland* (2008) case, the court commented that although freedom of expression and confidentiality of communications were primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression would be respected[18].

Availability

Providing availability means ensuring timely and reliable access to personal data. Each end-user of cloud services wants to be sure that, if necessary, he or she will have easy access to their data. It should also be noted that the principle of availability in practice is associated with specific risks. One special threat to availability in the cloud is accidental loss of network connectivity between the end-user and the service provider or of server performance caused by malicious actions, such as (Distributed) Denial of Service (DoS) attacks[19]. Other availability risks include accidental hardware failures both on the network and in the cloud processing and data storage systems, power failures and other infrastructure problems. Therefore, the end-users, before starting to use cloud services, shall check whether the cloud service provider has adopted reasonable measures to settle the risks. The service provider, in accordance to the provisions of the general data protection regulation, shall take appropriate technical and organisational measures in order to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any kind of unlawful processing of data. In the context of the analysed principle, the authors believe that cloud services contract shall include contractual clause on the service provider's effort to ensure that the end-users should be enabled easily access their personal data and that the service provider will make every effort to protect personal data against destruction and/or loss.

---

18 K.U. v. Finland, No.2872/02, § 43, 2 December 2008. Council of Europe, 2011 [interactive]. [accessed on 20-09-2013]. <http://echr.coe.int/Documents/Research_report_internet_ENG.pdf>.

19 A DoS attack is a coordinated attempt to make a computer or network resource unavailable to its authorised users, either temporarily or indefinitely.

Integrity

Integrity may be defined as the property that data is authentic and has not been maliciously or accidently altered during processing, storage or transmission[20]. Some authors (Rong, Z.; Minqi, Z.; Aoying, Z.; Weining, Q.; Wei, X., 2010) refer that keeping data integrity is a fundamental task in providing cloud services. Detecting alterations to personal data can be achieved by cryptographic authentification mechanisms, such as message authentification or signatures. According to the general data protection regulation, the controller and the processor shall, following an evaluation of the risks, take the measures referred to in Paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data (Article 30(2)). An examination of this principle reveals that it would be highly recommended to include the principle of data integrity into cloud services contract describing the service provider's liability in respect for the end-user to take all possible measures for the assurance of data integrity.

Indemnification

During the examination of specific personal data protection principles, applicable in cloud services environment, it was observed that indemnification issue and/or liability for failure to comply with the legal principles is extremely important. Directive 95/46/EC establishes that Member States shall provide that any person, who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive, is entitled to receive compensation from the controller for the damage suffered (Article 23(1)). The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage (Article 23(2)). The general data protection regulation also states that any person, who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this regulation, shall have the right to receive compensation from the controller or the processor for the damage suffered (Article 77(1)). In the case of several providers, the regulation establishes that where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage (Article 77(2)). The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage (Article 77(3)). The authors believe that it is highly recommended to include the contractual provision of indemnification of service provider, protecting the right of end-user to receive compensation if data protection provisions are breached.

---

20 European Commission. European Union Data Protection Directive 95/46/EC Article 29 data protection working party opinion 05/2012 on cloud computing. Brussels, 1 July 2012, p. 15 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>.

4. Practical analysis of cloud service provider contracts

In the following section of the article, the authors investigate practical aspects of personal data protection principles in cloud services in the context of end-user contracts. In order to evaluate the compliance with basic personal data protection principles, practical examples of selected cloud services providers are accessed. Taking into consideration the presented features and the definition of cloud services, the authors for the practical case study have chosen the following cloud services providers, delivering services for the consumers, as well as for the business enterprises in the European Union: Google, Dropbox, Amazon and Rackspace. They are among the biggest cloud services providers, and the contracts with end-users and their conditions have the significant amount for the wide range of consumers. Therefore, the analysis of the provisions of the public contracts in the context of the compliance with the data protection legal principles while delivering cloud services shall be interesting and valuable.

The object of the research – cloud services provider contracts, including privacy terms and/or policies.

The purpose of the research – evaluation and investigation of selected services provider contracts with end-users.

Several different methods were used to carry out the research. The authors used the method for the analysis of provisions of end-users contracts regarding cloud services. The comparative method was used to reveal the difference between selected cloud services contracts. Also, the method of analysis, together with the comparative method, allowed exploring the compliance of the provisions of selected cloud provider contracts to the basic European data protection principles. Using sources of scientific literature, the authors deployed a deduction method, which enabled arriving at sufficiently reliable conclusions.

For the purpose of the research, several of the most popular consumer-focused cloud services providers, also their end-users contracts were selected. The selected cloud services providers included the following: Amazon, Google, Dropbox and Rackspace. These providers deliver cloud services also to European consumers; therefore, it is important to assess the compliance with the European data protection principles.

Contracts are the main tools whereby providers set the terms of their relationship with customers, called Service Level Agreements (SLAs) or End User Agreements (EULAs). Privacy terms and conditions appear separately or incorporated into the others. The authors examined consumer-based cloud contracts, including privacy terms.

Thus, the mentioned research of cloud provider contracts examined 4 sets of standard terms and conditions of cloud services providers targeting individual consumers. The following personal data protection principles were evaluated: transparency, purpose specification and limitation, erasure of data, confidentiality, availability, integrity, indemnification. As it was stated above, taking into account the content of the principles, the authors grouped data protection principles, applicable in cloud services, into fundamental and recommendatory. This might be seen from the following structural figure (Figure 1).

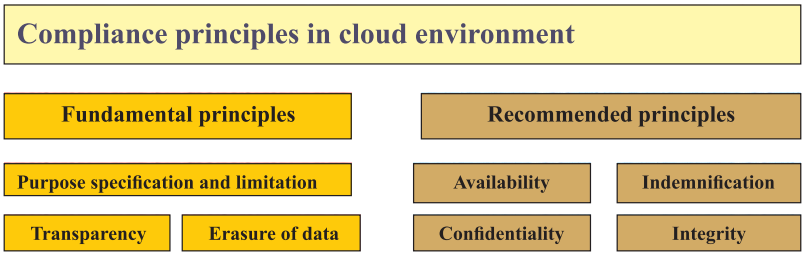

Figure 1. Compliance principles in cloud environment

Table 1. Evaluation results of legal data protection principles in Amazon cloud services contracts

Privacy policy/ Agreements / Legal principles	Amazon
1. Transparency	**Implemented.** Amazon informs its customer about the collected information. Collected information comprises of different types of information: data, received from the customers, automatic information, mobile, e-mail communications, information from other sources. Amazon specifies the ways in which it shares collected information about customers with affiliated business, third party service providers, promotional offers, business transfers. Amazon also informs its customer about the ways it releases personal information when it is appropriate with the compliance of law. In other cases, the customer has an opportunity to choose about sharing personal information.
2. Purpose specification and limitation	**Implemented.** Amazon uses the information that customer provides for purposes, such as responding to customer's requests, customizing future shopping for the customer, improving Amazon's stores, and communicating with the customer.
3. Erasure of data	**Implemented.** There is no provision, stating that personal data that are not necessary any more must be erased or truly anonymised. However, Help feature states that customers can disable or delete data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Web site of its manufacturer.
4. Confidentiality	**Half implemented.** There is no statement in the privacy policy. Amazon's Customer Agreement specifies the definition of confidential information. Also, the Customer Agreement defines the use of confidential information. However, the wording of the provisions makes binding the obligations of the end-users' and not the undertakings of the service provider.

5. Availability	**Implemented.** Amazon's privacy notice states explicit examples of information that the customer can access easily. Such information consists of including, but not limiting, to up-to-date information regarding recent orders, personally identifiable information, payment settings, e-mail notification settings, etc.
6. Integrity	**Implemented.** Amazon's privacy notice does not specify any integrity principle; however, Amazon Customer Agreement provides that Amazon will implement reasonable and appropriate measures designed to help the customer secure customer's content against accidental or unlawful loss, access or disclosure.
7. Indemnification	**Not implemented.** Amazon's privacy notice does not specify any sanctions, responsibility for the unlawful use of data. In addition, Amazon Customer Agreement states the limitation of liability that Amazon and their affiliates or licensors will not be liable to the customer for any authorised access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of customer content or other data.

The results are also represented in Figure 2*:

*In all the following figures (2, 3, 4 and 5) column scale with a numbering expression is used. Number 1 means thorough compliance with the referred data protection principle, number 0,5 means half compliance with the referred data protection principle, etc.

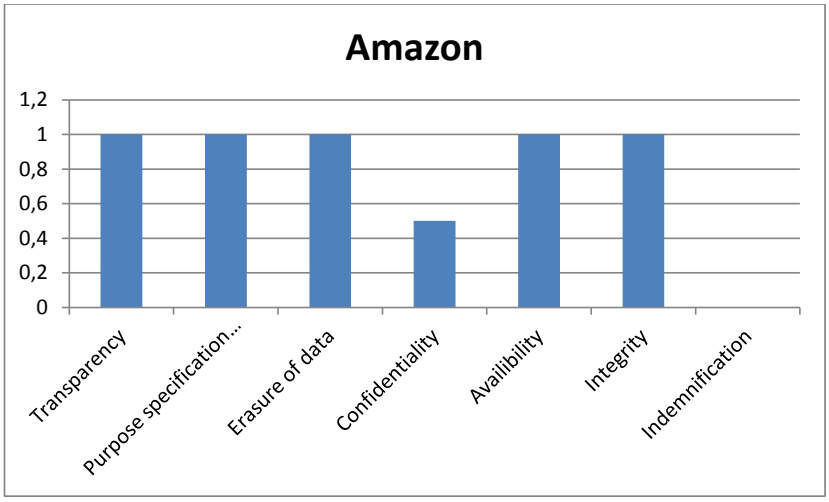

Figure 2. Evaluation of legal data protection principles in Amazon cloud services contract

Table 2. Evaluation results of legal data protection principles in Google cloud services contracts

Privacy policy/ Agreements / Legal rinciples	Google
1. Transparency	**Implemented.** Google comprehensively informs its customer about the collected information. Collected information comprises of different types of information: account data of customer, usage data, device information, log information, location information, unique application numbers, local storage. Google also informs its customer about the usage of collected information. The customer is also enabled to make meaningful choices about how information is used including, but not limited to, review and control, view and edit, use Google's editor, control and take information out. Google also states the types of specific information it shares with companies, organisations and individuals outside Google.
2. Purpose specification and limitation	**Implemented.** Google obviously specifies the goal – collection of information to provide better services to all of users – from basics, such as which language customer speaks to more complex things, such as which ads customer will find most useful or the people who matter the most to the customer online.
3. Erasure of data	**Implemented.** As it was stated above, Google enables its customer himself/herself to take information out of Google. Also, in Google privacy policy, there is a provision stating that if information is wrong, Google strives to give its customer ways to update it quickly or to delete it – unless Google has to keep that information for legitimate business or legal purposes.
4. Confidentiality	**Implemented.** Google's privacy policy establishes that Google restricts access to personal information to Google employees, contractors and agents, who need to know that information in order to process it for Google and who are subject to strict contractual confidentiality obligations. The policy also states that processing of personal information for the third parties is based on the compliance with Google's privacy policy and any other appropriate confidentiality and security measures. Google Cloud storage Terms of Service also provides the definition of confidential information and Google's obligation in regard to this information.

5. Availability	**Implemented.** Google's privacy policy establishes that whenever its customer uses Google's services, Google aims to provide the customer with access to customer's personal information. Google also informs its customer that if customer's Google Account is managed for the customer by a domain administrator, then customer's domain administrator and resellers who provide user support to customer's organisation will have access to customer's Google Account information.
6. Integrity	**Implemented.** Google's privacy policy establishes the statement about information security. It emphasizes that Google works hard to protect Google and users from unauthorised access to or unauthorised alteration, disclosure or destruction of information that Google holds. The policy also specifies particular measures, including, but not limited to, the encryption and verification.
7. Indemnification	**Not implemented.** Google's privacy notice does not specify any sanctions, responsibility for the unlawful use of data. Google SQL Terms of Service specify that Google and its suppliers are not responsible or liable for the deletion of or failure to store any customer data and other communications maintained or transmitted through the use of the services. It is also stated that the customer is solely responsible for securing and backing up its application, project and customer data.

The results are also represented in Figure 3*:

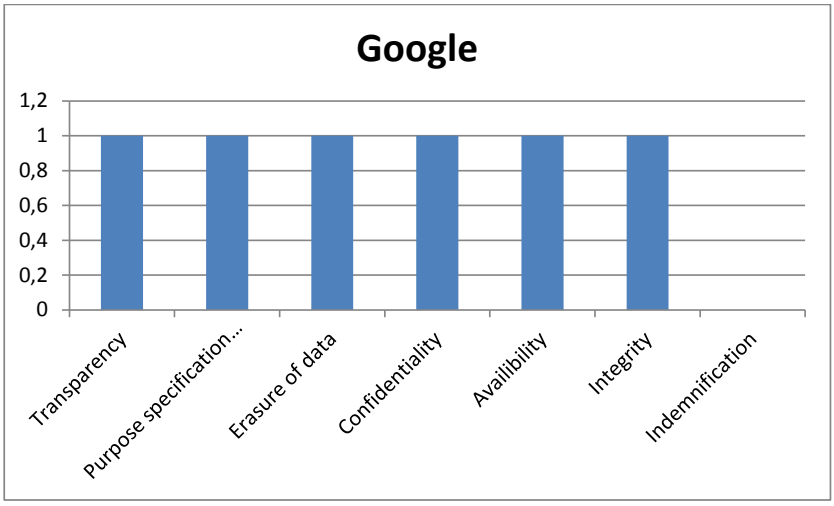

Figure 3. Evaluation of legal data protection principles in Google cloud services contract

Table 3. Evaluation results of legal data protection principles in Dropbox cloud services contracts

Privacy policy/ Agreements / Legal principles	Dropbox
1. Transparency	**Implemented.** Dropbox informs its customer about the collected information. Due to the terms of the privacy policy, information is collected in a number of ways: providing customer's personal data, uploading files, collecting data through the use of the service, collecting data through cookies. The privacy policy also provides the list of collected information, including, but not limited to, customer's name, e-mail address, credit card number, billing address, etc. The policy also provides that Dropbox may share some of customer's information with third-party applications, but only if the customer chooses to use those applications.
2. Purpose specification and limitation	**Implemented.** Dropbox uses information either for provision of services to the customer or improvement of the services. Dropbox also uses some of data for its own analytics purposes. In addition, the customer is enabled to choose not to have customer's data accessed by analytics.
3. Erasure of data	**Implemented.** Dropbox privacy policy enables its customer to review, update, correct or delete his/her personal information. Also, if customer's personally identifiable information changes, or if the customer no longer desires Dropbox service, he/she may update or delete it by making the change on customer's account settings.
4. Confidentiality	**Half implemented.** There is a statement in the Dropbox's privacy policy concerning confidential information. However, it is a difference between private and non-private information. The policy states that Dropbox may disclose customer's non-private, aggregated, or otherwise non-personal information, such as usage statistics of Dropbox Service.
5. Availability	**Implemented.** Dropbox's terms and conditions provide that the company is in the business of holding on to customer's personal files, so the customer can access them from anywhere or easily share them with others.

6. Integrity	**Implemented.** Dropbox in the privacy policy has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement. There is a link to the program provided and contacts for the raised possible questions.
7. Indemnification	**Not implemented.** Dropbox's privacy notice does not specify any sanctions, responsibility for the unlawful use of data. In the terms of services, there are statements whereas Dropbox limits its liability. For instance, if the customer uses some kind of apps, he/she is subject to provider's terms and policies, and Dropbox is not responsible for what they do with customer's data.

The results are also represented in Figure 4*:

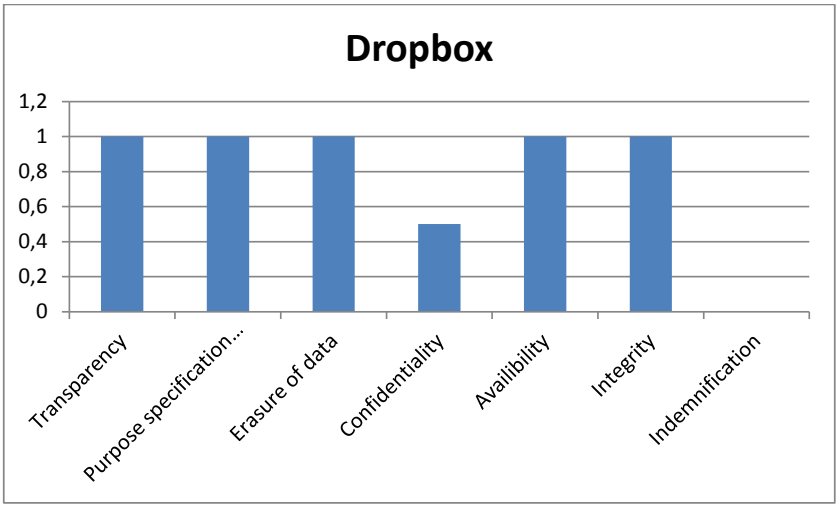

Figure 4. Evaluation of legal data protection principles in Dropbox cloud services contract

Table 4. Evaluation results of legal data protection principles in Rackspace cloud services contracts

Privacy policy/ Agreements / Legal principles	Rackspace
1. Transparency	**Half implemented**. Rackspace informs its customers about the transfer of personal data for third parties – affiliates and subcontractors. Rackspace informs its customers about collecting and storing information related to customer use of the Services, such as the use of SMTP, POP3, IMAP, and filtering.

	However, all the wording in the cloud term of services is not structured in a way favourable for the customer and might be identified as the business disclaimer. For instance, "You agree that we may use this information for our general business purposes and may disclose the information to third parties in aggregate statistical form, provided that we do not include any information that could be used to identify you."
2. Purpose specification and limitation	Not implemented. There is no obvious provision, stating the usage of collected data in the cloud term of services. Rackspace cloud terms of services establish that the customer agrees that Rackspace may use his/her information for their general business purpose.
3. Erasure of data	**Not implemented.** There is no provision, stating that personal data that are not necessary any more must be deleted.
4. Confidentiality	**Implemented.** Rackspace defines that both Rackspace and its customer agree not to use the other's Confidential Information, except in connection with the performance or the use of Services, as applicable, the exercise of respective legal rights under the Agreement, or as may be required by law. Also, they agree not to disclose the other's Confidential Information to any third parties, except in defined cases.
5. Availability	**Implemented.** Rackspace's cloud terms of services specify separate sections on access to data. Its customer will not have access to Customer's data stored in the Services during a suspension or following termination.
6. Integrity	**Not implemented.** Rackspace does not have knowledge of the data its customer stores within the Rackspace cloud system, including the quantity, value or use of the data. The customer is, therefore, responsible to take all reasonable steps to mitigate the risks inherent in the provision of the Services, including data loss.
7. Indemnification	**Not implemented.** Rackspace cloud terms of services do not specify any sanctions, responsibility for the unlawful use of data. Contrary, as it was already mentioned, Rackspace disclaimers constitute the biggest part of the provisions. The customer acknowledges that there are risks inherent in internet connectivity that could result in the loss of customer's privacy, customer data, confidential information, and property.

The results are also represented in Figure 5*:

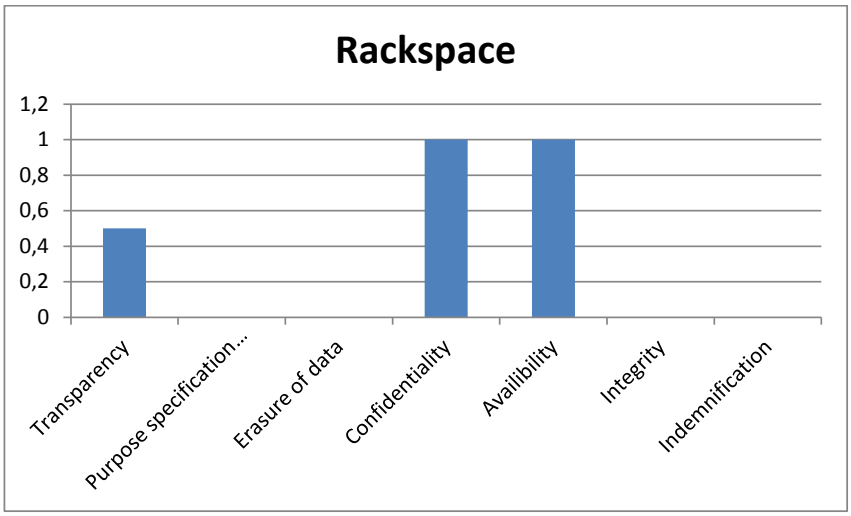

Figure 5. Evaluation of legal data protection principles in Rackspace cloud services contract

Summarizing the above mentioned statements, the overall results are as follows:

Privacy policy/ Agreements / Legal principles	Amazon	Google	Dropbox	Rackspace
1. Transparency	Implemented.	Implemented.	Implemented.	Half implemented.
2. Purpose specification and limitation	Implemented.	Implemented.	Implemented.	Not implemented.
3. Erasure of data	Implemented.	Implemented.	Implemented.	Not implemented.
4. Confidentiality	Half implemented.	Implemented.	Half implemented.	Implemented.
5. Availability	Implemented.	Implemented.	Implemented.	Implemented.
6. Integrity	Implemented.	Implemented.	Implemented.	Not implemented.
7. Indemnification	Not implemented.	Not implemented.	Not implemented.	Not implemented.

5. Conclusion

Before starting to analyse one of the major concerns in cloud environment – privacy and data protection issues, the article provides the comprehensive introductory part of the cloud services phenomenon. The authors introduced the definition of cloud services, main features of cloud services, advantages and major risks. The article mainly focused on one of the currently most actual concerns in cloud – data protection issue.

After the brief presentation of the legal documents, in which imperative norms regulating data protection and privacy issues are established, the authors presented legal requirements of data protection in cloud services in the context of contractual relations with end-users. Principles, applicable in a cloud services environment, were grouped into two main categories – essential principles and recommended principles. The essential principles include transparency, purpose specification and limitation and erasure of data. The recommended principles include confidentiality, availability, integrity and indemnification. The brief content of each principle established the grounds for possibilities of inclusion of each principle into the cloud services contracts.

From the brief analysis of the selected consumer oriented cloud services providers, it may be noted that more or less all legal principles, established in the legal acts, are reflected in the privacy policies and/or service agreements. However, it shall be noted that there is a big difference in wording of the analysed documents, e.g., Rackspace expresses policy statements in a way, which is more or less similar to the wording of disclaiming, and therefore, not being favourable for the customers. Google's policy expressions are user-friendly, involving customers to the data controlling process. Dropbox privacy policy also transfers lots of activities in controlling customers' data to the customers. Dropbox policy establishes contacts and customers may reach their provider easily asking raised questions regarding data privacy. All four cloud service providers do not have indemnification provisions regarding unlawful use of personal data.

References

24 October 1995 Directive of the Parliament and of the Council 95/46/EB on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [1995] O.L. L281/31.

Billhorn, J. *Cloud Computing Tips for Small Business*. 19 September 2011 [interactive]. [accessed on 20-09-2013]. <http://www.smallbusinesscomputing.com/biztools/article.php/10730_3939301_2/Cloud-Computing-Tips-for-Small_Business.htm>.

Buller, D.J. and Wittow, M.H. 2010. Cloud Computing: Emerging Legal Issues for Access to Data Anywhere, Anytime. *Journal of Internet Law*. (14, 1): 5. Aspen Publishers [interactive]. [accessed on 20-09-2013]. <http://www.klgates.com/files/Publication/9a019700-dd61-4f6d-ac05-027175530c50/Presentation/PublicationAttachment/e4a28659-de04-4223-bcee-048ec955fe03/Journal_Internet_Law.pdf>.

Case *Council/ Hautala,* 2001, I-9565, para. 25, European Court of Justice; Joined Cases C-174/98 και C-189/98 (Netherlands and van der Val/Commission), 2000, I-1, para. 27, European Court of Justice; C-64/05,

Case *Sweden/Commission* (IWAF-1), 2007, I-11389, para. 66, European Court of Human Rights [interactive]. [accessed on 20-09-2013]. <http://www.echr.coe.int/Documents/Short_Survey_2008_ENG.pdf>.

Choo, K.K.R. 2010. *Trends and Issues in Crime and Criminal Justice*. Australian Government, Australian Institute of Criminology [interactive]. [accessed on 20-09-2013]. <http://aic.gov.au/documents/C/4/D/%7BC4D887F9-7D3B-4CFE-9D88-567C01AB8CA0%7Dtandi400.pdf>.

Commission staff working document accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions.

Council of Europe. European Convention for Protection of Human Rights and Fundamental Freedoms, adopted 4 November 1950, entered into force 3 September 1953 [interactive]. [accessed on 20-09-2013]. <http://www.echr.coe.int/Documents/Convention_ENG.pdf>.

Data Protection Review: Impact on EU Innovation and Competitiveness. European Parliament, Brussels, December 2012 [interactive]. [accessed on 20-09-2013]. <http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=78970>.

Dictionary.com [interactive]. [accessed on 20-09-2013]. <http://dictionary.reference.com/browse/legal+principle>.

European Commission. Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the regions. Unleashing the Potential of Cloud Computing in Europe. Brussels, 27.9.2012 COM (2012) 529 final, p. 3-4 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf>.

European Commission. European Commission Memo: Unleashing the Potential of Cloud Computing in Europe – What Is It and What Does It Mean for Me? Brussels, 27 September 2012 [interactive]. [accessed on 20-09-2013]. <http://europa.eu/rapid/press-release_MEMO-12-713_en.htm.

European Commission. European Union Data Protection Directive 95/46/EC Article 29 data protection working party opinion 05/2012 on cloud computing. Brussels, 1 July 2012, p. 11 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>.

European Commission. 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. Brussels, 25 January 2012 [interactive]. [accessed on 20-09-2013]. <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.>.

European Union Charter of Fundamental Rights, the European Parliament, the Council and the Commission. 2000 [interactive]. [accessed on 20-09-2013]. <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

Gervais, D.J. and Hyndman, D.J. 2012. *Cloud Control: Copyright, Global Memes and Privacy* [interactive]. [accessed on 20-09-2013]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2017157>.

Internet: Case-law of the European Court of Human Rights. Council of Europe, 2011 [interactive]. [accessed on 20-09-2013]. <http://echr.coe.int/Documents/Research_report_internet_ENG.pdf>.

K.U. v. Finland, No.2872/02, § 43, 2 December 2008, Council of Europe, 2011 [interactive]. [accessed on 20-09-2013]. <http://echr.coe.int/Documents/Research_report_internet_ENG.pdf>.

Oxford Dictionary Online [interactive]. [accessed on 20-09-2013]. <http://oxforddictionaries.com/definition/english/netbook?q=netbook>.

Rong, Z.; Minqi, Z.; Aoying, Z.; Weining, Q.; Wei, X. *Security and Privacy in Cloud Computing: A Survey*. 2010 Sixth International

Conference on Semantics. Knowledge and Grids. Software Engineering Institute, East China Normal University, Shanghai, China. National Institute of Information and Communications Technology, Kyoto 619-0289, Japan; ISBN: 978-0-7695-4189-1, IEEE Computer Society Washington, DC, USA, 2010, p. 108 [interactive]. [accessed on 20-09-2013]. <http://www.computer.org/csdl/proceedings/skg/2010/4189/00/4189a105-abs.html>.

Svantesson, D. 2012. Data Protection in Cloud Computing – The Swedish Perspective. *Computer Law & Security Review*. 28: 476, Faculty of Law Bond University, Queesnsland, Australia [interactive]. [accessed on 20-09-2013]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2140906>.

TEISINIŲ DUOMENŲ APSAUGOS PRINCIPŲ ĮVERTINIMAS NUOTOLINĖJE KOMPIUTERIJOJE SUTARTINIŲ SANTYKIŲ SU GALUTINIAIS VARTOTOJAIS KONTEKSTE

Darius Štitilis

Mykolo Romerio universitetas, Lietuva, stitilis@mruni.eu

Inga Malinauskaitė

Mykolo Romerio universitetas, Lietuva, inga.malinauskaite@mruni.eu

Santrauka. *Įvadinėje straipsnio dalyje autoriai apibūdino nuotolinės kompiuterijos paslaugos reiškinio ypatumus – sąvoką, požymius, pagrindinius privalumus ir rizikas. Tinkamas duomenų apsaugos reikalavimų įgyvendinimas nuotolinėje kompiuterijoje – vienas iš pagrindinių šių dienų iššūkių. Autoriai, remdamiesi Duomenų apsaugos direktyva 95/46/EB, Bendruoju duomenų apsaugos reglamento pasiūlymu bei Europos žmogaus teisių teismo jurisprudencija, pristatė pagrindinius ir rekomenduojamus duomenų apsaugos principus, taikytinus nuotolinėje kompiuterijoje sutartinių santykių su galutiniais vartotojais kontekste. Tiriamojoje straipsnio dalyje autoriai analizavo pasirinktų nuotolinės kompiuterijos paslaugų teikėjų privatumo politikų ir/ar paslaugų teikimo sutarčių nuostatas bei tikrino jų atitiktį pagrindiniuose teisės aktuose įtvirtintiems teisiniams duomenų apsaugos reikalavimams. Atlikta analizė parodė, kad pagrindiniuose teisės aktuose numatyti teisinės duomenų apsaugos reikalavimai atsispindi nuotolinės kompiuterijos paslaugų teikimo privatumo politikose ir/ar paslaugų teikimo sutarčių nuostatose. Tačiau taip pat būtina pažymėti, kad pasirinktų nuotolinės kompiuterijos paslaugų teikėjų formuluotės yra skirtingos. Pavyzdžiui, „Google" privatumo politikos nuostatos yra aiškios, lengvai įtraukiančios vartotoją į duomenų kontrolės procesą. Kitų paslaugų teikėjų sutarčių nuostatos nėra lengvai suprantamos. Visų paslaugų teikėjų sutarčių su galutiniais paslaugų vartotojais sąlygos neturi žalos atlyginimo dėl neteisėto duomenų naudojimo mechanizmo sąlygos.*

Raktiniai žodžiai**:** *privatumas ir duomenų apsauga, nuotolinės kompiuterijos paslaugos, atitikimo principai, teisinis reguliavimas.*