Cloud Computing Data Protection – A Literature Review and Analysis

Florian Pfarr
University of Wuerzburg
Chair of Information Systems
florian.pfarr@uni-wuerzburg.de

Thomas Buckel
University of Wuerzburg
Chair of IS Engineering
thomas.buckel@uni-wuerzburg.de

Axel Winkelmann
University of Wuerzburg
Chair of Information Systems
axel.winkelmann@uni-wuerzburg.de

Abstract

Cloud Computing technologies are gaining increased attention both in academia and practice. Despite of its relevance and potential for more IT flexibility and its beneficial effects on costs, legal uncertainties regarding the data processing especially between large economies still exist on the customer and provider side. Against this background, this contribution aims at providing an overview of privacy issues and legal frameworks for data protection in Cloud environments discussed in recent scientific literature. Due to the overall complexity concerning international law, we decided to primarily focus on data traffic between the United States of America and the European Union. The result of our research revealed significant differences in the jurisdiction and consciousness for data protection in these two economies. As a consequence for further Cloud Computing research we identify a large number of problems that need to be addressed.

1. Introduction

Since the beginning of IT-supported business administration, the common way of supplying customers and employees with software solutions was based on client-server-architectures. Given that fact, the applying company itself hosts the servers and networks in-house. In this technology model, secure data protection is an important, but comparatively accomplishable issue. Today, an increasing number of software solutions are based on Cloud Computing technologies. That means the supporting hardware for the system is hosted by the provider and the users get access to the solutions over the Internet [2]. Cloud Computing offers can be various regarding the specification (e. g., platforms or infrastructure). Software as a Service (SaaS) describes the distribution of ready-to-use applications based on this technology model. Since Cloud Computing allow fast available, dynamic and stable IT services, this way of IT procurement has further intensified the interest in that solution [29].

Although the number of Cloud Computing users is steadily increasing, some factors still prevent a more rapid dissemination of the method, for example, technical criteria as scalability or especially law issues like data protection and privacy [1]. One of the basic ideas of Cloud Computing is the distributed storage of data on external servers. Besides the concerns over potential loss or theft of data, many customers are uncertain about the applied legal regulations on data protection and privacy in this environment [9]. Many states already established data security regulations to prevent abuse and protect customers from potential risks. However, those regulations are in many cases not applicable for new Cloud technologies [29]. Furthermore, the verbalization of existing legal measures is often vague and subject to differing interpretations [28]. As a result, many data protection regulations, e.g. the US Safe Harbor Agreement, are criticized on a regular basis in scientific literature.

To address the issues stated above, our objective in this paper is to review the literature on data protection and privacy in conjunction with Cloud technologies in order to establish a better understanding of the status of existent law in this environment as well as to provide an overview of problems regarding the topic discussed in recent academic publications. The remainder of the paper is organized as follows: In the next chapter we describe our framework of analysis and the chosen method. In chapter 3, we present the results of our review. The paper closes with a summary of the current state of academic research and a delineation of challenges for future studies.

2. Methodology

2.1. Literature Selection Process

Many attributes characterize a precise literature review. However, lacking rigor is often considered as

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.616

IEEE computer society

one of the most crucial or even critical factor. According to vom Brocke et al. (2009), a lack of rigor in documenting the literature search process often causes problems regarding the reliability of a literature review [36]. To avoid this fundamental mistake, we systematically follow the five steps of the workflow shown in figure 1 to ensure a reproducible selection of the literature used to compile this review. A short description of each step will be given in the following paragraphs.

Since conducting a literature review on legislature always implies dealing with a vast number of different national requirements and directives, we had to define the extent of the search in a first step. For this review, we decided to focus on data protection law affecting the data traffic between the USA and the European Union (EU) since these two economic powers are strongly connected trading partners while following considerable different approaches concerning data processing law [29].

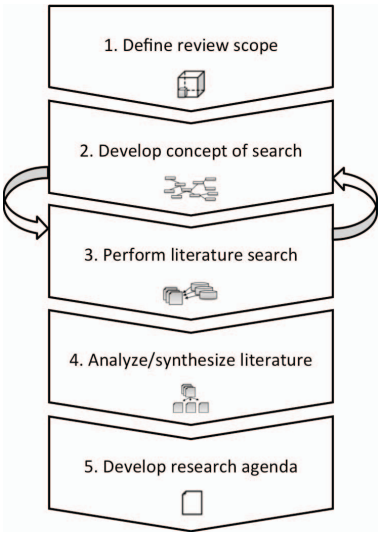

Figure 1. Framework for literature review (following [36])

The second step, i.e. the conceptualization, is executed in two stages. First, we collected significant data protection directives of the EU member states and the US as well as general terms describing this subject. Subsequently, we transferred the results from this search into a concept matrix based on the proposals of Webster and Watson (2002). With that categorization we want to obtain a better understanding of which topics are addressed by the respective literature source. Table 1 shows an example of the matrix-structure described above. Since articles usually focus on a specific problem of the topic, this form of representation also helped finding gaps and rarely considered issues in the current literature.

In the third step of our workflow-framework, we searched for related literature. This step included the selection of suitable databases for the research, the search process itself, an ongoing evaluation of the literature as well as an update of the matrix created in the previous step [36]. As for journals, we relied on the ranking of the Association of Information Systems (AIS). As for other publications including conference articles, we used the online databases EBSCO-host/Business Source Premier, ACM Digital Library, ScienceDirect, Google Scholar and Springerlink. The time period for this study was selected to begin in the year 2000.

Table 1. Concept matrix

	Publication a	Publication b	Publication c	...
Aspect 1				
Aspect 2				
Aspect 3				
...				

Afterwards, we performed queries in the selected databases. Since the keyword "Cloud Computing" delivered too many results for a detailed verification, we added more keywords to our queries. These keywords were privacy, privacy protection, privacy regulation, data security, and data protection. Additionally, Cloud Computing contracts are generally considered as data processing orders in contract law [1]. Hence, we also added the terms "data processing" and "data processing orders" respectively in our queries. Since our keyword searches with all possible combinations still resulted in a large quantity of scientific books, conference proceedings and journal articles, we started to explicitly search for specific directives on data protection and privacy directly related to the United States or the European Union. The outcome of this research showed the following directives: Directive 95/46/EC, Directive 2002/58/EC, Safe Harbor Agreement, Binding Corporate Rules, EU Standard Contractual Clauses, and General Data Protection Regulation.

Subsequently, we recorded these directives in the concept matrix and added them to our keyword list to perform further queries. Step 2 (conceptualization) and step 3 (literature research) were thus performed iteratively since every new keyword found while researching had also to be considered for all literature already added to the matrix before.

Additionally, we performed forward and backward searches in journals, proceedings and

books to find further literature sources, which could not be found by keyword searches.

2.2. Review and Classification Process

Since the type and findings of the studies were heterogeneous, we had to develop a methodology for a common way to represent the content and aspects that had to be analyzed. Therefore, we followed the model of iterative research processes proposed by Flick (1995) shown in figure 2. This model offers the advantage that new findings found while revising the literature sources can easily be added to the concept matrix during the process of information consolidation. Hence, the most important problems and current challenges in Cloud Computing data protection could be identified step-by-step while ensuring a clear and consistent way of presentation.

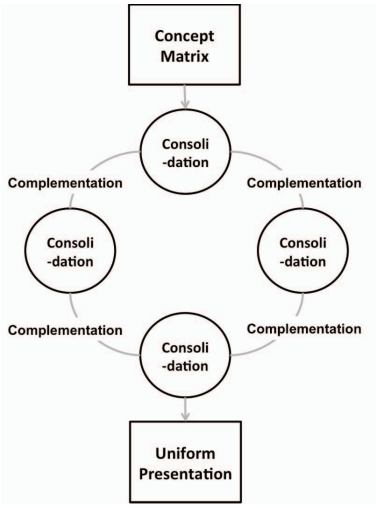

Figure 2. Iterative research process

Based on this approach, we were able to define five main aspects, which had to be further analyzed.

- *Lack of common regulations*
  Cloud Computing is a concept based on global thinking. Therefore, establishing common rules is nearly impossible with regard to different laws, regulations, or political systems in the connected countries [28]. Against this background, we analyzed whether existing or planned directives are able to harmonize the legal situations regarding Cloud Computing privacy in the specific countries.

- *Legal uncertainty*
  Privacy protection requires an established legal framework. However, the law situation regarding personal data in the two analyzed economic areas (USA/EU) varies considerably. Since privacy is a fundamental right of every citizen in the EU, its protection is a responsibility of every member state [29]. In the US, on the contrary, the enforcement of privacy law is generally considered to be less strong than in the EU. Additionally, e.g. the definition of personal data differs notably. Hence, the knowledge about a transfer of data between member states of both unions often results in uncertainty on customer-side, especially for users in the EU [9]. Moreover, some of the existing directives can be interpreted variously and thus be applied in different ways [32]. For that reason, our analysis aimed to elaborate the level of protection provided by current measures in the two economies.

- *Missing control mechanisms for users*
  Although there are some exceptions like the establishment of an in-house private cloud, the use of Cloud technologies usually implies the data transfer over the Internet and storage of information on external servers hosted by the service providers. This implies a limitation of the user's possibilities of control. Since the data is transferred automatically and often without comprehensible inspection, there is a potential risk of loss or manipulation of sensible information. Additionally, the localization of the servers is often not supported. Therefore, the user cannot clearly define the privacy laws that should be applied. This means that data may even be abused without breaking a law depending on the regulations of the provider's state of origin [28]. As a consequence we also inspected privacy directives regarding control possibilities for users and the provider's duty to notify customers in case of unauthorized data processing.

- *Unauthorized access by third parties*
  Besides the risk of unauthorized processing of personal data by providers, there is a possibility of abuse of information by third parties, e.g. for commercial purposes or data espionage [28]. Hence, we also analyzed whether privacy directives take this risk into account or not.

- *Cross-border data flows*
  The main privacy directive of the EU established in 1995 regulates data flows within the union. Member states are obligated to integrate this directive in national law [17]. This regulation also allows transfer of data to countries with an acceptable level of privacy. Reversely, this means

that personal data flow is forbidden between EU member states and third countries whose privacy level is classified as "inadequate". Nevertheless, there are exceptions. The application of regulations like the Safe Harbor Principles, the Binding Corporate Rules, or Standard Contractual Clauses yet allow transfer of data between EU member states and third countries without adequate data protection. Although these alternatives are accepted by the EU, they are far away from the level of severity regarding the protection of personal data as the European Data Protection Directive [28]. This is why we also analyzed international privacy law with regard to the legal problems caused by cross-border transfer of data.

3. Findings

3.1. Analysis of Publication Date, Research Methods, and Theory Types

After performing our database query including forward and backward searching efforts, we identified 33 articles that provided the basis for our further analyses. The publication dates illustrated in figure 3 clearly show the increasing significance of the topic in the past four years. The low number of identified articles in the current year 2013 can be explained by the fact, that our literature selection process ended in April 2013 and hence could not cover articles still to be published in the ongoing year.

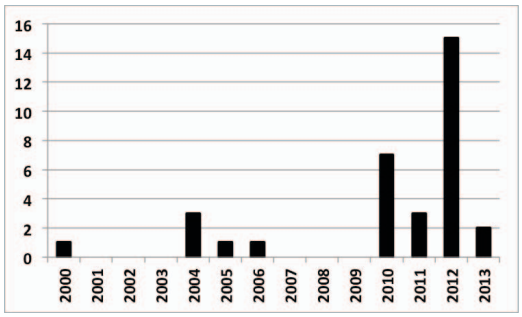

Figure 3. Literature basis by publication date

The identified contributions were classified by the used research method (see table 2) as well as the applied type of theory (see table 3). To categorize the research methods, we used the established scheme proposed by Palvia et al. (2004). Out of 14 different research methods, we discovered just 6 being applied in our literature basis. Besides commentaries (n = 15), which are articles that did not fit into other categories or lacked in empirical evidence, library researches turned out to be the most common used method (n = 7). Overall, it is noticeable that quantitative methods have hardly been applied in this context except for a survey we found (n = 1).

Table 2. Classification by research method

Classification by research methodology	Frequencies n	Frequencies %	Articles
Commentary	15	46%	[3], [6], [10], [11], [12], [13], [14], [20], [24], [26], [29], [34], [35], [38], [40]
Conceptual Model	2	6%	[4], [22]
Library Research	7	21%	[1], [5], [7], [30], [33], [39], [41]
Literature Analysis	6	18%	[16], [18], [21], [23], [28], [32]
Case Study	0	0%	
Survey	1	3%	[25]
Field Study	0	0%	
Field Experiment	0	0%	
Laboratory Experiment	0	0%	
Mathematical Model	0	0%	
Qualitative Research	0	0%	
Interview	0	0%	
Secondary Data	0	0%	
Content Analysis	2	6%	[17], [19]
Σ	33	100%	33

Regarding the theoretical background, we used the classification proposed by Gregor (2006). The far majority of articles in our literature basis are based on analytical theories (n = 22). These are descriptive theories without specification of causal relationships among phenomena or predictions [15]. A smaller amount of publications could be classified as explanations (n = 6). The theory types explanation and prediction (n = 3) as well as design and action (n = 2) were rarely applied, while pure prediction theories could not be identified at all.

Table 3. Classification by types of theory

Classification by types of theory	Frequencies n	Frequencies %	Articles
Analysis	22	67%	[1], [3], [7], [10], [13], [14], [16], [17], [19], [20], [21], [22], [23], [24], [25], [26], [28], [30], [32], [33], [40], [41]
Explanation	6	18%	[6], [11], [12], [34], [35], [39]
Prediction	0	0%	
Explanation and Prediction	3	9%	[5], [18], [38]
Design and Action	2	6%	[4], [29]
Σ	33	100%	33

3.2. Content Classification

Table 4 shows a summary of the content classification regarding addressed privacy regulations in the examined literature. Since articles usually

addressed several regulations, we decided for the reasons of clarity to give an overview instead of a detailed list whereas table 5 in the following subchapter shows specific issues addressed in selected articles.

The very first efforts on secure information processing in electronic markets date back almost 50 years when the United States started to develop the *Fair Information Practice Principles (FIPPs)* in 1970. The FIPPs contain principles for personal data transfer without applying additional individual clauses and were widely disseminated due to the simple adaptability of these principles. This directive also built the basis for various following data privacy laws, especially because it defined the protection of personal data as a human right [28].

Table 4. Classification by regulations

Scope	Name of standard	Publication of standard	Description	n
European Union	Directive 95/46/EC	1995	Directive	22
	Directive 2002/58/EC	2002	Directive	8
	General Data Protection Regulation	2012 (draft)	Regulation	13
EU - USA	Safe Harbor	2000	Self-regulation	25
EU - Third countries	EU Standard Contractual Clauses	2010	Proposals	7
Intra-company	Binding Corporate Rules	2008	Guidelines	8

One of the directives based on the FIPPs is the European Directive on Data Protection from 1995. Although there are other regulations, *Directive 95/46/EC*, as it is called officially, is considered as the primary regulatory standard for personal data processing and data transfers in the EU [20]. Additionally to specific minimum standards on data security, Directive 95/46/EC contains the OECD's guidelines on data protection and had to be incorporated into national law by every EU member state [18]. According to Porwal et al. (2011), this directive is only hardly attributable to Cloud Computing since its restrictions regarding the use of data are too strong [29]. As mentioned before, Directive 95/46/EC prohibits data transfer to third countries without adequate level of data protection. The decision whether a state meets these requirements is made by the EU commission. Therefore, many companies located in the European Union refuse to cooperate with providers situated in those countries unless they apply this directive to their data protection rules [12].

In addition to Directive 95/46/EC, the EU commission enacted the *Data Protection Directive 2002/58/EC* in 2002 to better comply with the need for privacy protection and secure data transfer within the European Union [5]. Similar to Directive 95/46/EC, the new regulations had to be implemented into national law of the member states. However, there are no further binding requirements for the implementation into the legal system of each state other than the compliance with the determined minimum standards [26].

In January 2012, the EU commission presented a first draft for a *General Data Protection Regulation* to harmonize data protection law in the European Union [18]. Since its aim is to address the challenges of new technologies that are not sufficiently covered by previous directives (e.g. Cloud Computing), this regulation has major significance for both providers and customers [1]. It is planned to become effective for all member states in 2016 and to largely replace Directive 95/46/EC [34].

In 2000, the USA developed the *Safe Harbor Agreement* [39]. The purpose of this agreement is to simplify the transfer of information and data across borders and to improve electronic trade. The included principles on privacy are rather general and only applicable for data transfer into the United States. In order to take part in this initiative and agree to the terms of the Safe Harbor Agreement, companies have to self-register into a public list managed by the US Department of Commerce [35]. Since the participation is optional and not required and there further is no government inspection regarding the compliance of the regulations on provider-side, the EU still raises concerns about the protection of data by the Safe Harbor regulation [39].

The EU commission's decision on *Standard Contractual Clauses* in 2010 opened up another alternative for transferring personal data across borders [1]. The implementation of these clauses allows the processing of data by third parties outside the EU. Therefore, Standard Contractual Clauses are considered to principally be an appropriate instrument for Cloud Computing in order to ensure an adequate privacy level [33]. However, our research also revealed that these clauses lack in adaptability.

Another approach for legal transfer of personal data between the EU and third countries is the application of the *Binding Corporate Rules.* Companies implementing these guidelines in their data protection rules make specific commitments for the processing of personal data [17]. In that regard, the applicability of the Corporate Binding Rules to Cloud environments is worth mentioning [38]. However, these rules are only applicable within a single company and therefore proposed for the use in multi-national corporations, for example.

Table 4 illustrates that the Safe Harbor Agreement (n = 25) and the Directive 95/46/EC (n = 22) are primarily discussed in academic literature. Directive 2002/58/EC and the Binding Corporate

Rules were covered by a much smaller amount of articles (n = 8). Almost the same number applies to Standard Contractual Clauses (n = 7). Although not even entered into force, the General Data Protection Regulation draft published in 2012 is already pursued by a relatively high number of articles (n = 13). That fact reveals the significance of this future regulation.

3.3. Problems of data protection regulations

Table 5 illustrates the main problems and challenges of current international privacy regulations between the USA and EU examined in our analysis. Detailed descriptions of the problem areas will be given in the following paragraphs.

Table 5. Issues in academic literature

Issues in academic literature	Article
Lack of common regulations	
Inconsistent data protection law in the EU	[29]
Standardization of software	[26]
Legislature in third countries	[28]
Variety of regulations within the EU	[12]
Variety of data protection law within the US	[33]
Difference of Safe Harbor and EU standards	[39]
Definition of personally identifiable information	[33]
Legal uncertainties	
Different interpretation of laws	[1]
Lack of regulatory requirements in the US	[35]
Lack of independent monitoring	[18]
Non-compliance with Safe Harbor	[14]
Missing control mechanisms for users	
Problems regarding server localization	[25]
Self-regulation of providers in third countries	[38]
Impossibility of total transparency	[18]
Difficulty of consideration of specific user requirements	[21]
Deficits through missing information	[28]
Deficits through too much information	[34]
Unauthorized access by third parties	
Exploitation of Cloud weaknesses by criminals	[38]
Financial advantages for providers through advertisements	[28]
Economic espionage by intelligence agencies	[4]
Problems of the US patriot act	[18]
Cross-border data flows	
Adaptation of regulations for Cloud technologies	[12]
Unsufficient data protection by Safe Harbor	[22]

3.3.1. Lack of common regulations

The standardization of Data Protection Law in the EU was a primary goal of the European Data Protection Regulation of 1995 [29]. This measure defined minimal standards the member states had to implement in their respective national law. Apart from the different interpretations of these standards, countries were allowed to add individual rules, which led to further inconsistencies in the EU in opposition to goals relating to the unification of the data protection law [21]. Olislaeger (2012) states that this issue causes additional problems for the software development in order to comply with the national data protection legislature [26]. An inclusion of all relevant laws would lead to a substantial amount of additional work. A solution could be the limitation of adjustments with regard to certain areas whereas the core principles of the laws are left untouched.

Pearson (2013) states that another problem arises from the differences in the data protection rules of non-EU countries relating to Cloud Computing technologies [28]. The determining factor for the application of regulations is the location of the host server. However, Cloud Computing is based on virtualization and distributed storage techniques. If the data is hosted in different countries, all the respective laws apply at the same time. A possible solution based on Hansen (2012) is the exact identification of the data location at any given moment [17]. Since this is not supported by the technical data transfer protocols, a restriction of the area of data processing would be a way to prevent a routing outside of a specified area.

The introduction of additional guidelines such as the Directive 2002/58/EC or the Directive 2006/24/EC and their differing implementation in the EU member states further increase the complexity of the data protection laws [12].

Since the legislature is handled by each state, there is no equivalent to the EU-directive 95/46/EC in the United States [33]. Although the US at least considered the EU requirements with the development of Safe Harbor, there is serious doubt about this regulation regarding its compliance with the minimal EU standards on data protection [18].

The upcoming General Data Protection Regulation aims to deal with the problem of fragmentation and to harmonize the data protection standards in the EU [1]. Contrary to the directive 95/46/EU, this regulation has the characteristics of a decree and therefore is applicable to law throughout the EU [34]. Companies as well as Cloud Computing providers would significantly benefit from this reform since there would be no more necessity for an incorporation of all the differing legal systems of the EU member states [12]. Despite the overall positive feedback, the coherent arrangement is criticized as to be too bureaucratic. Furthermore, the claim of universal validity is considered questionable [3].

3.3.2. Legal uncertainties

Although there are strict regulations in the EU and the protection of personal data is viewed as a human right, there is uncertainty towards the European data protection rules [39]. Due to the

continuous technological change, there is a need for an ongoing adaptation of privacy law. However, there is currently no comprehensive approach regarding Cloud technologies [28]. A fundamental problem of the data protection rules is the different interpretation of specific laws. For example, Directive 95/46/EC does not clearly state whether the flow of data through multiple countries to the storage location is effecting privacy law or not [28].

Furthermore, Directive 95/46/EU does not include specific rules for sensitive information, e.g. on healthcare or physical assistance. Regulations for this specific data are intended to be part of the General Data Protection Regulation [12]. Current legislature also often lacks a definition of which data is personal and therefore has to be classified as sensitive. This hinders the decision concerning which data can be transferred to third countries and what type of data has to be barred from transfer [28].

Cross border data transfer between the EU and the USA increasingly raises concerns since the US government has predominantly denied the need to regulate data protection by law [35]. Hence, the protection of personal data has been handled rather weak [9]. Since the influence of the government on compliance with legal norms is minimal, the responsibility to implement individual data protection rules is subject to the companies [39]. Although the Safe Harbor Agreement provides data protection for data transferred to the US, this regulation is overall criticized since it solely relies on the self-assessment of companies and therefore lacks in independent inspections and monitoring [18]. Furthermore, many companies are suspected of non-compliance regarding to or bad implementation of the principles though being part of the Safe Harbor list [14].

3.3.3. Missing control mechanisms for users

In most cases, using Cloud applications implies the storage and processing of data on external servers. This generally leads to a diminished authority on the side of the remitter [25]. Some EU member states made the customer responsible to check the compliance of the provider's technical and organizational measures. This obviously leads to problems once data is stored on different servers in different locations. Borges et al. (2012) point out that there are numerous solutions to this problem, e.g. the inspection by a certified independent third party [1]. Another potential approach is the inspection based on certifications [18]. Related to Cloud Computing, the Eurocloud Star Audit seal of quality already implemented a certification that checks multiple categories of the provider [11]. Outside of the EU a similar process is neither intended nor possible since most providers are not interested in thorough data protection checks and therefore deny access to the required information by third parties [38].

In Hansen's (2012) opinion, another problem is the inspection of data by the client [17]. Customers are only allowed to get access to data concerning themselves. Hence, they are not able to analyze complete protocols of administrative operations in the system since this could include other client's information. EU Directive 95/46/EC states that a provider is only allowed to process a client's data after he has been given instructions for this operation. As Cloud servers usually store data of different clients it is difficult for the provider to comply with the needs of a single customer without contradicting the requirements of another client [21]. Hypothetically, the provider is obligated to obtain permission every time he is about to process customer's data, which obviously leads to difficulties in practice considering information overflow [12]. Apart from that, too few information increases the lack of transparency. In order to find a better balance in this issue, the General Data Protection Regulation aims to explicitly address the problems that arise from the duty to inform and disclose [17].

3.3.4. Unauthorized access by third parties

Basically, Cloud providers are only interested in their reimbursement and not bound to concrete standards creating certain security measures. Hence, cyber criminals can exploit potential weaknesses in the Cloud and assume the role of a client in order to get access to data [38]. Additionally, there is the risk of providers using a client's data to gain additional revenue, e.g. through advertisement placement. Since there are currently no technological barriers to prevent such unauthorized use of data, a need for individual contracts for the usage of data arises [28]. Otherwise, personal data transfer into a third country could lead to permitted data access by third parties. In addition, government agencies like tax offices also use data espionage for their own purposes [38].

Generally, there is a lack of judicial protection against inappropriate processing of data in the USA [31]. Cloud providers are legally bound by the patriot act to provide all customer data to the government of the US. This does not only affect US based companies but also foreign organizations maintaining a US branch office [18].

Another specific problem is the processing of data in countries that ignore human rights and deny remedy, e.g. China or Iran. In this case, there is a

potential risk of arbitrary access to Cloud servers with the intent of surveillance or prosecution [38].

In sum, current solutions lack in balance between privacy and the necessary access to data with the objective of fighting crime or global security [24].

3.3.5. Cross-border data flows

The Directive 95/46/EC as well as the national data protection laws define data protection requirements in the EU. The transfer of data to countries without certified data protection by the EU commission is forbidden [17]. The requirements for this certificate are high [1]. Therefore, exceptions like Standard Contractual Clauses, Binding Corporate Rules and specifically the Safe Harbor Agreement in the US have been put in place [12]. Those regulations or guidelines respectively, especially the Standard Contractual Clauses, are usually hard to fulfill for Cloud providers. Reasons for this include the lack of flexibility and the differences in the national data protection laws in the EU. In Pearson's (2013) opinion, the Binding Corporate Rules are more suitable for the dynamic Cloud environment. However, the data transfer has to stay inside the company [28]. Therefore, Borges et al. (2012) state that Binding Corporate Rules are not a suitable solution for Cloud Computing since the concept usually involves third party providers [1].

Further on, the Safe Harbor Agreement and the associated method of self-certification is considered to be insufficient to ensure secure privacy [38]. Hence, Gengler (2000) states that Safe Harbor does not provide an adequate level of data protection [10]. Hu et al. (2011) agree that neither the Safe Harbor Agreement nor the Standard Contractual Clauses, although being based on the Directive 95/46/EC, are a safe basis for data protection in Cloud environments [22]. Given the uncompromising way in which the Safe Harbor Agreement was adopted in the year 2000, a lot of US companies chose a reluctant attitude towards it. This is also manifested in the small amount of participants [14]. On the other hand, many companies refuse to include clauses of the Directive 95/46/EC and to commit themselves to the data protection regulations even after the EU implemented possibilities for legal transfer of personal data to third countries [29].

Besides the improvements stated in the previous paragraphs, the upcoming General Data Protection Regulation also aims to ease transfer of personal information significantly by enabling a less complicated cross-border data transfer in the EU [34]. Although this measure has not been passed yet and is still subject to modifications, scientific authors advise US companies to prepare for extensive changes once the regulation enters into force [12].

4. Summary and Conclusions

The purpose of this study was to profile the existing academic literature with regard to current measures for Cloud Computing data protection and the challenges resulting from the application of these regulations. Since a review of the entity of international legislature would be beyond the scope of this paper and impossible regarding space consideration, we primarily focused on data transfer between the economies USA and EU. Although data protection is one of the most critical factors for Cloud technology customers, our analysis of 33 publications revealed a lack of transparency and negligence of that subject in the investigated academic literature. However, an increase of articles addressing this sensitive topic could be observed in 2012 after the first draft for a General Data Protection Regulation in the EU was published.

The Safe Harbor Agreement as well as the Directive 95/46/EC gained most attention in the reviewed articles. While most authors considered the principles of Directive 95/46/EC to be strict and therefore comparatively secure, Safe Harbor is widely criticized because of its self-regulation character and low safety standards. Additional possibilities for legal data transfer out of the EU, i.e. Binding Corporate Rules and Standard Contractual Clauses, were rarely discussed and usually considered not to be helpful for Cloud solutions.

Our content analysis revealed numerous challenges for future research in this area. Many authors criticize the great discrepancy regarding data protection laws between the USA and EU. However, few specific examples can be found in publications. A detailed analysis and comparison of the specific IT law for both economies would allow an evaluation of the gaps in current legislature and enable to develop concepts to improve that situation. The same applies for the statements regarding a lack of direct applicability of current regulations to Cloud technologies: detailed answers to the question why existing privacy policies are not applicable to these solutions could not be found in our literature basis.

Limitations of our study could be seen in a number of ways, which also create opportunities for future research at the same time. First, we primarily investigated IS literature due to our technical background. Hence, a more detailed examination of legal literature is missing so far. Additionally, we focused on legislature regarding the data traffic between the USA and the EU as well as between EU

member states and other third countries. For Cloud Computing considering a global topic that is not restricted to certain areas, there are numerous issues left to analyze data protection law. Especially the emerging markets in Asia and South America could be important for further reviews. Another limitation of our study is the lack of detailed investigation in relation to the imminent General Data Protection Regulation since the currently accessible information is rather vague. Once implemented, this regulation is considered to entail significant changes in EU privacy law and data traffic between the USA and EU member states, which is already reflected in the increasing number of articles on the topic published after the release of the first draft in 2012. Further analysis of the respective literature forthcoming and particularly after the commencement of the regulation could provide better insight into whether the regulation will be able to live up to the promises.

Besides the limitations, we expect a broad impact from this research given the present relevance of Cloud Computing technologies and data protection issues. Against this background, our study provides a valuable overview of current key regulations to be taken into account by practitioners or companies, which are currently using Cloud Computing or tend to apply this technology. Furthermore, we propose several issues that can be addressed by researchers in future studies.

10. References

[1] Borges, G.; Brennschneidt, K.: Rechtsfragen des Cloud Computing – ein Zwischenbericht. In Borges, G.; Schwenk J. (Eds.): Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Springer, Berlin, 2012, pp. 43-77.

[2] Buyya, R.; Yeo, C. S.; Venugopal, S.; Broberg, J.; Brandi, I.: Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. In: Future Generation Computer Systems, 25(6), 2009, pp. 599-616.

[3] Caspar, J.: Zwischen Aufbau und Ausverkauf. In: Datenschutz und Datensicherheit - DuD, 36 (7), 2012, p. 478.

[4] Chaput, S. R.; Ringwood, K.: Cloud Compliance: A Framework for Using Cloud Computing in a Regulated World. In N. Antonopoulos; L. Gillam (Eds.): Cloud Computing - Principles, Systems and Applications. Springer, London, 2010, pp. 241- 255.

[5] Cheng, F.-C.; Lai, W.-H.: The Impact of Cloud Computing Technology on Legal Infrastructure within Internet - Focusing on the Protection of Information Privacy. In: Proceedings of the 2. International Workshop on Information and Electronics Engineering, Harbin, 2012, pp. 241-251.

[6] Desai, D. R.: Beyond Location: Data Security in the 21st Century.In: Communications of the ACM, 56, 2013, pp. 34-36.

[7] Eckhardt, J.: Datenschutz im „Cloud Computing“ aus Anbietersicht. In Borges, G.; Schwenk, J. (Eds.): Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Springer, Berlin, 2012, pp. 97-114.

[8] Flick, U.: Qualitative Forschung: Theorie, Methoden, Anwendung in Psychologie und Sozialwissenschaften, Rowohlt, Reinbek, 1995.

[9] Fromholz, J. M.: The European data privacy directive. In: Berkeley Technology Law, 15, 2000, pp. 461-484.

[10] Gengler, B.: Safe Harbour Unsafe. In: Computer Fraud & Security, 2000 (9), p. 5.

[11] Giebichenstein, R.; Weiss, A.: Zertifizierte Cloud durch das EuroCloud Star Audit SaaS. In: Datenschutz und Datensicherheit – DuD, 35 (5), 2011, pp. 338-342.

[12] Gilbert, F.: European Data Protection 2.0: New Compliance Requirements in Sight - What the Proposed EU Data Protection Regulation Means for U.S. Companies. In: Santa Clara Computer & High Technology Law Journal, 28 (4), 2012, pp. 815-863.

[13] Gilbert, F.: Proposed EU data protection regulation: the good, the bad, and the unknown. In: Journal of Internet Law, 15 (10), 2012, pp. 20-34.

[14] Grant, J.. International data protection regulation: Data transfer - safe harbor. In: Computer Law & Security Review, 21 (3), 2005, pp. 257-261.

[15] Gregor, S.: The nature of theory in information systems. In: MIS Quarterly, 30 (3), 2006, pp. 611-642.

[16] Gritzalis, S.: Enhancing Privacy and Data Protection in Electronic Medical Environments. In: Journal of Medical Systems, 28 (6), 2004, pp. 535-547.

[17] Hansen, M.: Datenschutz im Cloud Computing. In Borges, G.; Schwenk J. (Eds.): Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Springer, Berlin, 2012, pp. 79-95.

[18] Hansen, M.: Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In Camenisch, J. (Ed.): Privacy and Identity Management for Life. Springer, Berlin, 2012, pp. 14-31.

[19] Härting, N.: Starke Behörden, schwaches Recht - der neue EU-Datenschutzentwurf. In: Betriebs-Berater, 67 (8), 2012, pp. 459-466.

[20] Hiller, J. S.: The Regulatory Framework for Privacy and Security. In Hunsinger J. (Ed.): International Handbook of Internet Research. Springer, Dordrecht, 2010, pp. 251-265.

[21] Hon, W. K.; Millard, C.; Walden, I.: Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now. In: Stanford Technology Law Review, 16 (1), 2012, pp. 79-128.

[22] Hu, Y.-J.; Wu, W.-N.; Yang, J.-J.: Semantics-Enabled Policies for Information Sharing and Protection in the Cloud. In: Proceedings of the 3. International Conference on Social Informatics, Singapore, 2011, pp. 198-211.

[23] Janssen, M.; Joha, A.: Challenges for adopting cloud-based software as a service (saas) in the public sector. In: Proceedings of the 25. European Conference on Information Systems, Helsinki, 2011, Paper 80.

[24] Lahlou, S.: Augmented Environments and Design. In Lahlou, S. (Ed.): Designing User Friendly Augmented Work Environments. Springer, London, 2010, pp. 1-29.

[25] Matros, R.; Rietze C.; Eymannm T.: SaaS und Unternehmenserfolg: Erfolgskategorien für die Praxis. In Benlian, A. (Ed.): Software-as-a-Service – Anbieter-strategien, Kundenbedürfnisse und Wertschöpfungs-strukturen. Gabler, Wiesbaden, 2010, pp. 239-254.

[26] Olislaegers, S.: Early Lessons Learned in the ENDORSE Project: Legal Challenges and Possibilities in Developing Data Protection Compliance Software. In Camenisch, J. (Ed.): Privacy and Identity Management for Life. Springer, Berlin, 2012, pp. 73-87.

[27] Palvia, P.; Leary, D.; Mao, E.; Midha, V.; Pinjani, P.; Salam, A.F.: Research Methodologies in MIS: An Update. In: Communications of the Association for Information Systems, 14 (14), 2004, pp. 526-542.

[28] Pearson, S.: Privacy, Security and Trust in Cloud Computing. In Pearson, S.; Yee, G. (Ed.): Privacy and Security for Cloud Computing. Springer, London, 2013, pp. 3-42.

[29] Porwal, S.; Nair, S.K.; Dimitrakos, T.: Regulatory Impact of Data Protection and Privacy in the Cloud. In Wakeman, I. (Ed.): Trust Management V - 5th IFIP WG 11.11 International Conference, IFIPTM 2011, Copenhagen, 2011. Proceedings. Springer, Berlin, 2011, pp. 290-299.

[30] Schneider, J.: Datenschutzrechtliche Anforderungen an die Sicherheit der Kommunikation im Internet. In Borges, G.; Schwenk, J. (Eds.): Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Springer, Berlin, 2012, pp. 21-42.

[31] Schwartz, P.; Reidenberg, J. R.: Data Privacy Law. LEXIS Publishing, Michie, 1996.

[32] Soppera, A.; Burbridge, T.: Maintaining Privacy in Pervasive Computing - Enabling Acceptance of Sensor-Based Services. In: BT Technology Journal, 22 (3), 2004, pp. 106-118.

[33] Spindler, G.: Rechtliche Rahmenbedingungen des „Software as a Service"-Konzepts. In Benlian, A. (Ed.): Software-as-a-Service – Anbieterstrategien, Kundenbedürf-nisse und Wertschöpfungsstrukturen. Gabler, Wiesbaden, 2010, pp. 31-40.

[34] Taupitz, J.: Der Entwurf einer europäischen Daten-schutz-Grundverordnung - Gefahren für die medizi-nische Forschung. In: Medizinrecht, 30 (8), 2012, pp. 423-428.

[35] Thomale, P.-C.: Die Privilegierung der Medien im deutschen Datenschutzrecht. GWV, Wiesbaden, 2006.

[36] Vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: Proceedings of the 17. European Conference On Information Systems, Verona, 2009, pp. 2206-2217.

[37] Webster, J.; Watson, R. T.: Analyzing the Past to Prepare For the Future: Writing a Literature Review. In: MIS Quarterly, 26 (2), 2002, pp. 13-23.

[38] Weichert, T.: Cloud Computing und Datenschutz. In: Datenschutz und Datensicherheit - DuD, 34 (10), 2010, pp. 679-687.

[39] Wood, K.: Exploring security issues in cloud computing. In: Proceedings of the 17. UK Academy for Information Systems, Oxford, 2012, Paper 30.

[40] Zinser, A.: International data transfers between the United States and the European Union: are the procedural provisions of the Safe Harbor solution adequate?. In: Computer Law & Security Review, 20 (3), 2004, pp. 182-184.

[41] Zwingelberg, H.; Hansen, M.: Privacy Protection Goals and Their Implications for eID Systems. In Camenisch, J. (Ed.): Privacy and Identity Management for Life. Springer, Berlin, 2012, pp. 14-31.