Application of Data Protection Concepts to Cloud Computing

By Denitza Toptchiyska

Abstract:

The fast technological development and growing use of cloud computing services require implementation of effective legal infrastructure in order to deal with the privacy and data security implications that are raised.

The paper provides an analysis of the application of the data protection principles and concepts, adopted in the international regulatory frameworks, to cloud computing services, starting from the point that the main aim of data protection regulation is to protect personal sphere of individuals, from one side, and to support the free flow of information and data, from the other side. The current proposals and regulatory decisions in the field of cloud computing in EU are explored, focusing on the allocation of roles and responsibilities in client – service provider relationships and the application of the concepts for data controller and data processor. The paper also analyses the legal basis for lawful processing of personal data and safeguarding the rights of data subjects in cloud computing services. The issues are discussed and conclusions are drawn in the light of the need to ensure globally consistent regulatory framework in order to protect effectively the rights of the parties concerned.

Keywords:

Data controller, data processor, data protection legislation, cloud economy, cloud computing

1 Introduction

Cloud computing is a technological innovation in the ICT landscape related to the development of new business models based on processing, collection, storage, and analysis of data on remote computerized systems using internet or other networks [1]. Reducing IT costs and thus enabling more users to benefit from the last technological solutions as well as being a basis for further innovations in all sectors of economy are only some of the positive factors that cloud computing already brings in the society [2]. In 2012 the European Commission released as a part of the EU Digital Agenda a Communication on unleashing the cloud potential in the EU [3] setting a strategy aimed at increasing the productivity in EU on the basis of extended use of cloud computing services. In this context the EU data protection legislation faced the challenge to be interpreted and modernised in order to respond to the implications of cloud computing for the privacy of individuals and to ensure a trusted environment.

The effective application of the EU data protection legal regulation is hampered by the complex architecture of the cloud services. In most of the analyses services provided over the cloud are divided in three layers: provision of cloud infrastructure, software and platform. Services over these layers often involve multiple entities located in different jurisdictions globally [2]. Lack of transparency of the personal data processing through cloud computing services adds to the difficulties in ensuring high standards of protection of individual right to privacy. Deployment of cloud computing services in EU faces the challenges of differing national legislations in the field of data protection, due to the variations in the implementation of 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 (EU Data Protection Directive)[4].

The EU data protection model has been adopted in the 1990s following the Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data [5]. The EU model is based on technology neutral concepts and principles whose application is not limited to a specific technological context and often requires interpretation [6].

Because of the complexity of cloud computing and the challenges related to its technological infrastructure, the application of data protection concepts and principles requires further specification and clarification in order to ensure efficient protection of individual privacy and legal certainty. The article aims to clarify the application of the concepts of data controller and data processor in the context of the relations between the cloud service providers and customers. The analysis is made on the basis of the existing international data protection frameworks as cloud services are often related to transborder transfer of personal data involving different jurisdictions.

2 The concepts of data controller and data processor in the cloud context

2.1 EU legal framework

The concepts of data controller and data processor are essential in the EU data protection model forming the basis for allocation of responsibilities for ensuring lawful processing of personal data and for defining the applicable national data protection law [7]. The legal definitions for the terms "data controller" and "data processor" are included in the EU Data Protection Directive, providing that the data controller is the party that alone or jointly with others determines the purposes and means of the data processing [8]. The data processor, on the other side, is the party which processes personal data on behalf of the controller [9]. According to the EU Data Protection Directive the data controller is responsible for the lawful processing of personal data and ensuring the rights of data subjects.

The comprehensive approach towards data protection is considered as an advantage of the EU data protection model. However the assessment of the effectiveness of the EU Data protection directive indicates as a weakness the simplistic definitions of data controller and data processor which cannot adequately cover all entities involved in the data processing in an interconnected technological environment [6]. As example a cloud based free email service could involve separate storage and mailing functionalities for the customer while having a different legal entity providing analysis of clients' e-mails based on which advertisements are shown to the customer.

The EU Data Protection Directive as a legal instrument is the basis for harmonization of national data protection regulations of the EU member states. At EU level guidance on the uniform interpretation of the data protection concepts is provided by the Article 29 Working Party acting as an advisory body on data protection issues for the European Commission [10]. At national level the supervisory authorities are responsible for monitoring the application of national data protection regulations.

2.1.1 Opinions of the Article 29 Working Party

The Article 29 Working Party considered the distinction between the data controller and data processor in different opinions that bring important clarification on the responsibilities of the cloud service providers and cloud service customers.

Opinion 10/2006

In 2006 the Article 29 Working Party adopted an opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) [11], a Belgian based cooperative providing an international financial messaging service. The opinion clarified the role of the organization in the processing of personal data. The case was provoked by a press release in 2006, informing that SWIFT provided data to the United States Department of the Treasury contrary to the EU data protection legislation. SWIFT refused responsibility, stating that the cooperative was acting solely in the role of data processor and emphasising that according to the contractual provisions in the frames of which the personal data were processed, SWIFT was a "subcontractor."

In order to determine whether SWIFT acted as a data controller or as a data processor, the Article 29 Working Party gave priority to the factual circumstances before the provisions of the data processing contract. The Working Party accepted that the role of a subcontractor in the commercial or civil law equals to the role of a processor under the EU Data Protection Directive. However on the basis of the facts the Working Party concluded that the role of SWIFT regarding the processing of personal data has evolved in a way that went beyond the competence of the processor. The factual circumstances that were taken into account by the Working Party in order to qualify SWIFT as a controller of the data processing included that the management of SWIFT cooperative was able to control the data processing by taking autonomous decisions regarding the purposes and means of the processing. The decisions on the development, marketing and changing the services and processing of data as well as the competence to decide on the service agreements and policies were qualified by the Working Party as *practical and legal means of processing* [12], for which the competence is assigned to the data controller according to the EU Data protection directive.

Considering the role of the financial institutions that used the SWIFTNet FIN service, the Working Group concluded that they act in the role of joint controllers for the SWIFT activities, as they were able to influence the decisions. However the Working group highlighted that *the joint responsibility does not necessarily mean equal responsibility* [13].

The Opinion on SWIFT case has an important impact on the provision of cloud computing services involving processing of personal data from EU, as it affirms that the role of the organizations involved in the data processing should be assessed by the competent national authorities on the basis of factual circumstances independently of the qualifications given in the contracts for the data processing. In the case of cloud computing where many parties are often involved as contractors and subcontractors the allocation of responsibilities could often lead to joint accountability. However the EU legislation lacks the definition of the scope of joint responsibility as well as objective criteria for identifying the respective share of responsibility.

Opinion 1/2010

Another document that has to be taken in consideration in order to clarify to roles of the parties involved in the cloud computing services is the Opinion 1/2010 of the Article 29 Working party on the concepts of "controller" and "processor" [14]. The document aims to clarify the concepts in view of the globalization and increased complexity of the organizational and technological ways for data processing. In the Opinion 1/2010 the Working Party emphasises the importance of clear and uniform interpretation of the concepts "controller" and "processor" in order to achieve effective implementation of the EU data protection model.

On the basis of the definitions provided in the EU Data Protection Directive, the Working Party identifies three basic elements in the concept of data controller: the personal aspect, the possibility of pluralistic control and the essential elements that distinguish the data controller from the data processor i.e. the possibility to determine the purposes and the means of the personal data processing.

Clarifying the idea behind the concept of "data controller", the Working Party highlights that although the concept has been developed on the basis of Convention 108 of the Council of Europe, it has evolved to have its independent meaning under EU law. According to the Convention 108 provisions the data controller is only the body that is competent to decide the purposes and means of personal data processing, while under the EU law as data controller is qualified the body that *factually* determines them, even in the cases when it is done contrary to the law. Following its position from the SWIFT case, the Working party emphasizes, that in order to determine if a body acted in the role of a data controller, it is essential to make analysis of the factual circumstances of the case, while defining the purposes of the data processing.

To facilitate the process of actual identification of data controllers, the Working party differentiated three categories of situations in which data controllers act. The first one is when the controller controls the data processing on the basis of explicit legal competence. In such case the data controller is designated by national or EU law [15]. The competence for determining the purposes and means of the data processing of the second category of data controllers derives implicitly from common legal provisions or established legal practice (for instance, employers processing the data of their employees). For the third category of data controllers, the control that they exercise over the data processing is a result of their factual influence that can be assessed on the basis of the factual circumstances and contractual responsibilities. However the Working Party reiterates that although the contracts can help to clarify the case, the factual analysis prevails. According to the analysis of the Working Party the third case could result most often to divergent interpretations. Cloud computing usually falls under the third category where factual analysis has to be done in order to distinguish data controller and data processor.

The EU Data Protection Directive provides that the controllers determine the purposes and means of the data processing. According to the interpretation provided by the Working party, the determination of the purposes of the data processing qualifies the actor as data controller. The determination of the means of processing refers to decisions ensuring the lawfulness of the data processing and more specifically its compliance with the data quality principles. Such decisions always qualify the actor as data controller. However concerning the technical or organizational means of data processing, the decision can be taken by the data controller or to be delegated to the data processor.

In the Opinion 1/2010 the Article 29 Working Party also clarifies the concept of data processor, developed in the EU legislation. According to the interpretation of the legal definition, in order an actor in data processing to be qualified as a processor, it should be a separate natural or legal entity that undertakes the data processing on behalf of the data controller. The EU Data Protection Directive requires a contract or a binding legal act to regulate the relations between data controller and data processor in order to ensure that the delegation of processing will not entail lower standard of data protection [16].

The Working Party recommends that the contract shall be in written form for evidence purpose and shall have a minimum content, stipulating in particular that the data processor shall act only on instructions from the controller and implement technical and organizational

measures to adequately protect personal data. According to the interpretation provided by the Working Party the contract does not have constitutive effect for the controller/processor relations. In addition the Working Party underlines that regardless if the contract has been prepared by the controller or the processor if the controller agrees on the contract it takes the responsibility to comply with the legal requirements for lawful processing.

Opinion 05/2012

The Opinion 1/2010 of the Working Party provides the basis for the application of the controller/processor distinction in the context of cloud computing services which was further developed in its Opinion on Cloud Computing adopted in 2012 [17]. According to the analysis of the Working Party the main risks for the individual right to privacy, associated with cloud computing services are related to the lack of control over the personal data processing, insufficient information about the parties involved in the data processing (processors/ sub-processors) and their location as well as the third parties to which is given access to information.

Considering the applicability of the controller/processor concepts in the relations between cloud client and cloud provider, the Working Party drew conclusions on the basis of the criteria listed in its Opinion 1/2010. The cloud client is qualified as data controller if it determines the purposes of the processing and deciding on the delegation of the processing activities to an external organization. The entity providing cloud services (hardware, platform or software) is considered to be a data processor. However the relations when personal data are processed via cloud services could be much more complex. In order to assess them in view of the EU data protection legislation it is essential to consider the factual circumstances of the data processing. In many cases it is possible that the cloud provider acts as joint controller or separate controller when it processes data for new purposes. The Working Party emphasizes the importance of clear allocation of responsibilities in the complex cloud environment where multiple players from different jurisdictions globally are usually involved, in order to avoid cases where it is not possible to identify the responsible subject.

Even if the cloud client cannot negotiate the terms of standardized contracts offered by cloud providers, if the cloud client agrees on them, it will be sufficient ground to be qualified as a data controller. The Working Party affirms that it is the responsibility of the client to choose the option in which the personal data will be processed in compliance with the applicable data protection legislation. In contrary to this position, it is argued that if the consumer as controller cannot impose control on the processor, there should be an exemption from the liabilities of controller if the information is processed in third-party equipment [18].

For processing operations done via cloud services it is usual separate tasks of the processing to be allocated to different processors. It is also a common case when processors are allocating some tasks for the processing to sub-processors. The Working Party emphasizes that in such cases the data controller – the client must be informed as well as to be provided with guarantees that the sub-processor will meet the security requirement of the applicable national legislation of the EU member state. According to the interpretation of the Working Party it is not necessary to have a direct contract between the data client and sub-processor, but it is important that the contract between the processor and sub-processor should reflect the provisions of the data protection contract between the data controller and the cloud providers that acts as data processor. In such cases it is advisable the contract to be based on the standard contractual clauses for the transfer of personal data to processors established in third countries approved by the European Commission [19].

In this model sub-processing is permitted only with the prior written consent of the controller and with a written agreement imposing the same obligations on the sub-processor as are imposed on the processor. In case the sub-processor fails to fulfil its data protection obligations the processor shall remain fully liable to the controller for the performance of the sub-processor's obligations. A provision of this kind could be used in any contractual clauses between a controller and a cloud service provider, where the latter intends to provide services through subcontracting to assure required guarantees for the sub-processing.

In the three opinions analysed above the Article 29 Working Party presented consistent interpretation of the data controller/data processor concepts. In order to ensure high level of protection of individual privacy as well as to avoid cases when the responsible party for the data processing cannot be identified, the Working Party adopts quite broad interpretation of the concept of data controller. Moreover in the case of cloud computing the obligations of the data controllers/processors are further increased as for instance with the requirement to inform the client for all sub-processors involved in the data processing and to ask for prior agreement. The additional obligations imposed of the data controllers and data processors as well as the requirement of detailed contracts specifying the terms of the data processing will ensure better privacy protection. However they will entail further administrative burden on the cloud service providers and monitoring authorities [6].

2.1.2 Article 29 Working Party decision about Microsoft

In April 2014 the Article 29 Working Party approved the Microsoft agreement for cloud service [20]. The approval is regarded as an important step towards wider use of cloud computing, as it brings more certainty and clarity in the application of EU standards to cloud computing industry [21]. The Working Party confirmed that the Microsoft agreement meets the requirements of the standard contractual clauses for transfers to processors in third countries approved by the European Commission in 2010. The approval aims to reduce the number of national authorizations required to allow international transfer of data from EU member states. However it is possible that such authorization is still required in some member states according to their national legislation.

On the basis of the agreement Microsoft will be able to provide cloud services to EU clients as a data processor. Following the approach taken by the Article 29 Working party in its opinion on cloud computing, the contractual obligations of Microsoft include prior notification to the client in case of appointing a new sub-processor. In case that the client does not agree with the appointment, it is entitled to terminate the contract.

2.1.3 Proposal for EU Data Protection regulation

Faced with the challenges of the fast technological development in 2012 the European Commission proposed a new Regulation containing the general rules on data protection. The regulation aims to remove the complexities stemming from the differences between the national data protection legislations and to facilitate the deployment of services which require transborder flow of personal data. Moreover in the framework of the data protection reform the EU aims to modernize the data protection rules in order to correspond to the new technological environment [22].

In relation to the data controller concept the European commission proposed the criteria that qualify the data processing organization as controller to be further developed by adding that the controller defines not only the purposes and means but also the conditions of the data processing [22]. However the European Parliament decided not to approve the change at the

first reading of the proposal leaving the definitions of data controller and data processor unchanged from the EU Data Protection Directive [23].

In the proposal for Data Protection Regulation the application of EU data protection legislation is extended in two cases that will have important impact on the provision of cloud computing services. According to the new proposal the EU data protection legislation will be applicable in all cases of processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU independently if the processing takes place in the union or not [24]. In comparison, the EU Data Protection Directive associated the application of EU data protection legislation only with the establishment of the data controller. Furthermore the proposal for Data Protection Regulation states explicitly that it should apply to controllers and processors which provide the means for processing personal data for personal or domestic activities, although such use is excluded from the scope of the application of the regulation [25] The provision is important as it aims to regulate clearly the cases of private use of cloud computing services from EU individuals.

In its opinion of the proposal for Data Protection Regulation the European Data Protection Supervisor emphasizes that the proposed rules will increase the standard of privacy protection and accountability of the data controllers [26]. Regardless of the wide ongoing discussion on the usability and practicality of the legal definitions for data controller and data processor, the definitions stayed unchanged. As a consequence the parties involved in the provision of cloud services will continue to face uncertainty regarding their role and responsibilities. They will be forced to rely on Article 29 Working Party opinions which are not legally binding.

2.2 Regulation of the data controller/data processor concepts in other international privacy frameworks

2.2.1 OECD Privacy Guidelines

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data contain the concept of data controller defining it as the organization which according to the national law is competent to decide the contents and use of the personal data [27]. Although the concept of the data processor is not introduced in the guidelines, the organizations acting in the role of agents on behalf of the data controller for the collection, storing, processing or dissemination of personal data, are excluded from responsibility in relation to the data processing. The complete responsibility for ensuring the lawfulness of the data processing is assigned to the data controller.

In 2013 the OECD Privacy Guidelines have been revised in order to ensure interoperability and to facilitate further the international transfers of personal data taking in consideration the technological developments and the widespread use of cloud services. The revision aimed to simplify and consolidate the data protection regulations as well as to reinforce the principle of accountability on the basis of which the data controller remains accountable for the personal data transfer that controls independently of the location of the data [28]. To this end the new concept of privacy management programme have been introduced in order to ensure the application of OECD guidelines by the data controllers. The OECD guidelines provide that the privacy management programme should cover all data processed under the control of the controller, including the data that are processed by the agents of the data controller on its behalf. Keeping the complete responsibility to the data controller aims to grantee in any case a party to which the recourse for unlawful implementation of data protection rules can be addressed.

2.2.2 Safe Harbour Framework

In difference to the EU comprehensive approach in data protection, the US relies on sectoral laws adopted for the public and private sectors [29]. Some US regulatory instruments impose obligations on the data owners to ensure secure processing of personal information by third parties, usually on the basis of contractual provisions. In addition, some legal instruments impose restrictions to service providers that have access to personal information [30].

The EU data protection standards in US are ensured on the basis of the Safe Harbor Framework, approved by the European Commission in 2000 [31]. The framework was adopted following the requirement of the EU Directive 95/46/EC providing that the data transfers are allowed only to non-EU countries, ensuring adequate level of data protection.

The Safe Harbor Framework is based on a set of principles that have been issued by the US Department of Commerce aimed to support commercial relations with the EU. The organisations decide voluntarily to adhere to the Safe Harbour framework that entails their obligation to comply with the data protection principles embodied in it. In order to qualify for the Safe Harbour Framework, an organisation can join a self-regulatory privacy programme or provide its own self-regulatory privacy policies. Regardless if the organisations adhere through self-regulation mechanism or on the basis of a sectoral law, they are subject to statutory penalties for non-compliance.

The Safe Harbour Framework imposes obligations on the US organisations processing personal information of individuals subject to EU legislation to ensure the compliance of the data processing with the embodied principles. However within the defined principles the framework does not contain the terms "controller" and "processor". The idea that a third organisation could be involved "*on behalf of and under the instructions"* of the organisation administering the data processing is implied in the concept of the "agent". The Safe Harbour framework requires the organisation administering the processing to ensure that the agent is bound by the Safe Harbour principles or is subject to the EU Directive 95/46/EC/. Otherwise the organisation is obliged to enter into a written contractual agreement providing that the agent will maintain the requested data protection standards. When personal data are transferred to a third organisation acting as an agent, the organisation administering the processing is not required to notify the individuals about the purposes of processing, the third party to which the information is disclosed, or the options that individuals have in order to limit the use or disclosure of the information.

The interpretation of the Safe Harbour Principles follows the US legislation which does not contain the controller/processor distinction [32]. However guidance about the application of the Safe Harbour principles is provided in the frequently asked questions annexed to the Decision of the European Commission providing some clarification on the implementation of the concepts of data controller and data processor following the requirement of the EU data protection directive. For instance an US organisation receiving personal information from EU solely for processing is not required to join the Safe Harbour framework, as the responsibility for complying with the EU Data protection directive is imposed on the EU controller. The EU controller is obliged to have a contract with the US organisation acting as a processor, ensuring that the EU standards of data protection legislation will be respected [33]. When an US organisation acting as a processor has joined the Safe Harbour Framework the contract with the EU data controller will not require prior authorisation, in case it is not required by the national legislation.

For US organizations joining the Safe Harbor Framework it is important to have a clear idea of the role that they have in the processing in order to comply with the relevant obligations. The interpretation of Safe Harbor Framework requires balancing between the US and EU legal concepts [34].

2.2.3 APEC Privacy Guidelines

The APEC Privacy Framework adopted by Asia-Pacific Economic Cooperation (APEC) in 2004 aims to improve the standard of information privacy protection in the APEC countries as well as to increase transborder flow of personal information between those countries [35]. Following the OECD Guidelines, the APEC Privacy Framework defines the concept of "personal information controller" as the party that controls the collection, holding, processing or use of personal information. The APEC framework assigns the full responsibility for the processing on the controllers and excludes from responsibility the person or organization undertaking such functions under the instructions by another person or organization, thus implying the agent concept from the OECD guidelines. Further the APEC framework imposes on information controllers but not on their agents the obligation to take appropriate safeguards against risks to personal data.

3 Conclusions

The beneficial effect of the cloud computing on the economy and society is internationally recognised. Deployment of cloud computing services requires a data protection framework that from one side supports the high standards of protection of individual rights and from the other side is based on clear and unambiguous concepts and rules that provide legal certainty and predictability. The EU data protection framework is regarded as the highest standard for privacy protection compared to other international legal frameworks. The effective application of the EU data protection regulations in the cloud computing requires clear distinction of the responsibilities of the organisations involved in the data processing.

In all frameworks examined above the concept of data controller is embodied although defined with different wording. The EU concept of data processor can be transposed to some extent to the concept of agent in the OECD, Safe Harbour and APEC privacy frameworks. The main difficulties arise when the role of an entity involved in data processing should be qualified as controller or processor. The complexity of the cloud services industry also imposes challenges by its own in clearly identifying the role of each entity involved. On those premises the Article 29 Working Party approach to give priority to factual circumstances in defining whether organization acts as data controller or data processor comes as very helpful and practical solution. Despite the guidelines provided by the Article 29 Working party the application of the concepts still could lead to various implementations in the frames of the national laws of the EU member states which can affect negatively the deployment and provision of cloud computing services in the EU. For this reason it is recommendable that those guidelines are embodied into a legally binding regulation in order to provide the needed certainty for rapid deployment of cloud services across EU.

The proposal for EU data protection regulation, although keeping the same broad definitions for the data controller and data processor, aims to further ensure the application of the EU data protection standards binding their application with the jurisdiction under which operates not only the data controller but also the data processor. The international data protection frameworks keep the principle of sole accountability of the data controller regarding the lawfulness of the data processing. New mechanisms including the requirements for risk

assessment and management programme have been provided aiming to ensure that all data processing will be covered by the applicable data protection legislation. However there are still divergences in the definition of roles and responsibilities under the data protection frameworks which undermine the efficiency of the individual rights protection in the cloud environment.

References

[1]. UN, Information Economy Report 2013, The Cloud Economy and Developing Countries available at http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf (accessed 25.04.2014)

[2]. Gasser U. (2014), Cloud Innovation and the Law: Issues, Approaches, and Interplay, Berkman Center, online at Series: http://cyber.law.harvard.edu/research/cloudcomputing (accessed 25.04.2014)

[3]. European Commission (EC), "Unleashing the Potential of the Cloud in Europe," COM(2012) 529, Brussels, 27.9.2012

[4]. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995

[5]. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" - WP 169 (16.02.2010)

[6]. Robinson N., Graux H., Botterman M., and Valeri L. (2009), Review of the European Data Protection Directive online at http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf (accessed 25.04.2014)

[7]. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" - WP 169 (16.02.2010)

[8]. Art. 2 (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995

[9]. Art. 2 (e) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995

[10]. Art. 30 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995

[11]. Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP128 (November 22, 2006)

[12]. Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP128 (November 22, 2006), p. 11

[13]. Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP128 (November 22, 2006), p. 12

[14]. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" - WP 169 (16.02.2010)

[15]. Art. 2 (d), sent. 2 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995
[16]. Art. 17 (3) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995
[17]. Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP 196 (July 1, 2012)
[18]. Irion K. and Luchetta G.,(2013) Online personal data processing and EU data protection reform online at http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform (accessed 25.04.2014), p. 46
[19]. Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010)593)
[20]. Article 29 Data Protection Working Party, Ref. Ares(2014)1033670 - 02/04/2014, online at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf (accessed 09.05.2014)
[21]. Harrison J.,EU Data Protection Authorities Endorse Microsoft's Cloud Computing Agreement, online at https://www.scl.org/site.aspx?i=ed36831 (accessed 09.05.2014)
[22]. EC, "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," Brussels 25.1.2012, COM(2011) 11 final
[23]. European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading)
[24]. EC, "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," Brussels 25.1.2012, COM(2011) 11 final, art. 3
[25]. EC, "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," Brussels 25.1.2012, COM(2011) 11 final, Recital 15
[26]. Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe" (16.11.2012)
[27]. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980 as revised in 2013), art. 1(a)
[28]. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980 as revised in 2013), par. 16
[29]. Schwartz P.(2013), Information Privacy in the Cloud online at http://scholarship.law.berkeley.edu/facpubs/1906/ (accessed 25.04.2014)
[30]. Sotto L., Treacy B., and McLellan M. (2010), Privacy and Data Security Risks in Cloud Computing online at http://www.hunton.com/files/Publication/4845e31f-63d8-4f9a-9a36-a074e4170225/Presentation/PublicationAttachment/6f52b2fd-2973-48cc-9f23-

c941f1e19358/Privacy-Data_Security_Risks_in_Cloud_Computing_2.10.pdf (accessed 25.04.2014)
[31]. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce
[32]. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce
[33]. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce
[34]. Kuner Ch. (2008), Membership of the US Safe Harbor Program by Data Processors online at http://www.huntonfiles.com/files/webupload/CIPL_Safe_Harbor_3.08.pdf (accessed 25.04.2014)
[35]. APEC Privacy Framework (APEC, 2004)